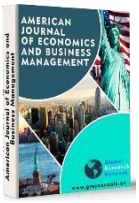


American Journal of Economics and Business Management

Vol. 9 Issue 2 | **pp.** 215-240 | **ISSN:** 2576-5973
Available online @ https://www.globalresearchnetwork.us/index.php/ajebm

Article

Role of Machine Learning in Securing U.S. Digital Advertising Ecosystems Against Fraud and Market Manipulation

Tanvir Rahman Akash[1], Md Shokran[2], Jannatul Ferdousi[3]

1,2. Master of Science in Business Analytics Trine University, USA
3. Master of Busness Administration, San Francisco Bay University, USA

Abstract: The ad fraud and act of coordinated manipulation has become a more sensitive issue in the highly complex ecosystems formed by fast-left programmatic digital advertising. Fraudulent advertising traffic in the United States through the work of automated bots, click farms, and organized campaigns costs a lot of money, worsens the performance metrics of campaigns, and prompts more general inquiries about information integrity and national security. Rudimentary rule-based systems of detecting fraud are unable to scale to changing and evolving attacks, and require newer and more intelligent approaches to security. This study will discuss the use of machine learning to enhance security of the American online advertising ecosystem by identifying fraudulent and possibly cross-border manipulative activity based on user behavior and ad clickstream logs. This study uses a publicly available fraud detection data set, which consists of 2,043 records of ad interactions that have behavioral, time, technical, and geographic features. The main aspects are the intervals of clicking, duration of a session, number of clicks per session, bouncing rate, Devices and browser, geo-location. Machine learning methods are used under supervision to identify ad clicks as legitimate or abnormal, whereby the abnormal behavioral patterns can be observed as signs of automation and coordinated abuse. The standard classification measures are used to estimate the model performance; they are accuracy, precision, recall, F1-score and receiver operating characteristic analysis. The results indicate that machine learning models are useful in obtaining complex non-linear relationship patterns in clickstream behavior that are better than traditional heuristic methods in detecting fraudulent traffic. Behavioral and session-level attributes prove to be close predictors of fraud and geographic ones should present valuable hints at the fraud potential presence of cross-border manipulation. Even though the dataset does not directly accuse foreign actors of any activity, the findings show that machine learning can be used to assist in early detection and risk evaluation of manipulation attempts in digital advertising pipelines. This study will be of value to the emerging literature on ad-tech security because it established the practical relevance of machine learning to increase the levels of trust, transparency, and resilience in American digital advertising ecosystems.

Keywords: Machine Learning, Digital Advertising Security, Ad Fraud Detection, Clickstream Analysis, Programmatic Advertising and Foreign Manipulations Indicator

Citation: Akash T. R., Shokran Md., Ferdousi J. Role of Machine Learning in Securing U.S. Digital Advertising Ecosystems Against Fraud and Market Manipulation. American Journal of Economics and Business Management 2026, 9(2), 215-240.

Received: 10th Jan 2026
Revised: 30th Jan 2026
Accepted: 07th Feb 2026
Published: 14th Feb 2026

1. Introduction

A. Ecosystem Development and Multifacetedness of the U.S. Digital Advertising

Within the last ten years, digital advertising has moved to the forefront of the U.S. economy due to the massive innovation of programmatic advertising, real-time bidding (RTB), and data-driven targeting technology. Advertisers are making more and more use of automated strategies to present personal content on websites, mobile apps, and Internet-

connected gadgets at volumes and velocities previously unknown. These systems allow fine audience targeting, better ROI and real time optimization of performances [1]. An identical automation and scale that boost advertisement efficiency have also augmented complexity within the ecosystem. The current digital advertising ecosystem consists of various intermediaries such as demand-side platform, supply-side platform, ad exchange, data broker and publisher. The transactions are in a high-speed format and have low levels of transparency within the advertising supply chain, which makes it very difficult to audit traffic quality and user authenticity. Cyberspace troublemakers use such structural vulnerabilities to add fraud traffic, distort the indicators of engagement, and earn an unlawful profit [2]. Also, digital advertising platforms have a global presence that allows cross-border involvement which makes it quite challenging to separate between honest international traffic and organized manipulation that has been carried out outside the United States [3]. With the advertising budgets ever increasing and moving to digital platforms, the integrity, security and reliability of the advertising ecosystems are becoming an urgent issue. To solve these issues, sophisticated analytical techniques, able to work on a large scale, evolve to meet new threats and safeguard the interests of advertisers both financially and reputation-wise, are needed.

B. Problem Statement

Regardless of ongoing technological advancement, the U.S. digital advertising ecosystems undergo significant losses to ad fraud and manipulative practices including automatized traffic, bot-based clicks and orchestrated abuse [4]. These practices misrepresent campaign performance indicators, cause adverse confidence among advertisers, and cause the wasteful deployment of marketing funds. The conventional rule-based models of fraud detection are not always adequate because they use fixed thresholds and pre-established patterns that do not keep pace with the swiftly changing methods of attacks and large amounts of data. Moreover, the increased application of behavioral and geographic manipulation opens the threats of cross-border and possibly foreign-origin operations [5]. This means that there is an urgent requirement in adaptive, scalable and intelligent detection mechanisms that can detect fraud and manipulative behavior in real-time.

C. Machine learning as a security facilitator in online advertising

Machine learning has become a significant solution to such complex security issues in the digital advertising space. By contrast with traditional systems with heuristic-based systems, machine learning models have the ability to analyze large amounts of behavioral and clickstream data to reveal hidden patterns, correlations and anomalies, which are indicators of fraudulent activity [6]. Through historical data education, these models are constantly enhanced to be able to differentiate between legitimate human behavior and automated or malicious interaction. The techniques of supervised learning allow properly classifying the clicks of an ad into two categories namely fraud and legitimate by utilizing the labeled sets and deriving predictive variables like frequency of clicks, length of session and bouncing rates [7]. Parallel to that, unsupervised and anomaly detection methods are useful in detecting new attack patterns, previously unfamiliar, and thus they are efficient in stopping new tricks of fraud. Real-time detection and automated response of machine learning is also important in the high-speed advertising environment where a delay in intervention can lead to huge losses. Since threats in digital advertising keep on changing, machine learning offers flexibility and scalability to achieve dynamic ecosystems [8]. The combination of behavioral, technical and geographic indicators makes it especially applicable to curb fraud and determine the risk of manipulation by advertising pipelines in the modern world.

D. Objectives of the Study

This study seeks to assess the effectiveness of machine learning in identifying the risk of ad fraud and manipulation of digital advertising platforms in the U.S. Specific objectives:

- To process the user behavior and click on the stream information to spot fraudulent ad interactions.
- To generate machine learning models to distinguish between legitimate and fraudulent ad clicks.
- To assess the performance of the models through conventional classification measures.
- To determine the important behavioral and technical characteristics of fraud detection accuracy [9].
- To analyze geographic and session-based proxy variables of abnormal advertising activity.
- To determine the extent to which machine learning can be used to improve the security of digital advertisement.

E. Research Questions

This study explores the possibility of improving fraud detection and manipulation risk evaluation in the digital advertisement setting through machine learning methods. Research questions:

1. How effective can machine learning models be able to detect fraudulent ad clicks based on user behavior and click data?
2. What behavioral, temporal and technical characteristics play the largest roles in determining the accuracy of fraud detection?
3. How far is it possible to identify the potentially manipulative or cross-border advertising activity using geographic and session-level indicators?

F. Significance of the Study

This study could contribute to the academic and practical importance as it will show how machine learning can be used to enhance security in the U.S. digital advertising ecosystems. Ad fraud has been a long time menace in invalidating advertiser trust, overcharging, and manipulating performance metrics [10]. This study offers a scientific contribution to the comprehension of the manifestation of a fraudulent activity in actual advertising settings due to its emphasis on behavioral and/or clickstream indicators. Academically, the study will add to the existing body of research on the fundamental principles of ad-tech security through empirical assessment of machine learning procedures to identify fraud using testable advertising data. It underlines the significance of behavioral analytics and feature-level insight in the identification of the legitimate user engagement and the automated abuse [11]. The results also confirm the relevance of geographic and session-based signals as the alternative tell-tales in the measurement of the manipulation risk. In essence, the study provides useful information to advertisers, advertising platforms, and policy makers aiming at enhancing transparency, accountability, and trust in the digital advertising systems. The machine learning-based solution suggested will help in the support of scalable and dynamic security structures that can respond to the changing threats. In the end, the research contributes to the creation of robust, smart, and data-related resolutions in preserving digital advertising ecosystems against fraud and possible manipulations.

Literature Review

A. Online Advertising Systems and Privacy Lapses

Digital advertisement ecosystems have become very automated and data-driven systems, which are based on bidding in real-time, user-profiling, and programmatic advertisement delivery. Such systems entail the involvement of various interrelated parties, which include advertisers, publishers, ad exchange, demand side platforms as well

as supply side platforms. Although this automation has made it more efficient and scalable, it has also created great security threats [12]. The advertising supply chain is also complicated, which lowers the level of transparency and leaves blind spots that can be used by the malicious actors. Fraud traffic may be introduced on different levels, and it becomes even more challenging to detect and assign it. The high turnover and speed of transactions are the main factors that create security challenges in the digital advertisement world. The advertisement impressions and clicks are processed in milliseconds, which restricts the possibility of monitoring or checking it manually. This speed is abused by fraudulent actors who use it to create fraudulent clicks and impressions without detection systems being able to react to them. Also, using third-party sources of data and cross-platform integrations expose more to manipulated or spoofed traffic [13]. These weaknesses undermine accuracy of measuring the campaign, inflate advertising budget, and weaken trust among stakeholders. The other significant issue is that digital advertising is global. Advertising platforms are not limited by national borders and this allows traffic to be sent by different geographic regions. Even as international outreach is critical to legal marketing, it enables ill-minded actors to conduct their activities in areas with little regulatory supervision. By conducting coordinated manipulation campaigns, it is possible to capitalize on geographic diversity in order to avoid detection and this makes the enforcement of security even more complex. Digital advertisement ecosystems continue to experience systemic problems in terms of fraud aversion, quality assurance of traffic, and risk management when it comes to manipulation. To cover these gaps, it is necessary to use complex analytical methods that can handle large volumes of data and respond to changes in threat patterns.

B. Ad Fraud Methods and Behavioral Spreadsheets

Ad fraud is a very broad category which covers various types of fraud schemes aimed at creating invalid advertising engagement. Popular methods are bot-based click frauds, impressions stuffing, domain spoofing and automated traffic generation with compromised devices [14]. These actions are supposed to replicate the valid user activities and maximize fraud revenues. The behavior pattern of fraudulent traffic is usually typical, including excessively high levels of click rates, extremely short or discontinuous times of click, unnatural session time, and uneven engagement rates. Fraud in the advertising systems can be detected with the help of behavioral indicators. Also, there are session-based metrics, such as the number of clicks per session and bounces, which give a picture of the authenticity of user engagement. Unethical interactions are often associated with quick series of clicks with little or no real interaction, which leads to inflated and false-looking click counts and uncharacteristic session metrics. Another indicator is the diversity of devices and browsers, since a large portion of fraudulent campaigns can reuse a few technical settings to push massive traffic. Fraud is also detected by temporal patterns [15]. The automated systems can generate clicks at a predetermined time or unnatural time window, which is not in line with the natural human behavior [16]. These patterns may be used in combination with geographic determination to demonstrate coordinated activity, or scripted activity. Even though individual indicators do not necessarily lead to the conclusion of fraud, the combination of indicators can be used to enhance the accuracy of detecting fraud. These behavioral characteristics can be used to create effective detection models and thus understanding them is crucial and the basis of applying machine learning methods in detecting fraudulent interactions in advertising.

