Journal of Cybersecurity and Privacy

Article

Ads and Fraud: A Comprehensive Survey of Fraud in Online Advertising

Shadi Sadeghpour and Natalija Vlajic *

Engineering and Computer Science, York University, Toronto, ON M3J 1P3, Canada; shadisa@cse.yorku.ca
* Correspondence: vlajic@cse.yorku.ca

Abstract: Over the last two decades, we have witnessed a fundamental transformation of the advertising industry, which has been steadily moving away from the traditional advertising mediums, such as television or direct marketing, towards digital-centric and internet-based platforms. Unfortunately, due to its large-scale adoption and significant revenue potential, digital advertising has become a very attractive and frequent target for numerous cybercriminal groups. The goal of this study is to provide a consolidated view of different categories of threats in the online advertising ecosystems. We begin by introducing the main elements of an online ad platform and its different architecture and revenue models. We then review different categories of ad fraud and present a taxonomy of known attacks on an online advertising system. Finally, we provide a comprehensive overview of methods and techniques for the detection and prevention of fraudulent practices within those system—both from the scientific as well as the industry perspective. The main novelty of our work lies in the development of an innovative taxonomy of different types of digital advertising fraud based on their actual executors and victims. We have placed different advertising fraud scenarios into real-world context and provided illustrative examples thereby offering an important practical perspective that is very much missing in the current literature.

Keywords: digital advertising fraud; web-bots; ad fraud detection

check for updates

Citation: Sadeghpour, S.; Vlajic, N. Ads and Fraud: A Comprehensive Survey of Fraud in Online Advertising. *J. Cybersecur. Priv.* **2021**, *1*, 804–832. https://doi.org/10.3390/jcp1040039

Academic Editors: Mario Antunes and Carlos Rabadão

Received: 5 November 2021
Accepted: 10 December 2021
Published: 16 December 2021

1. Introduction

Advertising has a long history that goes back to ancient civilizations. It started 4000 years ago in Egypt, Greece, China, and India, where wall or rock paintings were the way advertising was performed. In the 18th century, advertisements appeared in weekly newspapers. Over time, and as a result of innovative technologies, advertising has progressed to reach the radio, TV, and other modern communication mediums. Nevertheless, the birth of the Internet has marked a particularly important point in the history of advertising. Notably, online/digital marketing has allowed advertisers to reach very targeted user groups and display ads in ways that are more helpful, more personalized, and relevant to wider audiences. The first online ad appeared in 1994 when only 30 million people had access to the World Wide Web (WWW) [1]. Since that time, online digital advertising has become the most prominent and most effective form of advertising and an essential income source for many individuals and companies. Unfortunately, over the past two decades, this thriving industry has come under the influence of many problem-causing factors such as bot traffic, data fraud, click fraud, etc. According to [2], online ad fraud is a severe and widespread challenge for the online advertising industry and costs advertisers $8.2 billion each year. TrafficGuard/Juniper [3] reported that the total cost of ad fraud in 2020 was $34 billion, and it is predicted it will increase to $87 billion by 2022.

The primary purpose of this study is to bring awareness to the importance as well as the challenges of combating fraud in the online digital advertising ecosystem. In particular, the main contributions of this work are as follows:

- First, we describe the key elements of an online advertising system/platform, including their roles and interactions. We then systematically review different forms of digital advertising platforms.
- We introduce various schemes of advertisement placement as well as different revenue models in online ad platforms.
- We outline different approaches which cyber criminals are known to deploy in order to abuse online advertising models and conduct fraud. Subsequently, we introduce a new classification of all types of fraud in online adverting. This classification is structured around a set of ad fraud W3H questions: Who does What to Whom and How.
- To date, several cutting-edge solutions have been proposed to address the problem of fraud in online ad platforms. This article provides a thorough overview of the proposed methods and technologies in detecting and preventing fraudulent practices from the scientific as well as the practical perspective.
- Finally, we conclude the article by highlighting some open challenges and future research directions in this field while putting a special emphasis on machine learning techniques for the detection and prevention of fraud in online ad systems.

Most of the previous research literature in this field (including [4,5]) have looked at the problem of advertising fraud in very generic ways, without explicitly identifying or naming the most likely fraud perpetrators and targets. The main novelty of this work is the fact that we focus on the categorization of ad fraud based on the main human actors (executors vs. victims). Furthermore, we provide illustrative real-world examples of different types of advertising fraud, thereby providing an important practical perspective that is very much missing in the current literature. Additionally, and to the best of our knowledge, there are no existing surveys that have identified the most important open challenges and future research directions in this field with a strong emphasis on the application of machine learning.

The remainder of this article is structured as follows. In Sections 2–6, we provide a general overview of the digital advertising ecosystem, while in Sections 7 and 8 we specifically focus on the topic of digital advertising fraud. In particular, in Section 2 we introduce the main elements of an online advertising ecosystem, the critical interactions among these elements, and various technologies involved in the delivery of the right ads to the right people at the right time. In Section 3, we specifically discuss different forms of digital advertising, and in Section 4 we describe two primary types of publisher-advertiser contract. In Section 5, we explain three most common types of revenue models used in digital advertising systems. In Section 6, we cover the concept of user tracking and profiling techniques as pertinent to digital advertising. Finally, in Section 7 we explore different types of fraud in the ad ecosystem, while in Section 8 we present a taxonomy of ad fraud prevention and detection methods. In Section 9, we outline the main conclusions of this study.

2. Online Advertising Ecosystem—Key Components

In this section, we introduce the main elements of an online advertising ecosystem, the critical interactions among these elements, and various technologies involved in delivering the right ads to the right people at the right time.

As shown in Figure 1, an online ad system consists of three key players: publishers, advertisers, and users [1]. The interactions between these players are facilitated by an intermediate infrastructure—the so-called ad platform.

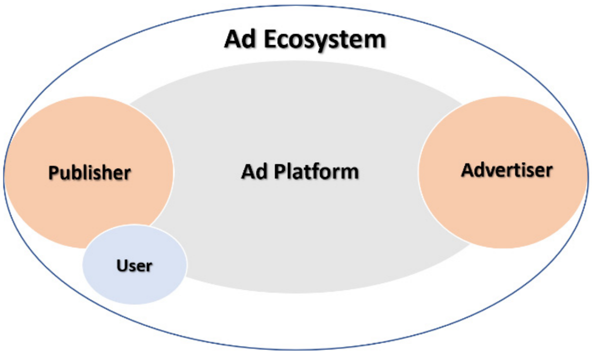


Figure 1. The key components of online digital advertising ecosystem.

Publishers or sellers are the providers of ad system inventory (ad inventory or the amount of ad space in a publisher web page). They are the entities that create (and sometimes manage) the actual online content in a set of web pages [6]. Publishers receive money to put advertisers' content in front of online audiences by integrating advertisers' content into their web pages. Publishers' web pages are considered the users' entry-points into the ad ecosystem.

Advertisers are persons or companies that want to promote a product or a brand by displaying a related ad on third-party (i.e., publishers') websites. Advertisers generally aim to place their ads on popular high-traffic sites.

Users are the power engine of the ad ecosystem, as their requests for pages containing ads are what advertisers are looking for, and their actual views of (or clicks on) ads generate revenue for publishers. Furthermore, the data obtained by monitoring users' actions on a publisher's website will determine the specific location of various advertisements on the pages of this site.

Ad Platform is a framework that connects advertisers to publishers. Alternatively, it is a group of entities that facilitate matching the demand and the supply end of the ad ecosystem [6]. On one side, ad platforms assist publishers in finding the best match between their audiences and the advertisements they are supposed to showcase; on the other side, they help advertisers reach the most appropriate potential audience and customize the advertising material to them. The modern ad platforms are made up of a number of distinctive intermediate entities, including Ad network, Ad Exchange (AX), Supply Side Platforms (SSPs), Demand Side Platforms (DSPs), and Data Exchange. Each of these entities has unique responsibilities and mechanisms of operation; and, when all the entities work synergistically, they make the ad platform processes more effective, flexible, and transparent. The role of different entities comprising the Ad Platform is illustrated in Figure 2 and described below.

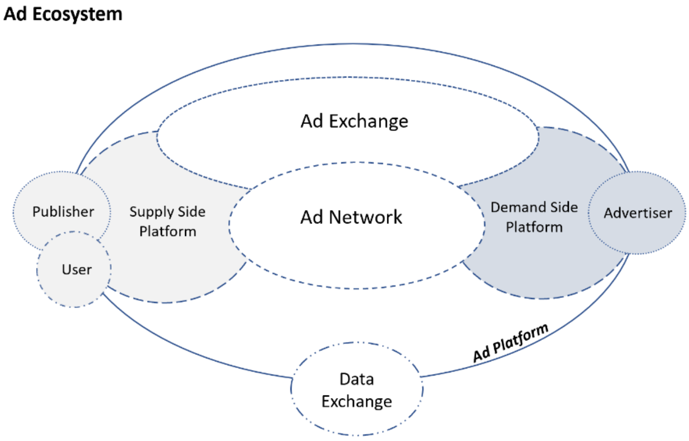


Figure 2. Sub-elements of Ad platform in online advertising ecosystem.

Ad Network emerged in the mid-1990s [7] as one of the first components (i.e., facilitators) of online advertising technology. They came into existence due to the fact that for many advertisers, running direct buys from publishers at high volumes was not sustainable. Hence, ad networks' purpose is to collect inventory from a range of publisher sites, segment it (e.g., based on geolocation, age, gender, interest, behavior of potential customers/users), and sell it to advertisers in advance and 'bulk'. In other words, Ad networks work with publishers to more efficiently sell ad impressions that they have not sold directly to advertisers. They also work with advertisers to develop coordinated and most effective ad campaigns across different sites. Examples of large ad networks include Google AdSense, Media.Net, BuySellAds, and Conversant.

Ad Exchange (AX) is an open marketplace that auctions publishers' ad impressions in real-time among multiple bidding advertisers and sells them to the highest bidder. The whole process may take a millisecond. The key advantages of Ad exchanges (over Ad networks) are that they give advertisers better control, targeting capabilities, and monetary transparency. Namely, they allow advertisers to serve their ads to the right viewer, at the right time, and through the right publisher. Moreover, they enable advertisers to keep track of where their ads are served, and which ad spaces are most cost-effective. However, it should also be noted that many Ad exchanges struggle with the problem of low-quality inventory, as good quality ad spaces are often already purchased by big Ad networks. Examples of large Ad exchanges include Google DoubleClick, OpenX, AppNexus, SmartyAds, and AdECN.

Supply Side Platforms (SSPs) serve publishers by managing and selling their inventories (i.e., available ad space) in multiple ad networks and exchanges [8]. Through strategy optimization, a publisher's SSP will aim to increase the publisher's profit by increasing the advertisers' demand for its ad inventory. Examples of real-world SSPs are Google's DoubleClick for Publishers (DFP), PubMatic, Rubicon Project, BrightRoll, and AppNexus Publisher Suite.

Demand Side Platforms (DSPs) serve as advertisers' agents (i.e., representatives) in multiple ad networks and exchanges, and they are responsible for selecting the right audiences and the most appropriate media to represent the advertisers' ads. Examples of real-world DSPs are Google's DoubleClick Bid Manager (DBM), TubeMogul, Oath DSP, Amazon DSP (AAP), Sizmek, and TradeDesk.

Data Exchange or Data Management Platform (DMP) is a third-party data aggregator that publishers and advertisers interact with to obtain additional user-related information, leading to better advertising. In general, DMPs collect users' data to profile them according to their interests. As such, DMPs can facilitate a publisher or an SSP to find the best match for their ad inventory (based on their audience's interests) among many different DSPs. To generate accurate user profiles, DMPs harvest vast amounts of data from the Internet and deploy advanced data mining tools. Lotame, Salesforce DMP, OnAudience.com, and Snowflake are examples of real-world DMPs.

3. Different Forms of Digital Advertising

Twenty years ago, digital advertising mainly comprised simple, randomly selected banners prominently placed on websites [9]. At present, digital advertising deploys many different and highly targeted types of online activities. The framework that allows modern-day digital advertising to serve customized real-time advertisements to online users is Computational Advertising (CA). In [8], CA is also defined as "a scientific sub-discipline at the intersection of large-scale information retrieval, statistical modelling, machine learning, optimization, text analysis," and even microeconomics. In today's WWW, CA is also seen as an umbrella term for several different advertising strategies, which could be used individually or in combination with each other, including Contextual Advertising, Sponsored Search (Search Advertising), Display Advertising, and Behavioral Advertising.

3.1. Contextual Advertising

A user's visit to a web page typically indicates their implicit interest in the specific topic/content of this page [8]. Consequently, an ad that directly correlates to the content of a web page has much higher chances of being viewed by the visitors of the given page. The type of advertising that capitalizes on this principle—by linking the context of an ad with the content of the page displaying this ad—is known as Contextual Advertising. An example of contextual advertising would be an ad offering a special price on a flight to Australia placed on an Australian airline company's website. Placement of 'contextual ads', which could be text-only or rich-media, can lead to improved user experience as well as increased revenue to the publisher, advertiser, and their respective ad network or exchange [10].