C. Artificial Intelligence of Ad Fraud Detection

Machine learning has become one of the effective methods of ad fraud detection, as it is capable of processing complex, high-dimensional data. As opposed to rule-based systems, machine learning models have the capability to use historical trends and evolve with changing attack techniques. The techniques of supervised learning are typically applied when labeled data sets exist so that the models can learn how to classify

interactions as fraudulent or legitimate through the relationships between features [17]. These models are able to model non-linear relationships between behavioral, technical, and time-related variables that are often ignored by the traditional methods. Besides the supervised learning, unsupervised and semi-supervised methods will also come in handy in identifying new patterns of fraud. Anomaly detection does not need explicit labels of fraud to identify abnormal behavior and accordingly are effective in detecting novel or new attacks to the system [18]. The use of feature engineering is especially important in the context of machine learning performance, which is due to the fact that the expression of behavioral metrics is greatly affecting the accuracy of detection in a well-designed intervention. Such methods as scaling of features, coding of nominal variables, and time aggregation improve the effectiveness of the models. Machine learning is also used in real-time detection and automated response which are necessitated in the fast-paced advertising landscape. Detecting systems are capable of evolving with changes in user behavior and fraud strategies by constantly updating structure with the new information [19]. Issues like model drift, imbalance in the classes and interpretability are also aspects that need to be taken into account. Even in the face of these hurdles, machine learning is a scalable and adaptive platform on which the digital advertising systems can be secured against fraudulent activity.

D. Digital Advertising on Geographic and Manipulation Risks

In digital advertising ecosystems, geographic data is becoming more and more relevant to deciding the risk of manipulation. Although the legitimate advertising campaigns mostly aim at the global audience, abnormal geographic traffic patterns can be the evidence of organized or manipulative activity. An increase in traffic in certain areas or certain specific areas alone, particularly accompanied by unusual behavioral signalers, may indicate the existence of automated or coordinated campaigns [20]. Such tendencies are especially applicable when the issue of cross-border manipulation is considered, as a set of malicious actors can use geographic diversity to cover their fraudulent activities. Manipulation threats are not limited to financial fraud and may be taken to the level of influencing information exposure through the use of advertising tools. Utilizing coordinated campaigns can help to hype certain narratives or unleash a particular demographic using advertising platforms. Even though geographic data cannot alone make intent and attribution, it is a good contextual information when combined with the behavioral and technical aspects. The session-level and time-based patterns also enhance the discovery of coordinated activity by showing a concurrent behavior between two or more users or devices [21]. Machine learning models allow incorporating geographic indicators into more extensive risk assessment models. Models can be used to detect clusters of abnormal behavior by forming location data with clickstream behavior, which can require additional investigation. This is a risk-based practice that aids in the early identification and prevention without necessarily assigning blame to particular actors. Since digital advertising is still perceived to intersect with larger societal and informational issues, it is vital to integrate geographic analysis into the system of fraud detection to increase ecosystem resilience and integrity.

E. Empirical Study

In the article The Role of Artificial Intelligence in Ad Fraud Detection in the Block chain and Programmatic Advertising Ecosystem by Munise Hayrun Sağlam and Ibrahim Kircsova, the authors consider how artificial intelligence improves ad fraud detection in the current programmatic advertising landscapes. The research highlights that the magnitude, velocity and mechanization of real-time bidding systems have greatly made the systems susceptible to frauds like click fraud which incurs huge financial losses on the part of the advertisers. The authors emphasize the usefulness of the machine learning and deep learning methods that allow detection of the abnormal patterns of behavior that cannot be detected by the traditional rule-based systems. Also, the chapter addresses the

concept of the introduction of the block chain technology as the supplementary solution that will ensure transparency, immutability, and traceability of advertising transactions [1]. Blockchain enhances the supply chain of ad interactions, with trust and data integrity, by storing this data on a distributed ledger. The article highlights that secure infrastructure can be enhanced with AI-driven analytics to achieve high detection accuracy and reliability of campaigns. This article is of great interest to the current study because it supports the significance of machine learning to detect fraud and puts the aspect of machine learning in greater technological ecosystems. The lessons help to argue that smart, evidence-based strategies are critical to protecting digital advertising systems to an even greater number of sophisticated fraud and manipulative practices.

In the article, Personalization and Consumer Privacy: Balancing Targeted Marketing and Trust by Akhtaruzzaman Khan, Sanjida Akter Sarna, and Md. Abul Kalam Azad, the authors highlight the mounting tension that exists among personalized digital marketing programs and their impact on consumer privacy. The analysis reveals that consumer engagement, conversion rates, and brand loyalty are increased with the help of data-driven personalization using user behavior analytics [2]. It also highlights the fact that there are high ethical and privacy risks brought on board by more data gathering and tracking of behaviors. The results highlight the fact that customers are growing more receptive to the way their personal information is gathered, processed, and utilized, especially when it comes to automated and algorithm-driven marketing. Such regulatory frameworks as GDPR and CCPA are mentioned as necessary tools to provide transparency and accountability throughout the data practices. This article applies to the current study because it supports the significance of proper data management by implementing machine learning tools within the digital advertising landscape. Though machine learning also supports the detection of fraud and effective advertisement, the article promotes that the trust, ethical governance and the ethical system design must be taken into consideration in order to achieve the sustainability of it in the long-run. These remarks can be used to argue that safe and transparent machine learning systems are necessary to retain consumer trust and prevent fraudulent and deceptive activities in online advertising.

In the article Combating Evolving Threats: A Systematic Review of Online Ad Fraud Detection by Baranidharan Subburayan, David Winster, K. Dhanalakshmi, and R. Rajkumar, authors give a review of the research on the topic of online ad fraud detection and brand safety that was published between 2011-2024. The paper illustrates the ongoing and dynamic character of ad fraud especially click fraud and how the scam methods keep evolving to avoid being detected [3]. The review describes machine learning as one of the key elements of modern ad fraud detection and shows that it is better than the traditional approach, which is based on rules and cannot process large and complex advertising datasets. It also talks about the increasing significance of mobile advertising, whereby, user actions and data trends on mobile devices have a specific set of user data that needs special detection techniques. In addition to the issue of click fraud, the article highlights newer forms of threats like impression fraud and placement fraud which increase the advertising security problem. Also, the review highlights the growing significance of brand safety and the necessity to safeguard the reputation of an advertiser in automated advertising settings. The article is very pertinent to the current research issue because it enables the application of machine learning in detecting fraud and validates the need to have adaptive, collaborative, and scalable solutions in securing digital advertising ecosystems.

In the article Strategies for Combating Synthetic Identity Fraud: The Role of Machine Learning and Behavioral Analysis in Improving the Financial Ecosystem Security by Okunola Orogun, Lanre Ogungbe, Niyi Adegboye, Tolu Adetuyi, and Samuel Alabi, authors investigate a more sophisticated approach to detecting a synthetic identity fraud based on machine learning and behavioral analysis. The paper highlights the importance of the fact that contemporary frauds have come to depend more on the combination of real and fake qualities in order to bypass the traditional detection mechanisms [4]. Using the

methods of proximity, graph convolutional networks, and behavioral clustering, the study proves how machine learning can help to differentiate natural human behavior, automated, or malicious behavior. The authors emphasize the efficiency of behavioral cues and network affinities in detecting coordinated fraud patterns, but admit the issue of data quality and scalability and the computational complexity. Despite the fact that the research falls in the framework of finances and identity management, the methodological implications are very applicable to the context of digital advertising fraud detection where automated and synthetic action is also used to compromise the integrity of the system. The article substantiates the thesis that the machine learning models which are based on behavior are more effective in their detection compared to the traditional even-based approaches.

In the article AI-Powered Business Analytics in Marketing: Strategy of Analysis of Consumer Data on a Large Scale to Make a Decision in the U.S. Market by Md Saiful Islam, Md Shokran, and Jannatul Ferdousi, authors investigate how analytics based on artificial intelligence can optimally improve marketing decisions in the U.S. market by analyzing consumer data on a large scale. The paper shows how AI methods like sentiment analysis, predictive modeling and recommendation systems identify valuable behavioral patterns of online review data, both structured and unstructured. The results emphasize the effectiveness of AI-related solutions in comparison with conventional analytics as they are capable of identifying temporal patterns, customer engagement cycles, and the subtle changes in consumer behavior that cannot be detected using traditional tools. Despite the article focusing on marketing analytics, its methodological knowledge is of great relevancy to the sphere of digital advertising security studies [5]. The focus on recognizing behavioral patterns, detection of anomalies in metrics of engagement, and predictive modeling is similar to the methods of ad fraud detection based on machine learning. The research also highlights the role that AI systems can help in processing large high-velocity data to reveal hidden patterns, which is essential in detecting abnormal or manipulative advertising interactions. These lessons are helpful in the current study because they substantiate the role of AI as a scalable and adaptive analytics tool that can improve trust, precision and resilience in contemporary digital advertising ecosystems.

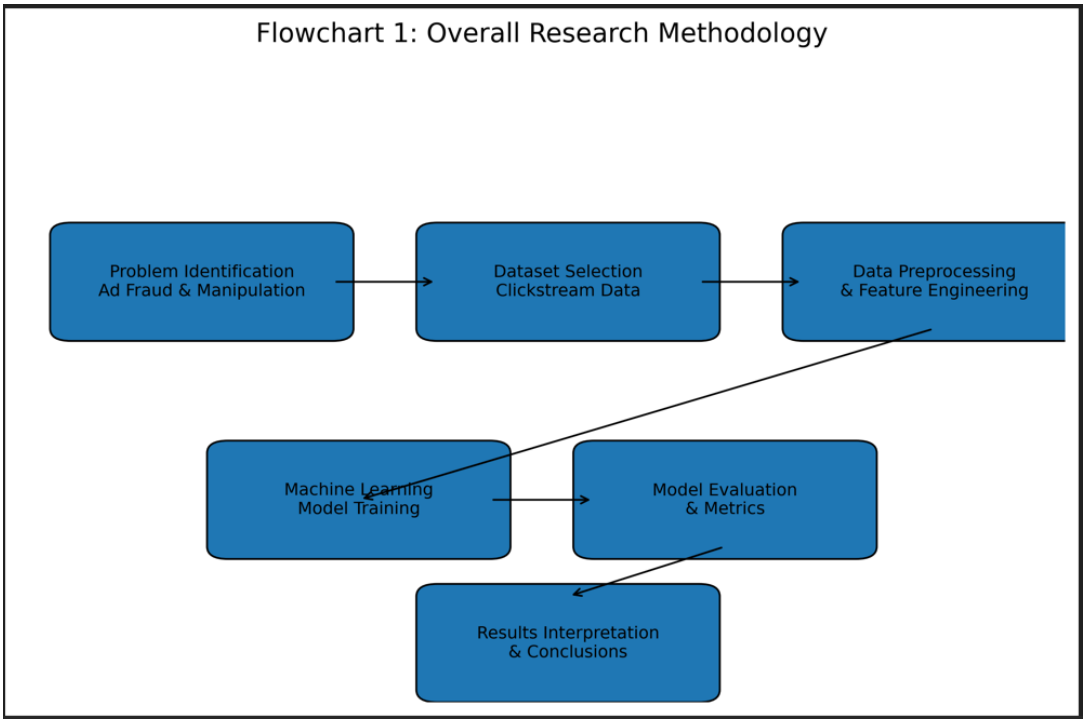
2. Methodology

MethodologyThe This study uses a quantitative and machine learning-based approach to analyses the risks of fraud and manipulation in the digital advertising ecosystems in the United States. The study uses structured ad clickstream data and supervised learning methods to determine fraudulent advertising interactions in terms of behavioral, temporal, and contextual attributes. The methodology incorporates the data preprocessing, feature engineering, model development and performance evaluation to determine the effect of detection [22]. They are focused on behavioral analytics and explainable machine learning in order to promote transparency and reliability. This methodical framework allows to analyze the threats of advertising security in a scaled manner and empirically evidence how machine learning can help in eliminating ad fraud.

A. Research Design and Approach

The research design that will be employed in this study is a quantitative-based research design that is data-driven to determine the importance of machine learning in identifying the risk of ad fraud and manipulation in the digital advertising ecosystem in the U.S. The study is an experiment where the supervised machine learning approaches are used to the labeled clickstream data to recognize the advertising interactions as being legitimate or fraudulent. This design will allow objective evaluation of model performance and empirically address the effectiveness of fraud detection [23]. The methodology focuses on behavioral and temporal study as it is clear that fraudulent advertising behavior frequently appears in the form of abnormal engagement instead of single technical signals.

Based on characteristics like click intervals, session duration, and frequency of interaction, the research study will capture nuanced abnormalities of the normal user behavior, which will demonstrate automatization or abusive collusion [24]. The first step in descriptive analytics is to comprehend traffic composition and behavioral distributions, then the second step is predictive modeling to assess classification capabilities. A combination of descriptive and predictive elements will enable the study to not only investigate the patterns of data behind the scenes, but it will also be capable of evaluating the machine learning performance in the real world. This structure is especially applicable to the large-scale digital advertisement settings where fraud is entrenched in high amounts of legitimate traffic. In general, the research design will guarantee the rigor of the methodology, scalability, and applicability to the real-life advertising security issues.