3.2. Search Advertising

In search advertising, also called the sponsored search method, the user issues a query to a search engine, and textual ads relevant to the queried keywords are displayed on the returned hits-page. In general, search engines try to rank the displayed ads not only based on how well the user's search keywords match the keywords provided by the advertisers, but also in a way that would maximize the search engine's revenue.

3.3. Behavioral Advertising

Behavioral advertising [11] targets users based on their behavior rather than the content/context of the pages they are currently visiting. As such, this type of advertising requires that the information about the users' browsing behavior (i.e., history) as well as their likes, wants, interests, and needs be collected over a more extended interval of time. (The practice of collecting user-related information is also known as user tracking.) In general, behavioral advertising has the potential to offer more targeted ads to the users, and by doing so, to also boost the revenues of the involved advertisers and ad networks/exchanges. However, this advertising type also raises serious concerns about user privacy, given its heavy reliance on user tracking.

3.4. Display Advertising

This type of digital advertising deals with the placement of rich media ads/banners, including animations, photographs, flash, audio, and video (as opposed to text-only) on third-party web pages [12]. Display advertising is typically used in combination with contextual or behavioral targeting.

4. Different Types of Publisher-Advertiser Contract in Digital Advertising

Two primary types of publisher-advertiser contract (i.e., ad purchase schemes) that ultimately decide which particular ad will be placed to which particular user and on which particular web page are: manual media buying and programmatic media buying. Each scheme is described in more detail below:

4.1. Manual Media Buying

In the traditional ad system, known as manual media buying, a publisher sells its advertising inventory directly to advertisers. The advertisers deliver their ad code to the publisher with little to no possibility of testing or adjusting their advertising campaigns on the fly. As such, this form of media buying gives the publishers and advertisers the least control over the actual audiences their ads will ultimately reach. It also has very limited scalability as any changes to the campaign have to be performed manually and need to go through the publisher's Ad Ops (online advertising operations) [13].

4.2. Programmatic Media Buying

In contrast to manual media buying, programmatic media buying uses technology to automate the purchasing of ad placements in the digital space [13,14]. In programmatic media buying, technology allows both advertisers and publishers to minimize the need for human intervention, which, as a result, also minimizes the time to set up, run, and optimize media campaigns. Additionally, with this type of media buying, automated targeting, tracking, and reporting of impressions (i.e., views of an ad) can also be easily incorporated. The main variants of programmatic media buying include real-time bidding (RTB), private marketplace (PMP), and programmatic direct.

4.2.1. Real-Time Bidding (RTB)

In the RTB system, buying and selling the ad space occurs via an auction within the time-interval that it takes for a web page to load, which can be only a few milliseconds. All advertisers interested in the auctioned ad space will bid for an impression in an automated manner, and eventually, the highest paying bidder will win the auction and display their ad on the given web page. RTB is the most prevalent ad placement method in online digital advertising.

In the RTB ecosystem, when bidding on an impression for a particular user, advertisers base their decisions/actions on the information about that user's previous browsing behavior. This requires as much information as possible to be gathered about that particular user through various mechanisms such as user tracking and cookie synchronizing. Figure 3 gives an example of how RTB works in combination with behavioral targeting. A user (Bob) visits a website (CNN here), which provides an opportunity for the publisher (CNN) to send an ad offer/auction to the ad exchange (DoubleClick) via its SSP (OpenX). (Note here, the SSP sends the ad request to an ad exchange, not an ad network). Consequently, the ad exchange (DoubleClick) queries multiple DSPs for advertisers' bids. A DSP (in this case, StackAdapt) may contact a data exchange (Oracle BlueKai) for the third-party user data, which will help the DSP's customer/advertiser decide whether to participate in the auction or not. If the advertiser (in this case, Netflix) decides to bid, the bid is generated and submitted. The winning advertiser is first selected by the ad exchange, then the SSP, if the SSP sends the bid request through multiple ad exchanges and receives multiple bid offers. In Figure 3, we assumed Netflix was the highest bidder, so its ad finally got to be displayed to Bob through CNN's website [14]. It is worth stressing that the key benefits of RTB include:

1. RTB has a flexible per-impression buying process which allows brands to bid on single impressions and in real-time, as opposed to the in-advance buying of publishers' inventory and for a predetermined fixed price as is the case in the manual media buying.
2. Advertisers and publishers use a single consolidated dashboard on their DSP or SSP platforms to deal with multiple partners, which results in much more straightforward and easier-to-manage campaigns and facilitates a more effective gathering of impression-level data/statistics.
3. Effective gathering of impression-level data/statistics can generally lead to a more adaptable, and ultimately a more profitable, advertising strategy.
4. RTB gives publishers the ability to sell ad space that was previously unwanted or unsold by making the pricing of this space flexible (i.e., self-adjusting) [13].

4.2.2. Private Marketplace (PMP)

Private Marketplace [15], or PMP for short, is an invite-only variation of the RTB model that operates without any middlemen in the form of ad networks or exchanges. Basically, in PMP, some select number of advertisers are invited to bid for the inventory of a particular publisher. More specifically, a handful of preferential advertisers are given the opportunity to bid against each other for a publisher's inventory before this inventory becomes offered in a public auction. This method is generally used by publishers with premium inventory, such as media sites such as The New York Times and Wall Street Journal. In contrast to the traditional RTB, PMP provides both advertisers and publishers with better transparency about ad placement and pricing.

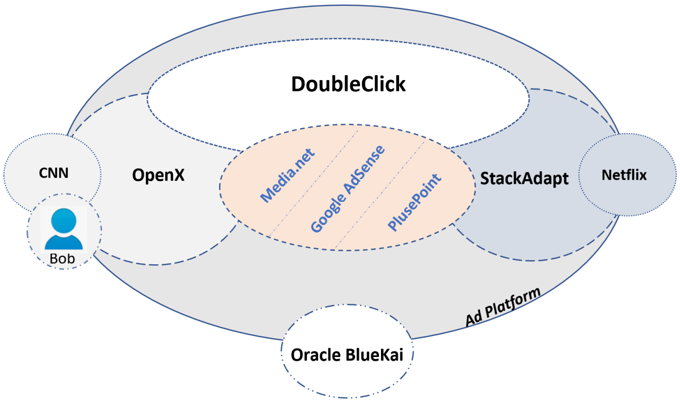


Figure 3. T How RTB works.

4.2.3. Programmatic Direct

Programmatic direct advertising scheme [16] allows advertisers to directly pre-purchase guaranteed ad impressions from premium publishers that attract their most desired audiences. Like the PMP model, it matches select publishers with select advertisers; however, advertisers and publishers agree up-front on specific inventory and based on entirely predetermined 'cost per thousand impressions' (CPM) prices. Additionally, similar to RTB, the programmatic direct scheme can be fully automated, requiring no human intervention to be run. However, unlike RTB, it involves no auction or bidding process as the CPM is predetermined.

5. Revenue Models in Digital Advertising Ecosystem

Advertisers are essentially companies with products to sell, and they invest money into buying online impressions hoping that these impressions will boost their profit. On the other side, publishers commit to displaying the advertisers' ads and, in return, will charge the advertisers a commission fee for the action(s) generated by the user. The amount of commission received by a publisher is called revenue [4].

In general, there are three types of revenue models that are used in digital advertising systems: impression-based (CPM), click-based (CPC) and action-based (CPA).

5.1. Impression-Based Model (CPM)

Impression-based model or cost-per-thousand-impressions (technically, "cost-per-millet" or CPM for short) is the model where the publisher receives revenue each time an advertisement displayed on their website is viewed a certain number of times (typically 1000 times).

5.2. Click-Based Model (CPC)

A paid and displayed ad should ideally result in a click event (e.g., a click on the given ad that redirects the user to the advertiser's website). Cost-per-click (CPC), also called pay-per-click (PPC), is a revenue model in which the advertiser pays a fee to the publisher each time one of their ads is clicked on.

5.3. Action-Based Model (CPA)

Cost-per-action (CPA) is a model in which the publisher receives revenue each time a customer completes a pre-defined business action as a result of the ad displayed on the publisher's website, such as completing an online order or filling an online application form.

The evidence presented in [17] shows that, out of the three above mentioned models, the CPC is the most common revenue model of the online advertising ecosystem. It should also be pointed out that, in addition to CPM, CPC and CPA, three other important metrics of an ad ecosystem are the so-called 'effectiveness' metrics—eCPM, eCPC and eCPA, respectively [1]. In contrast to CPM, CPC, and CPA, which are negotiated at the beginning of a campaign, eCPM, eCPC, and eCPA are three metrics that are calculated post-campaign, regardless of the actual revenue model initially established between the publisher and the advertiser, which in some cases could be a combination of CPM, CPC and CPA. eCPM, eCPC and eCPA are calculated by dividing the revenue obtained from an advertisement by the number of impressions, clicks, and actions recorded on this advertisement, respectively, expressed in units of 1000. As such, these metrics allow the advertiser to see how much revenue has been earned (and can be earned, going forward) when 1000 impressions/clicks/actions are achieved on the given advertisement. Ads with high effectiveness metrics should be preferred and further pursued, while those with low effectiveness metrics should ideally be dropped by the advertiser.

6. User Tracking and Profiling Techniques

Long gone are the days when advertisers would select a form of media to display ads without taking into consideration their actual audience [6]. Nowadays, we live in the era of customized ads, where advertisers are not only required to select specific users for specific ads based on the users' preferences and interests, but they are expected to do so in real-time. As a result of this evolution, the concept of user profiling, i.e., a collection of most significant facts about a given user and his/her interests [18], has emerged. The most common way to collect information about a user (i.e., build a user profile) is by tracking the user's online behavior, including the type and sequence of visited pages, over some time. In the research literature, several studies have looked into user profiling within the context of digital advertising. For example, in [19], the authors have described a targeted advertisement system that performs matching between the user profile and the page profile. The system creates a user profile in a multi-step process by integrating user-related information from multiple sources. Several user profiling approaches, including its related concepts, methods, and techniques, have also been discussed in [20–23]. These techniques comprise data mining and machine learning methods to extrapolate users' information.

The booming of Online Social Networks and IoT technologies have provided new avenues to collect data from users' actions. Technical mechanisms that facilitate online user tracking can be categorized in four major groups [24]: (1) Session-based, (2) Storage-based, (3) Cache-based, and (4) Fingerprinting.

1. Session-Based Tracking: A web session is defined as a sequence of user actions on an individual website within a given time frame. The purpose of session-based tracking is to facilitate the monitoring of user actions across multiple visited websites and/or over a longer interval of time. One common form of session-based tracking, called Session Identifiers Stored in Hidden Fields [25,26], involves passing a single identifier from one website to another through a URL. Another form of session-based tracking, called Explicit Web-Form Authentication [27,28], happens when a user logs in to a website and is asked to register before accessing the resources. In the third form of session-based tracking, window.name document object model (DOM) property [29] can be used to store data and be shared and applied by different visited parties/sites. Basically, the W3C Document Object Model (DOM) [30] is a cross-platform interface to access and interact with the content, structure, and style of web documents. It organizes all the objects in a tree structure, and it is language independent. The window.name property is resistant to page reloads, and it is accessible from other domains as well, which allows third-party content to exchange information with the first-party or with another third-party content [24].
2. Storage-based Tracking. Cookies, also known as HTTP cookies, are the most common method in this category. A cookie is a small piece of data (i.e., identifier) generated by a web server the first time a user visits the website hosted by this server. The identifier is then sent to be stored in the client's memory and retrieved each time the user visits the same website. It should be noted that a single website can incorporate content from multiple servers; thus, two different types of cookies are defined—first party and third-party cookies [31]. The first party cookies are set by first party servers directly associated with the URL of the page that the user has explicitly requested. The third-party cookies are widely used by advertising companies and are received when the browser implicitly fetches the third-party content (such as video ads) from

a third-party server. Cookies can also be classified in terms of their life span into temporary and permanent cookies. Temporary cookies are stored in the browser cache and are expired as soon as the browser gets closed [32]. In contrast, permanent cookies have an expiration date and remain in the browser memory until that particular point in time (i.e., they can survive throughout multiple sessions). (For more information on other less common forms of storage-based tracking techniques, see [25].)

3. Cache-based Tracking. The cache-based tracking mechanisms identify a browser instance and its respective user by deploying various types of caches such as Web cache [24,33], DNS cache [34], and Operational caches [24,35]. Namely, by relying on some distinctive items stored in these caches (e.g., previously acquired images or DNS records), it is possible to determine whether this specific user has already visited a given website or not.
4. Fingerprinting. This approach to user tracking relies on different methods that can facilitate the extraction of unique identifiers associated with a user's device (e.g., IP address, operating system, browser version, system and user languages deployed, etc.) [36–38]. These identifiers can then assist in tracking the user across multiple websites. For example, JavaScript and Flash can distinguish between different versions and architectures of operating systems and are referred to as the Operating System Instance Fingerprinting technique [39,40]. Furthermore, JavaScript can also facilitate the acquiring of information about the user's local time zone and local date in milliseconds.