This flowchart depicts the entire research procedure of machine learning-based ad fraud detection

The flowchart is a general outline of the research methodology that will be applied in the study to investigate the suitability of machine learning in protecting U.S. digital advertising ecosystems. The initial stage is problem identification which concentrates on the issues of ad fraud and manipulation [25]. It then continues to dataset selection whereby the clickstream data are selected as the major data. The second step is the preprocessing of data and feature engineering of the data in order to ready up the dataset to be analyzed. The training of machine learning models is then conducted in order to categorize advertising interactions. The method proceeds on with the evaluation of the models using performance metrics, and finally interpreting the results and concluding. Such systematicity, transparency and reproducibility in the execution of research is guaranteed by this structured workflow.

B. Data source and Dataset Characterization

This study employs a publicly available crowd-sourced dataset of fraud detection using user behavior and ad clickstream logs, consisting of 2,043 records of advertising interaction. The data set records the behavioral, temporal, technical, and geographic aspects of the digital advertisement clicks. The important characteristics are click interval, session length, number of clicks during a session, bounce rate, type of device, and type of

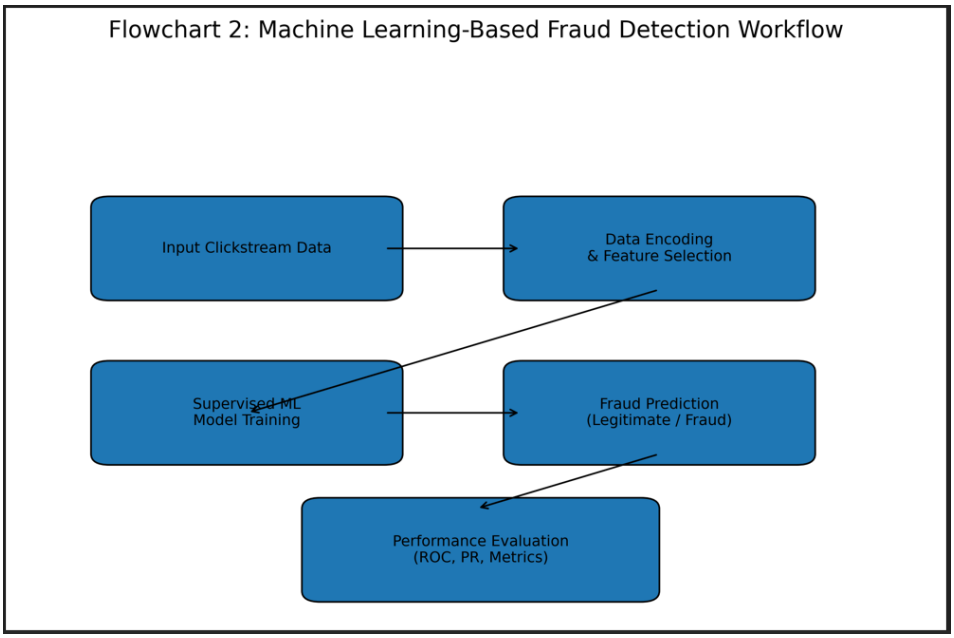
browser, geo-location, user and advertisement id. The target variable, click_label, indicates that every interaction is legitimate (0) and fraudulent (1), which allows using machine learning under supervision. Such a labeling structure enables the assessment of predictive models and allows comparing performance in terms of various metrics. The dataset is realistic with regards to the advertising traffic scenarios in which there is a presence of fraudulent interactions, and a high number of real legitimate users. Behavioral and session-level characteristics can give a good understanding of the engagement patterns, whereas temporal and geographic characteristics can help identify abnormal and possibly coordinated activity [26]. The data is published under a public domain license and therefore ethical, transparent and can be reproduced. Its systematic structure and its ability to be diverse make it the best format to examine ad fraud detection and the evaluation of machine learning based security measures in digital advertising ecosystems.

C. Preprocessing and Engineering of the Data

Before the development of a model, data is preprocessed to guarantee the quality, consistency, and compatibility of data with machine learning algorithms. Categorical data is converted into numeric values, e.g., browser type, device type, geo-location, user ID, and ad ID, to be open to training the model. Attributes that are temporal are also standardized to ensure consistency between records and minimize bias in scaling [27]. This is done by reviewing records with irrelevant, or redundant information to reduce noise and enhance efficiency in learning. The engineering of features is aimed at maintaining behavioral predictors of a true user interaction and fraud interaction. The metrics that are stored being session-based such as the duration of the session and the amount of clicks per session are relevant in tracking abnormal behavior [28]. The interval characteristics of clicking are highlighted to capture automation and similar repetitive patterns of interaction that are frequently related to bots and scripted activity. Another objective of the preprocessing stage is to balance the model complexity and interpretability by removing features with low impact whose removal will not make the model significantly better in prediction accuracy. The study improves the model performance with transparency because of the refined feature set [29]. This is a systematic process of preprocessing and feature engineering that is designed to make sure that a machine learning model is trained on quality and behaviorally pertinent data that is consistent with the goals of detecting fraud.

D. Development of a Machine Learning Model

The machine learning to classify advertising interactions as a case of fraud or legitimate is a supervised method. Stratified sampling is used to split it into training and testing subsets so that the original class distribution is maintained. This makes sure that legitimate and fraud cases are well represented in the process of model training and evaluation [30]. The reason why a tree-based ensemble learning model is chosen is because it can obtain non-linear relationships, mixed features with different types, and interpretable scores on feature importance. The model is trained on behavioral, temporal, technical as well as geographic attributes to learn characteristic patterns of fraudulent activity. Ensemble techniques perform well especially in the detection of fraud cases since these techniques minimize over fitting and enhance their generalization to different data patterns [31]. The model development focuses on explain ability besides predictive accuracy. The importance of features analysis is done to determine which variables have the greatest impact on the classification results. This improves the transparency and trust on machine learning-based security systems. The trained model makes probability predictions enabling it to be flexible in terms of selecting a threshold to detect fraud [32]. The development process of the model trades off the possibilities of detection, interpretation, and scalability, which makes it an appropriate tool to use in real-world digital advertising.



This flow diagram represents machine learning workflow in the detection of fraudulent advertising clicks

The flowchart below provides the machine learning-based fraud detection process used to categorize the advertising interactions as a genuine or a fraudulent interaction. It starts with an input clickstream data obtained due to online interactions of digital advertising. The data is then encoded and selected to convert raw behavioral and technical data into model able inputs. Training of machine learning models is done with supervised data that is labeled so that the patterns of fraudulent behavior can be learned [33]. The trained model provides a prediction of the frauds by categorizing the clicks as legitimate or fraudulent ones. Lastly, the performance is evaluated based on ROC, precision- recall and classification performance measures to give the model its effectiveness.

E. Model Assessment and Metrics of Performance

The evaluation of model performance is performed with the help of numerous measures to cover the imbalance in classes and the security-critical aspect of fraud detection. To determine the true positives, true negatives, false positives, and false negatives a confusion matrix is utilized to give a detailed interpretation of the classification [34]. To evaluate the accuracy of detection and the trade of false alarms and lost fraud incidents, precision, recall, and F1-score are computed. The importance of recall is explained by the high price of undetected fraud in the digital advertising landscape [35]. The analysis of trade-offs between detection of fraudulent clicks and false positives under various decision thresholds is done using precision-recall curves. Also, receiver operating characteristics (ROC) analysis and area under the curve (AUC) are used to assess the overall discriminatory ability of the model. Via visual analytics, the behavior of models can be interpreted and the limitations of performances pointed out. This multimetric evaluation model will also make sure that the effectiveness of the model is evaluated as a holistic approach instead of only focusing on the overall effectiveness [36]. The evaluation process allows drawing sensible conclusions about merits and demerits of the offered machine learning strategy to detect ad fraud because it integrates threshold-independent and threshold-specific metrics.

F. Limitations

This study has a number of limitations, in spite of the contributions it has made. The dataset itself is class-imbalanced and this impacts the sensitivity of fraud detection and can produce lower recall of fraudulent interactions [37]. Also, the data lacks explicit

designations of the foreign influence activities, which restricts the opportunity to make concrete attribution statements. Geographic indicators are thus seen as warning signs and not evidence of manipulation. Simulated size and data may not be representative of the complexity of both large scale and real-time advertising environments. These restrictions are recognized in order to be able to interpret findings in a responsible manner and to make the future research orient to more extensive datasets and sophisticated modeling methods.

I. Dataset

A. Screenshot of Dataset

	A	B	C	D	E	F	G	H	I	J	K
1	user_id	ad_id	click_time	click_interval	browser_type	device_type	geo_location	session_duration	num_clicks_in_session	bounce_rate	click_label
2	user_102	ad_95	1/1/2025 0:00	31.15773252	Firefox	Mobile	DE	257.0224074	2	0.20329004	1
3	user_435	ad_226	1/1/2025 0:01	120.733935	Edge	Desktop	DE	358.8911118	3	0.357177578	0
4	user_348	ad_38	1/1/2025 0:02	30.13515357	Edge	Desktop	US	323.0055612	2	0.261324939	0
5	user_270	ad_28	1/1/2025 0:03	46.57456423	Firefox	Mobile	UK	312.3472315	2	0.113106117	0
6	user_106	ad_244	1/1/2025 0:04	226.0982042	Safari	Desktop	IN	224.5957508	4	0.176551289	0
7	user_71	ad_235	1/1/2025 0:05	156.6150367	Firefox	Desktop	US	494.4107704	4	0.198601688	0
8	user_188	ad_184	1/1/2025 0:06	12.03139476	Safari	Desktop	IN	252.029326	3	0.802257273	0
9	user_20	ad_271	1/1/2025 0:07	67.18132209	Firefox	Desktop	DE	296.9747338	4	0.068404014	0
10	user_102	ad_235	1/1/2025 0:08	3.552439176	Firefox	Desktop	IN	281.2966371	4	0.349861956	0
11	user_121	ad_238	1/1/2025 0:09	78.67677056	Firefox	Desktop	UK	495.4711197	1	0.326500254	0
12	user_466	ad_265	1/1/2025 0:10	130.319312	Edge	Tablet	BR	270.9185387	5	0.307208102	0
13	user_214	ad_64	1/1/2025 0:11	15.13599041	Chrome	Mobile	UK	261.7658059	4	0.301468501	0
14	user_330	ad_176	1/1/2025 0:12	40.91052388	Firefox	Desktop	IN	311.8311148	1	0.540633083	1
15	user_458	ad_2	1/1/2025 0:13	60.86717811	Edge	Mobile	US	230.6459111	5	0.212494942	0
16	user_87	ad_141	1/1/2025 0:14	302.3860282	Chrome	Tablet	DE	311.1599717	4	0.335191785	1
17	user_372	ad_157	1/1/2025 0:15	599.8747291	Chrome	Desktop	BR	537.160358	1	0.015749648	0
18	user_99	ad_145	1/1/2025 0:16	5.514127462	Firefox	Mobile	US	329.9695556	2	0.141649006	0
19	user_359	ad_292	1/1/2025 0:17	171.7589856	Safari	Desktop	US	326.3245922	4	0.302186941	1
20	user_151	ad_152	1/1/2025 0:18	55.77309892	Safari	Desktop	UK	228.2095107	2	0.124643593	0
21	user_130	ad_192	1/1/2025 0:19	59.80011323	Safari	Desktop	IN	470.9207154	6	0.350442089	0
22	user_149	ad_72	1/1/2025 0:20	168.4201741	Firefox	Desktop	UK	493.9032701	4	0.357799994	0
23	user_308	ad_139	1/1/2025 0:21	300.7499991	Safari	Desktop	IN	385.2680376	6	0.340355542	0
24	user_257	ad_186	1/1/2025 0:22	361.7374544	Edge	Desktop	UK	365.3833223	4	0.242236038	0
25	user_343	ad_292	1/1/2025 0:23	103.2807532	Edge	Desktop	US	276.5234649	4	0.227468283	0
26	user_491	ad_60	1/1/2025 0:24	53.01588008	Edge	Tablet	DE	339.1337581	2	0.055135268	0
27	user_413	ad_197	1/1/2025 0:25	185.8853171	Edge	Tablet	IN	216.4842395	1	0.293834158	0
28	user_293	ad_294	1/1/2025 0:26	34.68217707	Chrome	Desktop	BR	187.3886024	3	0.367243392	0
29	user_385	ad_10	1/1/2025 0:27	99.63394091	Edge	Desktop	BR	151.2640083	2	0.300506093	0
30	user_191	ad_61	1/1/2025 0:28	53.28820943	Safari	Tablet	US	341.0673973	4	0.338642694	0
31	user_443	ad_225	1/1/2025 0:29	128.2739788	Firefox	Tablet	UK	162.1625528	5	0.057250197	0
32	user_276	ad_152	1/1/2025 0:30	32.99542427	Safari	Tablet	UK	250.0364597	0	0.41965355	0
33	user_160	ad_198	1/1/2025 0:31	25.52274807	Edge	Desktop	US	293.8770625	5	0.16102056	0
34	user_459	ad_51	1/1/2025 0:32	300.4747178	Chrome	Mobile	BR	399.52904	3	0.21739406	0
35	user_313	ad_259	1/1/2025 0:33	12.88399424	Edge	Mobile	BR	242.1779833	3	0.50423086	0
36	user_21	ad_58	1/1/2025 0:34	84.61614701	Firefox	Mobile	UK	411.3272313	5	0.321009301	0
37	user_252	ad_71	1/1/2025 0:35	29.94663227	Safari	Mobile	IN	393.9158913	0	0.608011778	0

click_data (1)