Over and above all, it should be noted that online tracking for advertising purposes has raised privacy concerns and is the subject of a number of emerging regulatory laws across the world. However, one of the most important pushes aimed at protecting user privacy seem to come from the major technology platforms, namely Google, Apple and Mozilla [41,42]. Apple has started to fight against consumer tracking through the so-called Smart Tracking Prevention ("ITP") feature in the Safari browser (introduced in 2017) [43] to limit user tracking by blocking third-party cookies. Similarly, in 2019, Mozilla [44] has launched an anti-tracking mechanism called Enhanced Tracking Protection to block third-party cookies by default and incorporate features to address browser fingerprinting. Interestingly enough, Google (as one of the biggest names in the digital advertising industry), first, in May 2019, published a set of measures for users to delete third-party cookies without losing their log-in information, and with the intention of making user-fingerprinting much harder for trackers. They then introduced an open-source initiative—the Privacy Sandbox—a new set of web standards to enhance user privacy online and support a vibrant ad-funded web ecosystem [45]. The Privacy Sandbox included a series of browser Application Programming Interfaces (APIs) designed to satisfy advertising use cases without relying on third-party cookies. Concretely, a technology developed from Google's Privacy Sandbox—FLoCs (Federated Learning of Cohorts) [46]—has been developed to facilitate more anonymized advertising by targeting people only based on their membership in larger groups/cohorts of users with similar interests and behavior. Nevertheless, Google recently stated that it would not build alternate tracking identifiers with similar cross-site tracking capabilities after phasing out third-party cookies. Google will make this change in late 2023 [47].

7. Fraud in Ad Ecosystem

Real-time transactions in the open platforms of online digital advertising make these systems vulnerable to various threats and fraud attacks. We explore the different types of ad fraud in the reminder of this section.

7.1. Categories of Ad Fraud

Zhu et al. [1] classify ad fraud into three major categories, namely: (a) placement fraud, (b) traffic fraud, and (c) action fraud (refer to Table 1 for further classification details). We review each of these categories in the remainder of this section.

Table 1. Ad Fraud Categories.

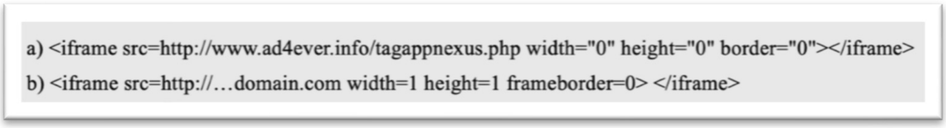
Category	Subcategory
Placement Fraud	Malvertising Stuffing and Stacking Fake Sites Domain Spoofing Ad Injection and Malware
Traffic Fraud	Impression Fraud Click Fraud
Action Fraud	Conversion Fraud Re-targeting Fraud Affiliate Fraud

7.1.1. Placement Fraud

Placement fraud is a general category of fraud in which ingenuine ads or other related content are placed on a legitimate publisher's website (perhaps through malicious means such as misuse of certain HTML features) or on a site entirely set-up by a fraudster, with the ultimate aim to inflate the number of user-clicks and/or impressions on these ads. (Note that advertisement contents, including texts, pictures, and videos, are commonly posted on publishers' websites through an embedded iframe HTML-tag.) The five most significant mechanisms and strategies that can be used to facilitate placement fraud include Malvertising, Stuffing and Stacking, Fake Sites, Domain Spoofing and Ad Injection.

1. Malvertising: Malvertising is a form of placement fraud that is carried out by utilizing advertising malware that gets injected into a publisher's website, and that ends up displaying unwanted ads or pop-ups on the computers of users visiting this site. Sood et al. [48] have pointed out that the common defects in the design of some website widgets pose a high risk of malvertising. Moreover, they have shown that Content Delivery Networks (CDNs)—as third-party ad servers which provide content to different domains on the Internet—are the primary means of spreading malvertising malware. By exploiting the servers of a particular CDN, attackers can inject malicious code in the form of malvertisement and achieve a broad distribution.
2. Stuffing and Stacking: Ad fraud techniques that make use of components which are placed inside a web page but cannot be viewed by the naked eye are called 'stuffing' and 'stacking. Stuffing fraud include two primary forms: keywords stuffing and placement stuffing. Keyword stuffing occurs when specific keywords are hidden in the HTML tags of a fraudster's web page with the intention to increase the value/ranking of this page and its respective ads. On the other hand, placement stuffing is the act of hiding non-textual (i.e., multi-media) components inside a web page, such as: an ad in a small 1 × 1 pixel iframe (refer to Figure 4). Placement stacking is a fraud technique where two or more ads are placed/stacked on top of one other, with only the top ad being actually visible to the user [49]. A single impression or click on such stacked ads would enable the fraudster to bill multiple advertisers.
3. Fake Sites: Placement of ads on fake websites is another strategy commonly deployed by online fraudsters. Fake websites used for the purposes of ad fraud typically have one or more of the following features:
    - they use legitimate domain names but have no legitimate content except for the ad slots;
    - they contain legitimate looking content, which is simply copied from other well-known websites;
    - they deploy domain names that are look-alikes of some highly popular domains (this is also known as domain-name spoofing and is discussed next).

Unfortunately, the high-quality appearance of these sites often makes it very difficult for ordinary users to recognize them as fraudulent.



```
a) <iframe src=http://www.ad4ever.info/tagappnexus.php width="0" height="0" border="0"></iframe>
b) <iframe src=http://…domain.com width=1 height=1 frameborder=0> </iframe>
```

Figure 4. Examples of stuffing ads. (**a**) Creation of an entirely invisible inline frame loading an Ad4ever page [49]. (**b**) Stuffing ads in a small iframe, e.g., 1 × 1 pixel [1].

4. Domain-name Spoofing: Domain-name spoofing is a general type of online fraud in which the fraudster deploys a (fake) domain-name that appears as a legitimate/ whitelisted domain-name. There are several different ways of how domain-name spoofing can be utilized specifically for the purpose of ad fraud: (i) A low-quality publisher disguises its domain-name as the domain-name of another premium publisher in order to sell its inventory to advertisers at higher prices. (ii) In the RTB systems, whenever a user/browser visits a web page, an ad-request containing the web page's URL (i.e., domain name) is sent, launching a bidding war among different advertisers for the right to display an ad on this page. In some cases, publishers are allowed to explicitly declare/supply their domain name in these ad-requests. Fraudulent publishers can use this opportunity to misrepresent their inventory—i.e., supply the domain name of a known premium publisher—thus attracting higher bids by advertisers [50–52].
5. Ad injection and Malware: This type of fraud can also take multiple forms. For example, malicious adware may be run on a user's computer to display unintended advertisement. Additionally, Internet service providers (ISPs) or Wi-Fi service providers may tamper with in-transit HTTP content to surreptitiously insert ads. In another situation, attackers can replace the legitimate websites' ads with their malicious ads or attempt to put them on top of the other ads to modify the web pages for their malevolent intent. As a result of this, both advertisers and publishers will lose their reputation. For example, in 2014, Comcast, one of the leading ISPs, started to serve ads to their customers through its accessible Wi-Fi hotspots by injecting data into retrieved websites [53]. In particular, Comcast injected its JavaScript snippets into the packets/pages being returned by another real server. This decision raised several security concerns. Mediagazer was one of the victims. A small red advertisement appeared at the bottom of the Mediagazer page saying: "XFINITY Wi-Fi Peppy", where Mediagazer did not sell this placement to XFINITY, but rather it happened as a result of ad injection. Even though Comcast did not have any malicious intent, the interaction of the JavaScript with the user's browser and/or the host website could have created security vulnerabilities.

7.1.2. Traffic Fraud

One of the biggest challenges in digital marketing and advertising, mainly for publishers, is to increase the overall network traffic on their websites with the ultimate goal to increase their revenue (i.e., profit). One (though illegal) way for publishers and SSPs to increase their revenue is by committing the so-called traffic fraud by artificially inflating the number of clicks or impressions on their website(s). Two specific subcategories of traffic fraud are: (a) impression fraud, (b) click fraud.

1. Impression Fraud: Impression fraud involves the fraudulent generation of visitor traffic to increase the number of impressions on a web page [54]. Impression fraud can be generated by bots or human labour hired to view web pages intentionally, or through the use of expired domains to divert visitors to fraudsters' websites. Some publishers combine two or more of these approaches to increase the number of generated impressions in the auctions of RTB systems. An interesting study presented in [55] shows that sourced traffic (they are unknown users from unknown places that can be purchased for low CPMs) and bots formed twenty percent of network traffic in 2010. However, this amount dramatically increased to sixty percent in 2015. This increment was directly related to the evolution of advertising platforms (from direct

sale in 1995 to RTB in 2015) and the level of fraud in the ad ecosystem (the level of impression fraud changed from low to very high in the same time interval).

2. Click Fraud: Pay-per-click (PPC), also known as cost-per-click (CPC) marketing, is an essential marketing strategy for businesses in the digital advertising environment. A viewer's click on an advertisement explicitly indicates an interest in the ad that may result in a purchase. Advertisers can assess an ad's performance by measuring/calculating their click-through rate (CTR) ratio. CTR is defined as the number of clicks an ad has received, divided by the number of times the ad was shown (clicks/impressions). The goal of click fraud is to increase the CTR on an ad. It is important to note that both publishers and advertisers may be motivated to conduct click fraud. Namely, publishers may have an interest in committing click fraud as they are rewarded based on the number of executed clicks on the ads they display to their audiences, this type of click fraud is called Publisher Click Inflation. Figure 5 illustrates this attack. On the other side, most advertising campaigns have limited budgets, and each fake click consumes a small portion of that budget. Thus, one way that an advertiser could financially hurt its competitors is by generating a large number of fake clicks on the competitors' ads. This type of click fraud is called Advertiser Competition Clicks. Similar to impression fraud, click fraud is conducted by means of bots and manual/human click farms [4].

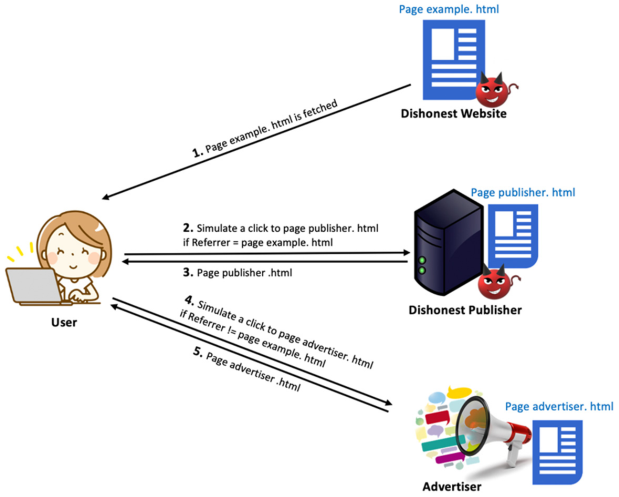

Page example. html
Dishonest Website
1. Page example. html is fetched
Page publisher. html
2. Simulate a click to page publisher. html
if Referrer = page example. html
3. Page publisher .html
Dishonest Publisher
User
4. Simulate a click to page advertiser. html
if Referrer != page example. html
5. Page advertiser .html
Page advertiser. html
Advertiser

Figure 5. An illustration of click inflation attack involving a fraudulent publisher publisher.com, a fraudulent website example.com, an advertiser advertiser.com, and a user. (1) The user clicks on (i.e., retrieves) example.html which contains a script code that silently redirect the user to publisher.com. (2) The user gets redirected to publisher.com which keeps two versions of webpages: a valid/original and a manipulated version. (3) publisher.com presents the manipulated page to the user if the referrer field in the HTTP request points to example.com. (4) publisher.com triggers/generates a click on its ads without the user's knowledge. Otherwise, publisher.com will direct the user to the valid webpage and allow him/her to decide whether or not to click on the ads [4].

7.1.3. Action Fraud

Action Fraud occurs when a fraudster falsifies a user's action in order to generate revenue for himself. Examples of such actions are filling an online form, placing online purchases, signing up, registering, or downloading an item corresponding to an ad. This type of fraud exists in several different forms, including conversion fraud, re-targeting fraud, affiliate fraud.

1. Conversion Fraud: Conversion is any interaction with an advertisement that ultimately generates value (e.g., online purchase). Consequently, conversion fraud occurs when a conversion is artificially generated by a non-human entity (e.g., a bot) or by a human with malicious intent. Typically, upon a click on an advertisement, the user is redirected to the branding site (or landing page), which shows summarized information about the advertised services or product. For any purchase through such a landing page, the user

is typically required to fill out a form by providing personal information such as name, address, and credit card number. One way of conducting conversion fraud is by filling these forms with fake or stolen customer information. Conversion fraud is generally committed either utilizing lead bots or by lead farms. Lead bots are automated computer programs that can fill out thousands of forms in a blink of an eye with either random or correct information. They are also able to click a link or download files automatically. On the other hand, in the lead farm method, genuine human labourers manually perform clicks to conversion with a malicious intent [1].