(Source Link: https://www.kaggle.com/datasets/programmer3/fraud-detection-dataset)

B. Dataset Overview

This study uses publicly available datasets on fraud detection, which is a user behavior and log of ad clicks, to determine how machine learning contributes to ensuring U.S. digital advertising ecosystems remain free of fraud and manipulation [38]. The data comprises 2,043 individual records of advertising interaction, and each one of the records signifies the interaction between a user and an advert in the form of one user-advert click. It models realistic patterns of legitimate as well as fraudulent activity which are usually witnessed in programmatic advertising settings. The data entails a full compilation of the behavioral, temporal, and technical, along with geographic characteristics that are crucial in detection of fraud. Such behavioral characteristics as the time of the session, the number of clicks per session and bouncing would reveal the quality of user interactions and allow to differentiate between real human-human and automated or scripted activity. The timing and frequency of interaction, as well as the temporal characteristics, such as click timestamps and click intervals, can be analyzed based on the temporal attributes that are important predictors of bot-based or organized fraud. Such technical features as the kind of browser used and the type of device served facilitate the analysis of cross-platform

interaction, whereas the geographic location data can be used to perform the spatial assessment of the traffic origin and the possible risks of cross-border manipulations. Uniqueness identifiers of users and advertisements help to detect repetitive interaction and coordinated behavioral patterns without disclosing personally identifiable information. The target variable, click label, indicates that each interaction can be legitimate (0), or fraudulent (1), which allows the development and testing of the supervised machine learning model. The data set has an imbalance in classes, which is representative of the real-world advertisement traffic, with legitimate interactions greatly exceeding fraudulent ones, thus, offering the realistic environment to evaluate the detection performance [64]. The dataset is published under public domain license and thus is ethically compliant, transparent, and results are reproducible. This data provides a solid and sufficient basis to consider machine learning-based solutions to the ad fraud detection and manipulation risk assessment of digital advertising systems.

3. Results and Discussion

This study outputs the analytical results of the machine learning techniques applied to the ad clickstream fraud detection dataset. The findings are aimed at determining the distribution of legitimate and fraudulent clicks, the most significant patterns of behavior and geography related to the commitment of fraud, and the effectiveness of the suggested machine learning model. Temporal, session-level, and spatial abnormal advertising interaction indicators are studied by descriptive and behavioral analyses [35]. The use of model-based assessments, such as feature importance, confusion matrix, precision-recall analysis, and ROC analysis, is utilized to evaluate the effectiveness of classification and highlight the limitations of performance in future sections of the paper through empirical evidence of the problem under analysis.

A. Legitimate and Fraudulent Ad Clicks Distribution

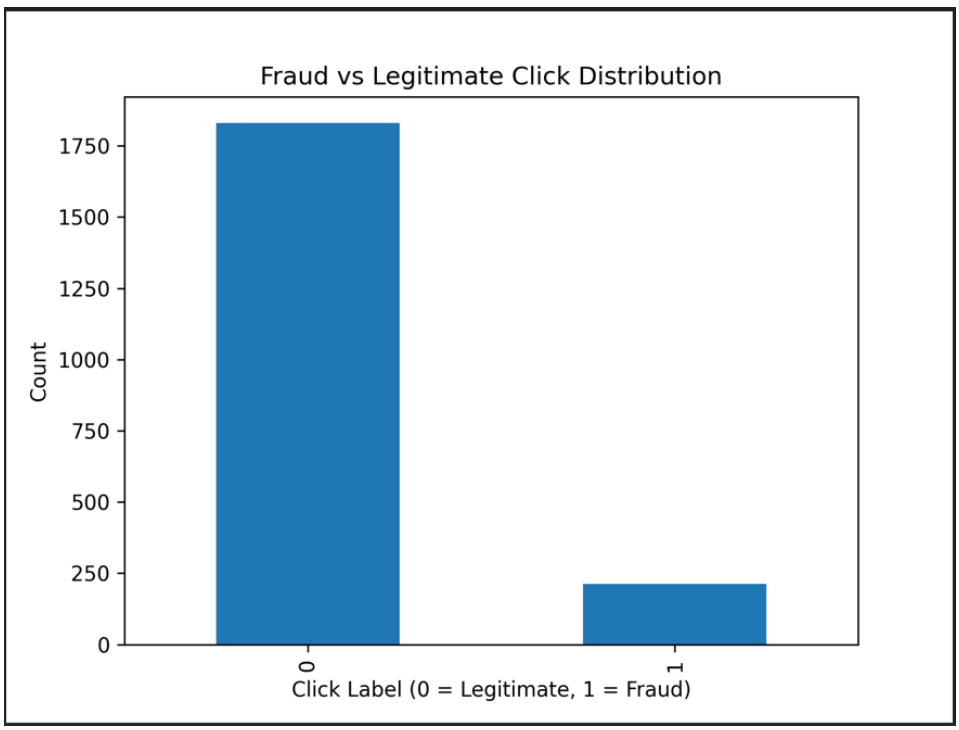


Figure 1. This image shows the distribution of the legitimate and the fraudulent clicks of adverts.

The figure 1 indicates the distribution of legitimate and fraudulent ad clicks within the dataset of clickstreams that were used in this research. The bar chart will provide an

obvious emphasis on the strong asymmetry of normal and fraudulent interactions, where the legitimate clicks (label 0) will have the highest number of interactions recorded, whereas the number of fraudulent clicks (label 1), will have a small but significant fragment of the dataset. Such distribution is representative of the federal digital advertising space, in which fraudulent activity is a percentage of overall traffic, but a significant threat in terms of financial and operational capital, as it continues to be large and persistent. Having multiple hundred fraudulent interactions suggests that ad fraud is a serious phenomenon that has the potential to skew campaign statistics, overstate engagement, and decrease advertiser ROI. Machine learning-wise, the nature of this class distribution introduces the significance of the application of sound classification strategies that are able to effectively identify minority class events without being skewed on the wider legitimate traffic. Such imbalance also explains why metrics of evaluation, including recall, precision, and F1-score, should be used to specify meaningful performance of fraud detection. The distinct distinction between the two groups confirms the suitability of the dataset to the supervised learning method because enough labeled examples of both legitimate and fraudulent clicks are present to train and test the model [36]. Against the background of winning U.S. digital advertising ecosystems, this allocation highlights the difficulty that the advertiser and the platform have in detecting fraudulent engagements concealed in heaps of legitimate traffic. The number creates a preliminary knowledge of how the dataset is organized and presents an idea that machine learning-driven detection processes are required in order to detect and address fraud in the contemporary digital advertisement platforms.

B. Click Interval Distribution Behavior Analysis of temporality

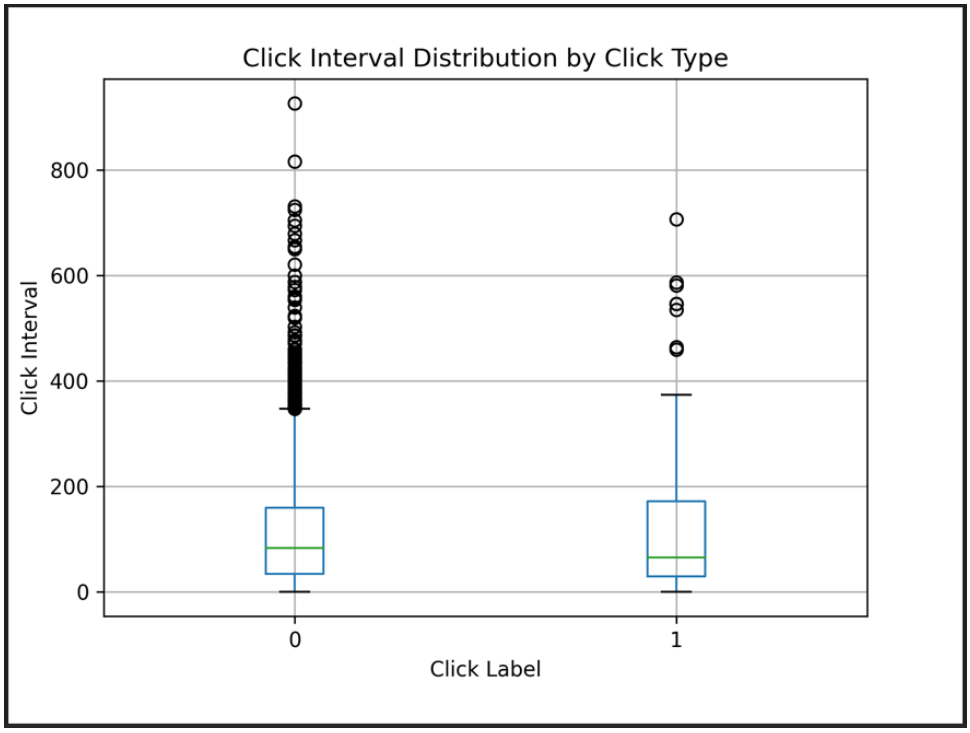


Figure 2. This image shows the difference in click intervals in the event of a valid and a fake advertisement contact.

The graph shown in figure 2 gives a comparison of the distribution of the click intervals between legitimate and fraudulent ad interactions on a box plot. The visualization shows that there are apparent temporal variations in the normal user behavior and suspicious clicking patterns. The legitimate clicks (label 0) have more dispersion of the intervals of clicks, a bigger median, and the presence of many extreme

values, which are characteristic of the inherent diversity of human browsing patterns within a session. Conversely, the median intervals of the clicks of fraudulent clicks (label 1) are relatively smaller, as well as the interquartile range is also smaller, which implies a greater degree of regularity and automation. Such distribution is usually linked to bot-driven or scripted activity, where clicks are produced at a scheduled or repetitive time delay as opposed to being naturally generated [37]. The extreme outliers in both classes indicate that though there is a certain amount of automated behavior resembling human timing, the fraudulent contacts are likely to be concentrated around a range of intervals. This time consistency is a resilient behavioral predictor of non-human action in the digital advertisement systems. In the machine learning sense the distinction between the two distributions shows the predictive power of click interval features in a classification task of fraudulent traffic. Their ability to learn complex deviations of normal behavior that otherwise cannot be demonstrated by simple rules can provide models that are trained on such temporal properties. Within the larger framework of protecting U.S. digital advertising ecosystems, this number underscores the role of time-based behavioral analysis of finding fraud concealed in large bodies of legitimate traffic. In general, the chart validates the fact that click interval analysis is an essential part of machine learning-based ad fraud detection and a significant factor that helps in curbing automated and orchestrated manipulation efforts.

C. Session Behavior Analysis: Connection of Session Duration and Click Volume

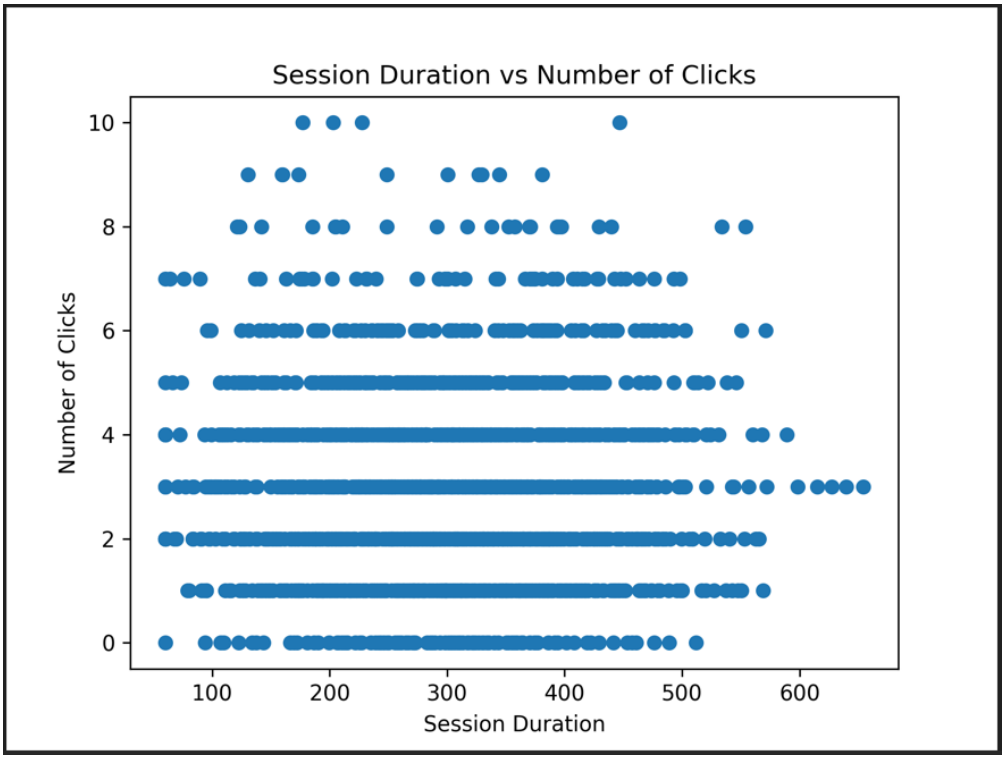


Figure 3. This image demonstrates the correlation between the length of the session and the amount of ad clicks.

Figure 3 explains the correlation between the length of the session and the clicks produced during each advertising session. The scatter plot will provide the result of patterns of behavior that can be used to distinguish normal user interactions and those that might be fraudulent. The legitimate user sessions will usually portray a proportional relationship between the session time and the number of clicks, with longer browsing sessions having a tendency of producing a medium number of clicks over time. This depicts normal interaction behavior since human users communicate with ads on the

digital content infrequently as they go through them. Conversely, clusters of sessions with fairly high numbers of clicks within a short or mediocre length of session are also emphasized in the visualization [39]. These trends are typical of scripted or robotized action, where the rate of exchanges is produced without any commensurate growth in the amount of time of real activity. The existence of several sessions with more than average number of clicks, in spite of the length of the session, indicates the evidence of non-human traffic trying to boost the engagement measures. The machine learning viewpoint of this relationship gives rich behavioral attributes to classification models because unusual combinations of session time and click frequency can be utilized to detect suspect activity [40]. The data points that occur everywhere in the plot also help to show that the digital advertisement interactions are not as stable, and that is why adaptive models can be needed to reflect non-linear relationships. When compared with the need to ensure that U.S. digital advertising ecosystems are secured, this value supports the significance of behavioral analysis at the session level to identify the cases of fraudulent traffic that otherwise go unnoticed within the context of the massive amount of legitimate interactions [41]. The chart proves that the duration of the session and the number of clicks are essential metrics that help detect the abnormal use of a system and optimize the functionality of machine learning-based ad fraud detection.

D. Fraudulent Advertising Activity Geographic Analysis

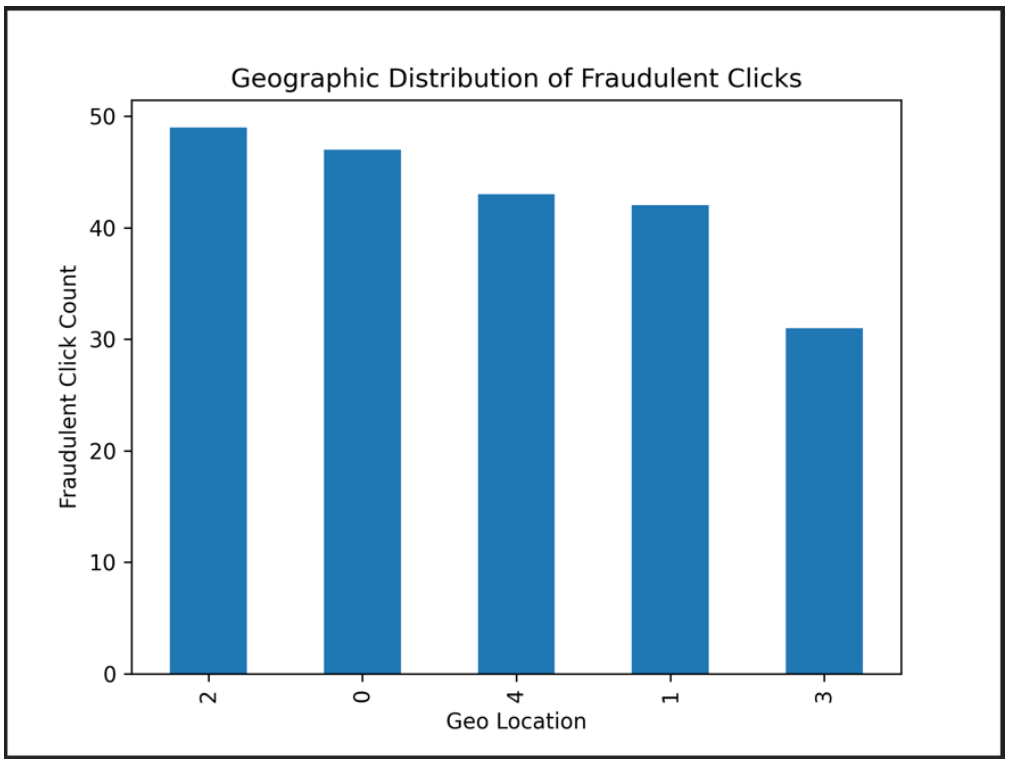


Figure 4. This image demonstrates the geographic distribution of fraudulent advertisement clicks.

Figure 4 shows the geographic distribution of fraudulent ad clicks found in the dataset, which also shows the difference in the degree of the fraudulent activity in different regions. It has been established that the number of fraudulent clicks is not equally distributed across the board but rather has significant concentration in particular geographical areas as can be seen in the bar chart. Some of the areas have more fraudulent interactions, implying that there are organized or automated traffic sources that have geographical locations of operations. Such imbalance is particularly important when discussing the issue of digital advertisement security since it shows how geographic

distributions can be used as valuable markers of manipulation danger when compared to behavioral data. Although the available geographic data is not going to determine intent or prove the attribution to the particular actors, the observed prevalence of fraudulent clicks indicates that there is an unusual traffic movement that does not follow the anticipated trends of organic user interactions [42]. These trends can be due to centrally deployed bot infrastructure, click farms, or script driven activity based on geographically constrained locations. Geographic indicators together with temporal and session-level indicators enhance the performance of machine learning models to detect suspicious activity and ensure that high-risk traffic is given a priority to investigate further. In the context of machine learning, the graph justifies the need to include geo-location as a predictive feature in concepts of fraud detection [43]. The difference in the number of fraudulent clicks paid in different regions allows models to deduce spatial relationships that otherwise would have been ignored by systems based on rules. Within the wider setting of achieving the U.S. digital advertising ecosystems security, this analysis highlights the essence of integrating the geographic indicators into the security risk frameworks. Through detecting breaches in regional traffic fraud, advertisement platforms are able to increase their surveillance, better reaction to fraud, and limit the recurrence to a cross-border manipulation efforts. Figure 4 illustrates that geographic analysis is essential to learn and reduce fraudulent behavior in the complicated digital advertising context.

E. FCI Fraud Detection Model Fraud Importance Analysis

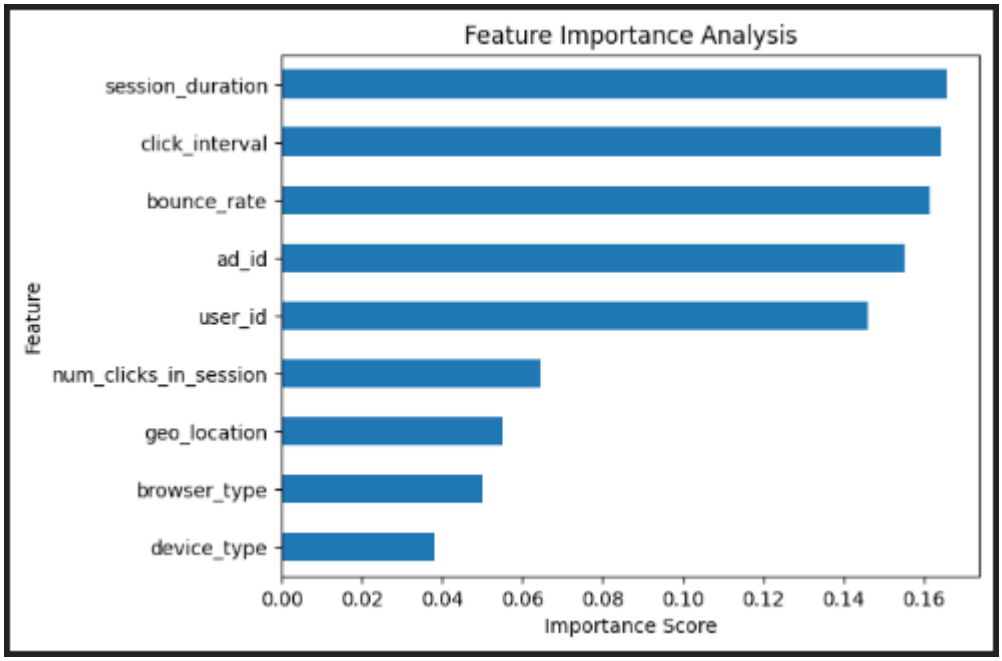


Figure 5. This image depicts ranked scores of feature importance in detecting ad fraud.

Figure 5 shows the results of the feature importance analysis based on the machine learning fraud detection model, which shows the relative value of each input variable to the classification of fraudulent and legitimate ad clicks. The findings also show that both session-level and temporal characteristics are a significant influence in detecting fraudulent activity. Of all the variables, it is possible to state that session duration and the interval between clicks is the most effective predictors, which shows the importance of user engagement timing and patterns of interaction in differentiating between the automated and real user activity. The bounce rate is also reported to have a high value of importance which indicates that it is effective in capturing abnormal engagement properties that are normally associated with fraudulent sessions. Identifiers (ad ID and

user ID) play a moderate role in predictive ability of the model, indicating that appearing to interact with the user with certain advertisements or user accounts multiple times can indicate coordinated or scripted activity. The fact that the number of clicks per session is also another added motivation to behavioral aggregation because abnormally high click rates within a session are usually the sign of the non-human interaction. Conversely, the technical features include geo-location, browser type and device type which have relatively low scores in terms of importance [42]. Although these features may be useful in offering contextual information, its lesser power means that fraud detection is more behaviorally-oriented than technically diverse. Security-wise, the ranking of the features improves the model transparency and interpretability that are required to establish confidence in machine learning-based ads security systems. Knowing the features behind decisions to detect, enables the advertisers and the operators of the platform to confirm that models are behaving in a certain way and mitigate them accordingly [43]. Considering the context of securing the U.S. digital advertising ecosystems, the number proves that machine learning models work well to rely on behavioral indicators rather than superficial features to detect fraud better and more resiliently. Figure 5 does confirm the importance of feature importance analysis in enhancing explain ability, accountability, and operational effectiveness in the context of ad fraud mitigation.