2. Re-targeting Fraud: Identification and targeting of valuable customers based on their previous online behaviour patterns are common practices in ad-serving platforms. This process is also known as re-targeting [56] or re-marketing. As mentioned earlier, different tracking techniques (e.g., use of cookies) can be deployed to facilitate user re-targeting. The fundamental goal of re-targeting fraud is to give a false impression about previous customers' behaviour and pretend they have an actual interest in a specific product or a service. In other words, through re-targeting fraud, fraudsters attempt to mislead advertisers into believing that fake users (e.g., a group of bots) are prospective purchasers and encourage them to put a higher bid price on impressions generated by these bots.
3. Affiliate Fraud: In affiliate marketing [57], a business entity (also called an affiliate) is rewarded for every visitor that is ultimately brought to the advertiser's site. Affiliate fraud encompasses a range of fraudulent activities that aim to fool the ad system into giving revenue to an affiliate while he/she actually does not qualify for it. Malware or Adware, cookie stuffing, and URL hijacking methods are three types of affiliate fraud. Malware or Adware (an unwanted software designed to generate advertisements on the screens [58]) installed in a user's device can redirect him/her to the advertiser's site via a fake affiliate marketing link. As a result, the affiliate can be in the position to claim a commission from the advertiser. In cookie stuffing based affiliate fraud (refer to Figure 6—different actors and revenue flow in the affiliate marketing system), an affiliate designs a web page to attract audiences potentially interested in a particular brand/product and then stuffs cookies into the audience's computer. If later any of those audiences decide to purchase from the advertiser's web page, the affiliate will be entitled to claim the commission. The last technique (Zhu et al. [1]), URL hijacking, which is also called Typosquatting, emerges as a consequence of the mistake users make by typing the name a website address. Typosquatting leads users to the wrong sites allowing the malicious affiliate to later claim commissions for actions that users might take in the future (malicious affiliate typically registers domains with misspelled names of popular websites) [59,60]. Table 2 summarizes all different categories of fraud in online digital advertising systems, and it specifies the actual conductors and victims of each enlisted type of fraud.

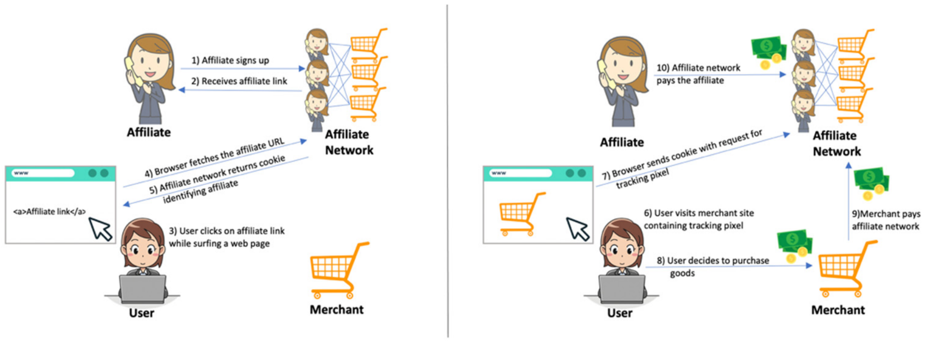

Affiliate
1) Affiliate signs up
2) Receives affiliate link
Affiliate Network
4) Browser fetches the affiliate URL
5) Affiliate network returns cookie identifying affiliate
www
<a>Affiliate link</a>
3) User clicks on affiliate link while surfing a web page
User
Merchant
Affiliate
10) Affiliate network pays the affiliate
Affiliate Network
7) Browser sends cookie with request for tracking pixel
www
6) User visits merchant site containing tracking pixel
9)Merchant pays affiliate network
8) User decides to purchase goods
User
Merchant

Figure 6. Different actors and revenue flow in the affiliate marketing system. (1)–(2) A publisher becomes an ad network affiliate and gets instructed to advertise product(s) of a particular merchant. (3)–(5) A user visits the affiliate website and ends up receiving affiliate-identifying cookie from the affiliate network. (6)–(10) The user purchases the merchant's good(s) directly through the merchant's site, but the affiliate gets credited for this purchase due to the exchange of the previously received cookie with the affiliate network [61].

Table 2. Ad fraud categorization: the perpetrator, the victims, and the objectives.

Type of Fraud	Does What (Sub-Type of Fraud)		Who (Fraudster)	to Whom (Victim)	How (Objective)	Ref.
Placement Fraud (ads and ad related content is placed on a legitimate publisher's website or a site set-up by a fraudster, with the goal of inflating the number of ad clicks and/or impressions)	Stuffing	Keyword Stuffing	Dishonest Publisher	Advertiser	● A dishonest publisher stacks multiple ad placements over one another—all advertisers are charged for the impressions/clicks even though only the top ad is visible to the user(s).	[62,63]
		Placement Stuffing				
	Stacking					
	Domain Spoofing/Fake Sites		Fraudster	Advertiser/User	● A fraudster mounts/publishes a copy of a well-known websites to mislead potential advertisers and/or users into thinking that they are dealing or interacting with the legitimate website.	[64,65]
	Malicious Toolbar/ Malicious Adware		Fraudster/ Dishonest Publisher	Advertiser/User/ Premium Publisher	● A user inadvertently installs a malicious tool-bar in their browser, which then allows the fraudster to inject ad windows into websites the user visits, thus artificially increasing the number of impressions on the shown/injected ads.	
	Ad/Content Injection		Dishonest Publisher/ Deceitful ISP/ Malicious Competitor Publisher	Advertiser/User/ Publisher	● A dishonest publisher installs ad-injection scripts on their website to show more ads per webpage and increase their per-impression and/or per-click revenue. ● A deceitful Internet Service Provider injects ads of their own choosing into the websites that their customers visit, (Only possible in case of unencrypted client-server communication).	[66]