F. Confusion Matrix Performance Analysis

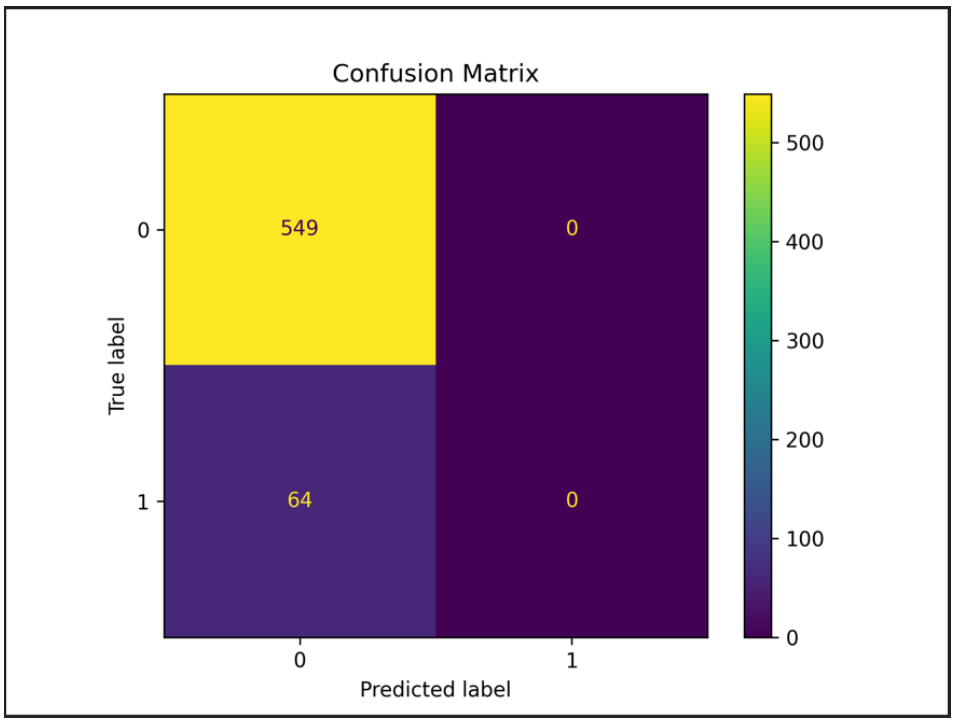


Figure 6. This image demonstrates a confusion table with the results of fraud and genuine clicks.

The confusion mat provided in Figure 6 summarizes the classification performance of the machine learning model used in ad fraud detection. The matrix shows the distribution of the actual and the predicted classes, which gives an understanding of the model in correctly identifying the legitimate and the fraudulent ad clicks. The findings demonstrate that there were a great number of true negatives, the legitimate clicks correctly categorized that prove that the model is effective to identify normal user behavior. The matrix also shows that any cases of fraud are falsely classified as legitimate leading to a very high number of false negatives and none of true positives [44]. This performance underscores a challenge that is usually faced in fraud detection operations

especially when one deals with unbalanced data where genuine interactions prevail. Although the model has good results in eliminating false alarms through eliminating false positives, its failure to detect fraudulent clicks accurately lowers its usefulness in the field of real life security. Underreported frauds may translate into future losses in money, misguided analytics and decreased advertiser confidence. Memory of the class of fraud is a more imperative measure than the general accuracy in that respect [45]. The confusion matrix highlights that better methods of model tuning, optimizing features, or balancing classes should be implemented to increase the sensitivity of the method in detecting fraud. Strategies that can be used to improve false negative and recall would include changing classification thresholds, adding cost-sensitive learning, or using resampling strategies. Within the scope of ensuring the U.S. digital advertising networks, this number highlights the importance of correct identification of the fraudulent actions in order to effectively eliminate them. Figure 6 presents a clear analysis of the work of the model and reveals the aspects of machine learning methods that should be improved to help in overcoming the challenges of ad fraud detection.

G. Fraud Detection through Precision-Recall Analysis

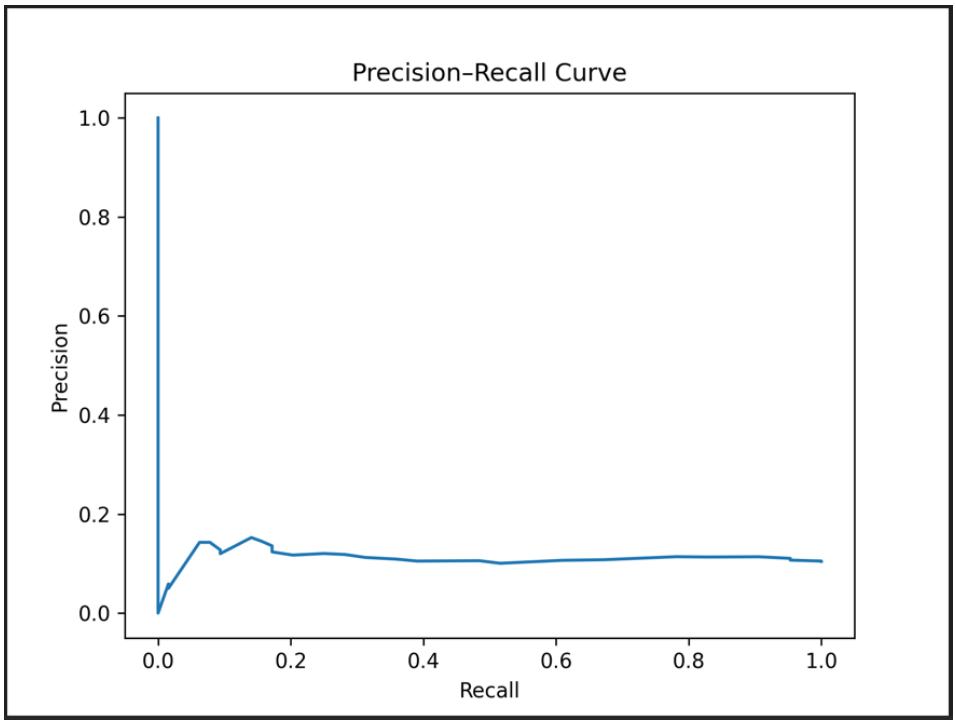


Figure 7. This image shows the accuracy-fraudulent clicks trade-off of the fraudulent clicks detection performance.

Figure 7 shows the precision-recall curve in order to determine the capability of the machine learning model to detect ad clicks that are fraudulent at different classification thresholds. This curve is especially useful in the tasks of fraud detection, where the positive category is fraud, and it is usually underrepresented. The analysis shows that accuracy is comparatively low at the majority of the levels of recalls, meaning that a significant percentage of detected fraud cases can contain false positives. Precision peaks momentarily at extremely low recall values indicating that only a small fraction of the most confident predictions will result in accurate fraud detection. When recall gets larger, the precision becomes smaller and reaches a stable level, and it is difficult to understand that the model is not always able to distinguish between fraudulent and legitimate clicks. This trade-off underscores a very important problem in ensuring the safety of digital advertising ecosystems: the more fraudulent activity is detected the more likely it is that

legitimate interactions will be misclassified. Such false positives may affect the performance of a campaign and the confidence of advertisers in the practical advertising environment. Low recall implies that a significant amount of fraudulent clicks are not detected, and it is possible to continue losing money and being manipulated [45]. As such, it is crucial to weight the precision and recall, to a maximum in order to reduce frauds. The shape of the precision-recall curve indicates, through machine learning lens, that a model further refinement, e.g. enhanced feature engineering or threshold tuning or class-imbalance techniques, is required. When applied in the context of this research, the curve will give a good understanding of the operational constraints to the existing model and will also help to emphasize the significance of recall-focused evaluation in dealing with ad fraud [46]. Figure 7 underlines that precision recall is essential to evaluate the effectiveness in the real-world and provide improvements to machine learning-based advertisement security systems.

H. ROC Curve Analysis and Model Discriminatory Capability

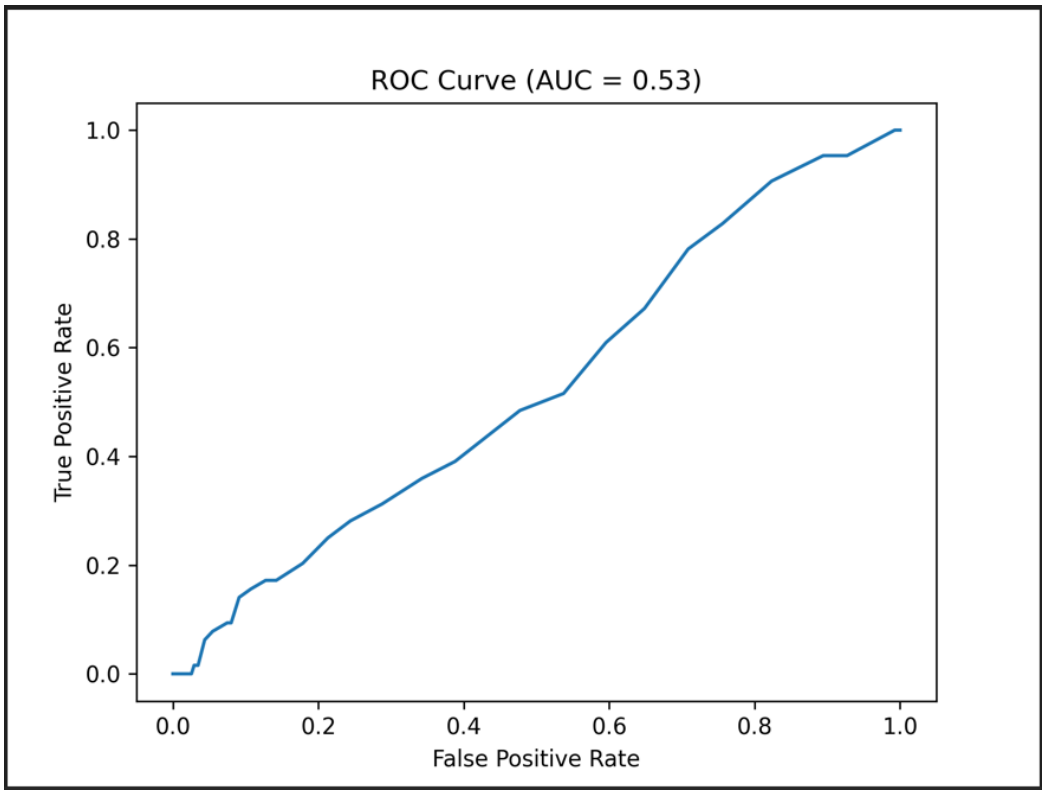


Figure 8. This image represents the ROC curve that assesses the discrimination performance of fraud detection models.

Figure 8 shows the Receiver Operating Characteristic (ROC) curve to determine the overall discriminatory capacity of the machine learning model in determining whether an ad click is legitimate or a fraud. The ROC curve is a plot of the true positive rate versus the false positive rate given a set of value of classification thresholds, which gives a complete picture of how the model models perform without fixing on one decision threshold. A value of 0.53 of Area Under the Curve (AUC) reported indicates that the model is only slightly better than random classification. This implies that it is not very effective when it comes to isolating fraudulent clicks and honest clicks using the current feature set and model configuration. The curve moving to the upper-right shows a trade-off between the correct identification of fraudulent clicks and the incorrect identification of legitimate traffic [47]. The higher the true positive rate the higher the false positive rate which means that an increase in the fraud detection leads to misclassification of the genuine interactions.

Such trade-offs are vital in real-world applications of digital advertising, where false positives are too high can destroy the campaign and weaken adherence to the advertiser, whereas a low detection rate leaves fraudulent operations intact. In terms of methodology, the ROC analysis shows that the model needs to be refined further. Performance may be enhanced with techniques like use of advanced feature engineering, adding new behavioral or contextual cues and optimization of model parameters to enhance discriminatory power [48]. Within the framework of capturing the U.S. digital advertising ecosystems, the number highlights the difficulties that can be encountered in detecting intensive and adaptive fraudulent activity. Figure 8 is a very candid evaluation of the weaknesses of the models, and it shows the significance of constant enhancement in the practice of machine learning in ensuring that the digital advertising infrastructure is not vulnerable to fraud and manipulation.

Discussion and Analysis

A. Fraud Prevalence in Digital Advertising Traffic Interpretation

It turns out that fraudulent clicks occur in a smaller percentage of all advertising interactions than legitimate ones can be obtained as shown in the original analysis of distribution. Although most of the traffic may seem real, the fact that there is a steady amount of fraudulent traffic is not negligible when weighed against the large scale digital advertising ecosystems [48]. A small proportion of fraudulent clicks can lead to huge losses of money, misleading performance reports, and ineffective budgetary spending during campaigns of scale. This unbalance is also representative of the real-life advertising conditions, in which malignant agents intentionally obscure fraudulent conduct in enormous quantities of legitimate user traffic in order to remain undetected [49]. The results highlight the necessity of the detection system of frauds to focus on sensitivity to the events of the minority-class instead of focusing only on the overall accuracy. High accuracy itself is not a good indicator with imbalanced datasets because it can lead to positive results because the models are mostly accurate in legitimate traffic and fail to detect fraud. This finding is consistent with the fact that specific evaluation metrics and detection strategies are required based on security-oriented applications. Security-wise, the fact that fraudulent activity continued to exist despite the fact that the latter is numerically less subordinates the adaptive character of ad fraud techniques [50]. Scammers constantly tighten their belts to enter the legitimate traffic patterns and ensure that they are difficult to detect. The prevalence observed shows the need to have automated, data-driven solutions that can run in continuity and scale. In general, this discussion suggests that the distribution of fraud matters should be considered to come up with effective machine learning models and warrant their implementation in the digital advertising environment of the U.S.

B. Fraudulent activity behavior indicators and temporal trends

When comparing the legitimate and fraudulent ad interactions, behavioral and temporal studies reveal that there are distinct differences in ad interaction [51]. Distributions of click intervals have shown that fraudulent clicks are more often distributed either at regular or abnormally low intervals, indicating they were due to automated or scripted action rather than the behavior of human beings. Legitimate interactions are more variable in terms of timing, as they represent different browsing behaviors and decision-making [52]. These results support the importance of features of time as excellent predictors of abnormal activity. This difference is further enhanced by session-level behavior. The correlation between length of the session and the number of clicks indicates that fraudulent sessions tend to produce disproportionately large numbers of clicks with no corresponding increase in the length of engagement [53]. These are typical of bots or click farms which are meant to artificially increase engagement metrics. Such anomalies are hard to identify by a set of rules since the limits can be easily compromised by advanced attackers. Machine learning models can especially be used to model these

subtle patterns in behavior [54]. Through training on several interacting features at once, models are able to detect small deviations of normal behavior that would otherwise be undetected with rule-based alerts. The findings indicate that behavioral analytics are the core of successful fraud detection and explain the necessity to introduce the time-based and session-based signals in the advertising security models.

C. Geographic Signals and Cross-Border Manipulation Signals

Geographic analysis has indicated that fraudulent clicks are not distributed evenly across all the regions, with some regions making a disproportionate contribution to suspicious activity. Although the intent and attribution cannot be proved solely by the geographic evidence, such patterns of concentration give important contextual clues when it is complemented with the behavioral evidence. Being abnormally geographically clustered in digital advertising ecosystems usually implies centralized infrastructure, e.g. bot networks or structured click activities [58]. The international character of the advertising service makes the combating of fraud more difficult, because honest international traffic should be separated and the dangerous cross-border activity. According to the findings, geographic features have a significant role to play in risk assessment as long as they are utilized as a component of a larger analytical model. Location-based signals are risk amplifiers that instead of providing conclusive evidence, they inform additional investigations and prioritization [59]. This policy and security analysis contenders in favor of a risk-based method to identify manipulation. Through the combination of geographic patterns and behavioral data advertising platforms will be able to promote situational awareness without unjust penalty of legitimate global audiences. The results highlight the significance of contextual analytics when it comes to the threat of foreign manipulation in the context of digital advertising ecosystems in the U.S.

D. Importance of the features and Interpretability of the model

The feature importance analysis offers insightful information into the way the machine learning version of fraud detection arrives at its decisions [60]. The most significant features are session time, time between clicks, and bouncing rate, which proves that behavioral dynamics are more predictive of fraud than the technical features that are not moving. The given finding supports the primary importance of user behavior analysis in either detecting automated or malicious interactions. User and advertisement identifier ratings of moderate importance indicate that recurring patterns of particular entities could be an indication of coordinated action. Conversely, a less significant value on device type and browser type shows that the current fraud schemes can readily spoof or turnabout technical identifiers, limiting their individual efficacy. One of the paramount conditions of implementing machine learning in areas that are sensitive to security is interpretability [61]. Knowing what features influence model decisions will boost trust, ease validation and make compliance with transparency requirements easy. The findings prove that explainable machine learning methods can be used to present actionable information and retain high detection rates. This balance is a key to the real-world implementation of digital advertising security systems.

E. Model Performance and Detection Limitations Evaluation

Evaluation metrics used in the models demonstrate the advantages and weaknesses of the approach adopted. According to the confusion matrix, the performance achieved in terms of the recognition of legitimate traffic is high whereas the ability to identify the fraudulent clicks and thus recognizing them correctly is challenging as the data shows that many false negative results have been achieved [51]. This is the result of the nature of the problem of detecting fraud, in which the bad intentions are specifically designed in a way that they appear to be normal activity. These issues are also highlighted in precision recall and ROC analyses. The poor recall of the class of fraud suggests that a significant number of the fraudulent interactions go unnoticed whereas a moderate precision shows there are false alarms [52]. These findings show that default model configurations might not be

adequate in high stakes security applications [53]. The results have brought out the value of model tuning, threshold optimization, and methods of class imbalance management [54]. Furthering the recall in detecting fraud is especially of primary concern where unnoticed fraudulent activity may result in further exploitation. This discussion highlights the necessity of progressive improvement and regular evaluation of the machine learning models used in the context of advertising.

F. Implications to U.S. Digital Advertising Ecosystems Security

The general conclusions indicate that machine learning has a great perspective of improving on security in U.S. digital advertising ecosystems, but it cannot work alone. Fraud detection forms robust bases of behavioral and time-based analytics, whereas geographic indicators allow general risk assessment [55]. The shortcomings of the models in terms of performance outline the necessity of the complementary solutions, such as enhanced data quality, adaptive learning, and human supervision [56]. Operationally, machine learning will be able to support scalable and real-time detection, which is better than the usual rule-based systems. Meanwhile, to preserve the level of trust and effectiveness, transparency, interpretability, and continuous evaluation are needed [57]. The findings indicate that machine learning must be incorporated into multi-layered security systems as opposed to being applied in solitude. Finally, the current study provides a better insight into the opportunities of using machine learning to reduce the risks of ad fraud and manipulation [58]. The findings can be used to support the creation of more resilient, adaptive, and trustworthy digital advertising ecosystems in the United States by considering not only the technical performance but also the contextual considerations.

Future Work

Although this paper indicates the relevance of machine learning as a tool in ad fraud detection and estimating the risk of manipulation in the digital advertising landscape in the United States, a number of directions are still available to future investigation. Another significant direction is the increase of the size and variety of the datasets in order to make them closer to the actual advertising conditions [59]. Multi-platform data that has been gathered over more time, as well as in larger sets, may assist in capturing both changing tactics used by fraudsters, seasonality, and other long-term behavioral changes, making the models more generalizable and resistant. Further studies on improving detection accuracy through the implementation of state-of-the-art machine learning methods, including deep learning and graph-based classifiers, can also be conducted in the future [60]. Graph analytics may be of use especially in detection of coordinated rings of fraudsters through the modeling of relationships between users, devices, advertisements, and geographic locations. Also, sequential and time-series models would be useful to enhance the identification of multifaceted time-based patterns related to automated or scripted activity [61]. The other promising field is the resolution of class imbalance and recall limitations that are witnessed in the study. To increase the sensitivity in fraud detection and minimize false negatives, techniques like the cost-sensitive learning, adaptive thresholding, and the hybrid ensemble techniques may be explored [62]. The use of explainable artificial intelligence (XAI) techniques would also promote transparency, as the stakeholders would understand and believe the decisions made by the model more. On security and policy grounds, future studies will be able to incorporate external sources of threat intelligence, e.g. known bot signatures or publisher reputation scores, to enhance risk evaluation. Additionally, creating frameworks of real-time deployment would enable machine learning models to run in real time within the advertising system to prevent, in advance, cases of fraud [63]. Lastly, future research may look at regulatory and ethical roles of automated fraud detection especially concerning fairness, privacy, and cross-border data authorization. These technical and contextual issues can be overcome to help

future studies enhance the creation of more robust, scalable, and reliable digital advertising security systems.

4. Conclusion

This study investigated how machine learning can be used to protect the U.S. digital ad ecosystems against ad fraud and possible manipulation of the system using user behavior and a data stream of ad clicks. Due to the rise of digital advertising based on automated and programmatic solutions, the integrity of advertising interactions has suffered as a result of fraud and manipulators. The results of this paper show that machine learning offers a scalable and data-driven solution to detecting abnormal behavioral trends that can be found in vast amounts of legit traffic of ads. Behavioral and time-based analyses indicated that there were distinct differences between lawful and fraudulent interactions especially in click time, time of session and engagement. These characteristics were also found to be key pointers of automated or scripted action, further supporting the significance of behavioral-based analytics in fraud detection in adverts. The geographic analysis also pointed to the way in which spatial patterns may be utilized to aid the risk assessment process by delineating areas in which the rates of fraudulent behavior are disproportionately high though these indicators should not be directly attributed. The machine learning model used in the current study had the capacity of capturing non-linear relationships among the behavioral features, which are complex in nature. The discussion of the feature importance analysis used session-level and time variables as predominant predictors, which increased the interpretability of the model and transparency in applications devoted to security. The drawbacks of performance assessment also became apparent especially in fraudulent clicks of high recall. The evaluation of precision-recall and ROC demonstrated the difficulties related to the lack of balance between classes and the dynamic quality of fraud methods, which means that further development should be offered to the models. The study, despite these constraints, affirms the fact that machine learning has massive benefits over traditional rule-based methods of detection as they provide adaptable and scalable and persistent detection of fraud. Machine learning cannot exist as a separate solution, but must be incorporated with multi-layered security systems which involve behavioral analytics, contextual indicators and human supervision. This study is an addition to the existing literature on the security of digital advertising, as it illustrates the practical implementation of machine learning to detect fraud and determine the presence of manipulation risk. The acquired knowledge will help to create a more resilient, transparent, and trustful digital advertising ecosystem in the United States, as well as may serve as the basis of future research conducted to address the upcoming threats and enhance the effectiveness of detection.

REFERENCES

[1] M. H. Sağlam and I. Kirçova, "The Role of Artificial Intelligence in Ad Fraud Detection in the Blockchain and Programmatic Advertising Ecosystem," in *Avoiding Ad Fraud and Supporting Brand Safety: Programmatic Advertising Solutions*, Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 43–82.

[2] A. Khan, S. A. Sarna, and M. A. K. Azad, "Personalization and Consumer Privacy: Balancing Targeted Marketing with Trust," *Journal of Business and Management Studies*, vol. 2, no. 1, pp. 68–86, 2020.

[3] B. Subburayan, D. Winster, K. Dhanalakshmi, and R. Rajkumar, "Combating Evolving Threats: A Systematic Review of Online Ad Fraud Detection," SSRN, 2025.

[4] O. Orogun, L. Ogungbe, N. Adegboye, T. Adetuyi, and S. Alabi, "Strategies for Combating Synthetic Identity Fraud: The Role of Machine Learning and Behavioral Analysis in Enhancing Financial Ecosystem Security."

[5] M. S. Islam, M. Shokran, and J. Ferdousi, "AI-Powered Business Analytics in Marketing: Unlock Consumer Insights for Competitive Growth in the US Market," *Journal of Computer Science and Technology Studies*, vol. 6, no. 1, pp. 293–313, 2024.

[6] R. M. Potluri, A. K. Jumasseitova, and L. S. Potluri, "The Role of Artificial Intelligence (AI) in Combating Digital Marketing Fraud and Bot Attacks," in *AI-Enabled Threat Intelligence and Cyber Risk Assessment*, Boca Raton, FL, USA: CRC Press, 2025, pp. 17–28.
[7] B. Singh, "Sidestepping Ad Fraud Through Interfaces of Artificial Intelligence Machine Learning," in *Avoiding Ad Fraud and Supporting Brand Safety: Programmatic Advertising Solutions*, Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 329–352.
[8] R. Sharma, K. Mehta, and P. Sharma, "Role of Artificial Intelligence and Machine Learning in Fraud Detection and Prevention," in *Risks and Challenges of AI-Driven Finance: Bias, Ethics, and Security*, Hershey, PA, USA: IGI Global, 2024, pp. 90–120.
[9] V. Dsouza, "Leveraging AI to Enhance Customer Trust in the Digital Ecosystem," 2024.
[10] R. A. Alzahrani, M. Aljabri, and R. M. A. Mohammad, "Ad Click Fraud Detection Using Machine Learning and Deep Learning Algorithms," *IEEE Access*, 2025.
[11] A. Majumder, "Rise and Impact of AI Agents in the Digital Landscape," *American Journal of Intelligent Systems*, vol. 14, no. 1, pp. 10–17, 2025.
[12] A. K. Kumar, V. K. Chidipothu, and M. Leelavathi, "Artificial Intelligence in Digital Currency Security: Transforming Global Marketing in the Blockchain Era," *Cuestiones de Fisioterapia*, vol. 54, no. 3, pp. 1907–1928, 2025.
[13] B. Singh, P. K. Dutta, and C. Kaunert, "Deep Diving into Financial Frauds via Ad Click, Credit Card Management and Document Dispensation in E-Commerce Transactions," in *Generative Artificial Intelligence in Finance*, 2025, pp. 99–123.
[14] S. V. J. Kolupuri *et al.*, "Scams and Frauds in the Digital Age: ML-Based Detection and Prevention Strategies," in *Proc. 26th Int. Conf. Distributed Computing and Networking (ICDCN)*, 2025, pp. 340–345.
[15] P. Kumar, "AI-Powered Fraud Prevention in Digital Payment Ecosystems: Leveraging Machine Learning for Real-Time Anomaly Detection and Risk Mitigation," 2024.
[16] D. A. Oduro *et al.*, "AI-Powered Fraud Detection in Digital Banking: Enhancing Security Through Machine Learning," 2025.
[17] A. Mutemi and F. Bacao, "E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review," *Big Data Mining and Analytics*, vol. 7, no. 2, pp. 419–444, 2024.
[18] O. A. Bello and K. Olufemi, "Artificial Intelligence in Fraud Prevention: Exploring Techniques, Applications, Challenges and Opportunities," *Computer Science & IT Research Journal*, vol. 5, no. 6, pp. 1505–1520, 2024.
[19] A. Singhal, "Navigating Ad Fraud in the Age of AI: Techniques for Detection and Prevention in Programmatic Advertising."
[20] D. B. Sholademi, "Leveraging AI for Detecting Deep Fakes and Combating Financial Fraudulent Identity Schemes."
[21] E. Papadogiannakis *et al.*, "Welcome to the Dark Side: Analyzing the Revenue Flows of Fraud in the Online Ad Ecosystem," in *Proc. ACM Web Conf.*, 2025, pp. 1522–1535.
[22] K. A. Y. R. Oshadi Karunanayaka *et al.*, "Artificial Intelligence in Digital Marketing: The Ethical Implications of Digital Influence on Markets and Consumer," in *Market Grooming: The Dark Side of AI Marketing*, Bingley, UK: Emerald Publishing, 2024, pp. 173–197.
[23] E. Kavoliūnaitė-Ragauskienė, "Artificial Intelligence in Manipulation: The Significance and Strategies for Prevention," *Baltic Journal of Law & Politics*, vol. 17, no. 2, pp. 116–141, 2024.
[24] E. O. Udeh *et al.*, "The Role of Big Data in Detecting and Preventing Financial Fraud in Digital Transactions," *World Journal of Advanced Research and Reviews*, vol. 22, no. 2, pp. 1746–1760, 2024.
[25] A. T. Olutimehin, "The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Cryptocurrency Platforms," 2025.
[26] R. Rajkumar, "Combating Evolving Threats," in *Avoiding Ad Fraud and Supporting Brand Safety: Programmatic Advertising Solutions*, 2025, p. 113.
[27] W. C. Aaron *et al.*, "Machine Learning Techniques for Enhancing Security in Financial Technology Systems," *International Journal of Science and Research Archive*, vol. 13, no. 1, pp. 2805–2822, 2024.
[28] M. Tyagi, P. Srivastava, and K. Khanna, "The Ethics of Ad Fraud: A Corporate Responsibility Perspective," in *Avoiding Ad Fraud and Supporting Brand Safety*, 2025, pp. 27–42.

[29] M. Z. H. George *et al.*, "Machine Learning for Fraud Detection in Digital Banking: A Systematic Literature Review," *arXiv preprint*, 2025.
[30] M. Volkivskyi *et al.*, "The Impact of Machine Learning on the Proliferation of State-Sponsored Propaganda," *ESP-IJACT*, vol. 2, no. 2, pp. 17–24, 2024.
[31] S. I. U. Mansoor, "Legal Implications of Deepfake Technology: In the Context of Manipulation, Privacy, and Identity Theft," *Central University of Kashmir Law Review*, vol. 4, pp. 65–92, 2024.
[32] F. Romero-Moreno, "Deepfake Fraud Detection: Safeguarding Trust in Generative AI," SSRN, 2024.
[33] A. Pokrovskaya, "The Role of AI in Protecting Intellectual Property Rights on E-Commerce Marketplaces," *Russian Law Journal*, vol. 12, no. 1, pp. 303–316, 2024.
[34] F. Rahman and A. Dubey, "Reinforcement Learning-Based Dynamic Brand Defense Techniques in Ad Networks," in *Proc. 2025 Int. Conf. Intelligent Control, Computing and Communications (IC3)*, IEEE, 2025, pp. 1074–1080.
[35] A. J. Hailey, "Digital Deception: How Artificial Intelligence Poses a Threat to the United States' Domestic Elections," Doctoral dissertation, 2025.
[36] R. Tanwar and M. Mahapatra, "Decoding Digital Deception: Exploring Motivations in Online Gaming Bullying, Cyber Frauds and Deep Fake AI," *International Journal of Interdisciplinary Approaches in Psychology*, vol. 2, no. 5, pp. 1847–1856, 2024.
[37] O. Angela, I. Atoyebi, A. Soyele, and E. Ogunwobi, "Enhancing Fraud Detection and Prevention in FinTech: Big Data and Machine Learning Approaches," *World Journal of Advanced Research and Reviews*, vol. 24, no. 2, pp. 2301–2319, 2024.
[38] P. Jeyachandran, "Leveraging Machine Learning for Real-Time Fraud Detection in Digital Payments," SSRN, 2024.
[39] O. Martins and B. Fonkem, "Leveraging Big Data Analytics to Combat Emerging Financial Fraud Schemes in the USA," *World Journal of Advanced Research and Reviews*, vol. 24, pp. 17–43, 2024.
[40] R. Simon, L. Ahuja, P. Chauhan, and U. Munshani, "Beyond the Surface: Deep Dive into Fraud Detection Technologies and Strategies for Robust Application Security," *Global Journal of Enterprise Information System*, vol. 16, no. 2, pp. 24–31, 2024.
[41] R. Mungai, "Synthetic Identity Fraud: A Critical Primary National Security Priority," Authorea Preprints, 2024.
[42] M. Yussuf, "Advanced Cyber Risk Containment in Algorithmic Trading: Securing Automated Investment Strategies from Malicious Data Manipulation," *International Research Journal of Modern Engineering and Technology Science*, vol. 7, no. 3, p. 883, 2025.
[43] A. S. Ayorinde, "Explainable Deep Learning Models for Detecting Sophisticated Cyber-Enabled Financial Fraud Across Multi-Layered FinTech Infrastructure," *International Journal of Cybersecurity and Digital Forensics*, vol. 5, no. 3, pp. 241–263, 2025.
[44] A. Majumder, "Intelligent AI Agents for Fraud and Abuse Detection: Leveraging Machine Learning, NLP, and Behavioural Analytics for Enhanced Security," 2025.
[45] M. Pietri, M. Mamei, and M. Colajanni, "Telecom Spam and Scams in the 5G and Artificial Intelligence Era," *International Journal of Information Security*, vol. 24, no. 3, p. 139, 2025.
[46] S. Terumalasetti, "Artificial Intelligence-Based Approach to Detect Malicious Users Using Deep Learning and Optimization Techniques," *Multimedia Tools and Applications*, vol. 84, no. 8, pp. 3979–4001, 2025.
[47] Y. S. Balcıoğlu, "Revolutionizing Risk Management: AI and ML Innovations in Financial Stability and Fraud Detection," in *Navigating the Future of Finance in the Age of AI*, Hershey, PA, USA: IGI Global, 2024, pp. 109–138.
[48] Z. A. Abbas, Z. M. Hilal, and H. G. Jabbar, "Click Fraud Detection in Online Advertising: A Comparative Study of Machine Learning Models," *International Journal of Safety & Security Engineering*, vol. 15, no. 3, 2025.
[49] O. Iguodala and A. Oyiborhoro, "AI-Powered Anti-Money Laundering (AML) and Fraud Detection," *World Journal of Advanced Research and Reviews*, vol. 26, pp. 3702–3714, 2025.
[50] L. A. Garcia-Segura, "The Role of Artificial Intelligence in Preventing Corporate Crime," *Journal of Economic Criminology*, vol. 5, p. 100091, 2024.
[51] S. Iseal and M. Halli, "AI-Powered Fraud Detection in Digital Payment Systems: Leveraging Machine Learning for Real-Time Risk Assessment," 2025.

[52] S. Iseal and M. Halli, "AI-Powered Fraud Detection in Digital Payment Systems: Leveraging Machine Learning for Real-Time Risk Assessment," 2025.

[53] X. Tang and H. Yu, "Towards Trustworthy AI-Empowered Real-Time Bidding for Online Advertisement Auctioning," *ACM Computing Surveys*, vol. 57, no. 6, pp. 1–36, 2025.

[54] M. E. Lokanan and V. Maddhesia, "Supply Chain Fraud Prediction with Machine Learning and Artificial Intelligence," *International Journal of Production Research*, vol. 63, no. 1, pp. 286–313, 2025.

[55] A. K. Al Hwaitat *et al.*, "Overview of Mobile Attack Detection and Prevention Techniques Using Machine Learning," *International Journal of Interactive Mobile Technologies*, vol. 18, no. 10, 2024.

[56] P. Kumar, D. Y. Gowda, and A. M. Prakash, "Machine Learning in Cybersecurity: A Comprehensive Survey," in *Pioneering Smart Healthcare 5.0 with IoT, Federated Learning, and Cloud Security*, 2024, pp. 175–197.

[57] H. Okoro, "Corporate Data Mining and Manipulation in Marketing," in *Impacts of Leakage, Whistleblowing, and the Rise of Propaganda*, Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 231–260.

[58] Y. Rohita *et al.*, "Enhanced Fake Account Detection on Social Media Platforms Using Gradient Boosting Algorithm," in *Proc. Int. Conf. Soft Computing and Signal Processing*, Singapore: Springer Nature, 2024, pp. 151–164.

[59] N. Rahul, "Improving Policy Integrity with AI: Detecting Fraud in Policy Issuance and Claims," *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, vol. 5, no. 1, pp. 117–129, 2024.

[60] A. J. Nair, S. Manohar, and R. Chaudhry, "Securing the Metaverse: Exploring the Role of Artificial Intelligence in Mitigating Emerging Threats," in *Augmenting Retail Reality, Part B: Blockchain, AR, VR, and AI*, Bingley, UK: Emerald Publishing, 2024, pp. 67–84.

[61] H. Ijaiya and O. O. Odumuwagun, "Advancing Artificial Intelligence and Safeguarding Data Privacy," *International Journal of Research Publication and Reviews*, vol. 5, pp. 3357–3375, 2024.

[62] A. Kotagiri and T. R. Bammidi, "Sustainable Safeguarding: Implementing Fraud Defense Systems for Authorized Push Payments," in *Proc. Int. Conf. Sustainable Development through Machine Learning, AI and IoT*, Cham, Switzerland: Springer Nature, 2024, pp. 130–140.

[63] B. Dileep *et al.*, "Fostering a Robust Financial Ecosystem With AI and ML," in *Artificial Intelligence for Financial Risk Management and Analysis*, Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 405–430.

[64] A. I. B. Ramli, "Big Data and Artificial Intelligence to Develop Advanced Fraud Detection Systems for the Financial Sector," *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, vol. 8, no. 12, pp. 31–44, 2024.

[65] M. M. Uddin, T. S. Hussain, and T. Rahanuma, "Developing AI-Powered Credit Scoring Models Leveraging Alternative Data," *International Journal of Informatics and Data Science Research*, vol. 2, no. 10, pp. 58–86, 2025.

[66] S. Baranidharan, D. Winster, K. Dhanalakshmi, and R. Rajkumar, "Combating Evolving Threats: A Systematic Review of Online Ad Fraud Detection," in *Avoiding Ad Fraud and Supporting Brand Safety: Programmatic Advertising Solutions*, 2025, pp. 113–144.

[67] "Fraud Detection Dataset," Kaggle. Available: https://www.kaggle.com/datasets/programmer3/fraud-detection-dataset