Table 2. *Cont.*

Type of Fraud	Does What (Sub-Type of Fraud)		Who (Fraudster)	to Whom (Victim)	How (Objective)	Ref.
Traffic fraud (techniques that deploy ingenuine web visitors to inflate the number of clicks and/or impressions on a website)	Impression Fraud		Dishonest Publisher/ Malicious Competitor Advertiser	Advertiser	• One way a malicious advertiser can financially hurt its competitor(s) is by generating a large number of fake impressions and/or clicks on the competitor' ads (e.g., by hiring 'human farms' or web bots).	[67–71]
	Click Fraud	Publisher Click Inflation				
		Advertiser Competition Clicks				
Action fraud (techniques that falsify user actions or mislead users into performing certain actions so as to generate revenue for the fraudster)	Conversion Fraud		Dishonest Publisher/ Malicious Advertiser/Fraudster	Advertiser/User	• To complete a purchase, the user is typically required to fill out a form by providing personal information such as name, address and credit card number. A dishonest publisher could conduct conversion fraud is by filling these forms with fake or stolen customer information so as to inflate the number of conversions coming through their site.	[5,72,73]
	Re-targeting Fraud		Fraudster/ Dishonest Publisher	Advertiser	• A fraudster or dishonest publisher can mislead an advertiser into believing that fake users (typically a group of 'pre-trained' web bots) are prospective purchasers and encourage them to put a higher bid price on impressions generated by these bots ultimately increasing their ad revenue.	
	Affiliate Fraud	Malware and Adware	Nefarious Affiliate	User/ Advertiser	• A nefarious affiliate creates a site/webpage that looks like the home page of a legitimate website and is hosted on a look-alike DNS/URL domain. During interaction with this fake site, the user's browsers gets stuffed with the nefarious affiliate's cookies, or the user ends up inadvertently downloading malware. Besides hurting the user and the advertiser, the existence of such a 'fake' site could also hurt the reputation and the profit of the legitimate (impersonated) publisher.	[2,5,72,73]
		Cookie stuffing				
		URL Hijacking		User/Advertiser/ Impersonated Publisher		

8. Taxonomy of Ad Fraud Prevention and Detection Methods

The techniques for detection and prevention of digital ad-fraud can generally be grouped into those that have been proposed/developed in academia vs. those that have been deployed in commercial systems. The techniques developed in academia tend to be mathematically sophisticated, which in turn makes their implementation by industry practitioners challenging. Moreover, it is hard if not impossible to evaluate the actual effectiveness of many academic models due to the lack of real-world datasets. On the other hand, although less sophisticated, commercial systems tend to be more straightforward to implement and are generally deployed at the pre-auction level [1].

8.1. Detection of Digital Advertising Fraud by Commercial Companies

Advertising technology companies are aware that click fraud and impression fraud are the most dominant fraud activities in online ad systems; therefore, they mostly offer services in detecting these two types of fraud.

Oxford Biochron [74] is an example of a fraud detection and verification company that focuses on the activity after the click leading up to the purchase event. They work to find well-disguised fraud targeting affiliate and lead generation advertising campaigns. DoubleVerify (DV) Inc. (New York, NY, USA) [75] is another prominent ad tech company that deploys cookies and fingerprint tracking methods in analyzing impressions. They help publishers deliver high quality traffic to their clients. Furthermore, DSPs and Ad exchanges can benefit from authentication techniques that DV offers to validate pre-bid decisions based on their inventories' quality (the DV solution determines whether the inventory is having an impact on customers. DV delivers an in-depth look at viewability metrics throughout the inventory, with consistent measurement across platforms, devices, and formats, assisting advertisers in delivering value and performance). DV takes snapshots of web pages and their advertisements and compares them to the graphical content extracted from HTML codes to detect invisible advertisements. They also apply a geometric analysis system to check the viewability of online advertisements. This method calculates the ads' location and the location of viewable areas of the browsers to discern stuffing or stacking fraud in the ad ecosystem. WhiteOps [76] is a pioneer among bot fighting ad tech companies, and it has designed FraudSensor (a JavaScript-based detection tag) and MediaGuard (real-time preventive technology with the global footprint of evidence-based intelligence) to detect bot traffic. In particular, these products eliminate non-human traffic from publishers' inventory and help them sell their inventory without fear of getting blocked. IAS (Integral Ad Science) [77], a media valuation company, addresses ad fraud, ad viewability, and brand risk issues and verifies online ad placement quality for both publishers and advertisers. IAS provides a particular service called 'True Advertising Quality', which scores sellers and buyers based on the metrics such as brand safety, ad fraud, content, structure, and viewability. Pixalate [78] delivers the following services to the parties in the digital advertising ecosystem: (1) they can detect non-human traffic in real-time and (2) they monitor almost 50 million URLs while preventing 15 types of ad fraud. They combine various methods such as viewability, domain masking and ads.txt file quality to protect online advertising parties against fraudsters. Forensiq by Impact [79] provides a fraud detection system that identifies malicious activities and eliminates bad actors to ensure that only quality traffic is being driven to the publisher's inventory. Forensiq technology has benefited from machine learning techniques to offer the best in class bot-traffic identification and ensure better ad viewability, ad placement, and brand safety. ClickGUARD [80] is a well-known company that tries to prevent and detect click fraud. ClickGUARD offers a real-time monitoring system for all incoming traffic to instantly monitor every visitor's source, network, and post-click behavior details as clicks happen on the ads. The system analyses the visitor behavior characteristics of every click against common fraud patterns. Moat Inc. (New York, NY, USA) [81] performs real-time ad analytics and offers various ad performance metrics to validate ad impressions and assess audiences. These metrics include: viewability assessment, non-human traffic detection, audience characterization, audience attention and engagement evaluation.

8.2. Detection of Digital Advertising Fraud in Academia

8.2.1. Placement Fraud Detection

As discussed earlier, placement fraud refers to fraudulent activities intended to manipulate or modify the content of a publisher's web pages in order to increase the number of impressions or clicks, as well as a variety of other actions that range from malvertising, ad injections to domain-name spoofing.

To combat placement fraud, Li et al. [82] have introduced a topology-based detection system called MadTrace, capable of automatically generating detection rules to inspect advertisement delivery processes and discover malvertising activities. MadTracer has two major components. The first component is responsible for identifying malvertising content-delivery paths by analysing a larger set of ad click-paths and their features. The second part is an analyser that monitors the infected publisher pages to study cloaking techniques and expand the detection results. The authors claim that their evaluation has shown that MadTracer works effectively against real-world malvertising activities. In particular, MadTracer has caught 15 times as many malicious domain-paths as Google Safe Browsing and Microsoft Forefront combined, as well as several large-scale malvertising campaigns, including a new type of click-fraud attack.

Thomas et al. [66] have presented a detailed investigation into the scope and negative impact of ad injections and their supporting ecosystem. They have designed a multi-staged pipeline to detect ad injections and the value chain behind them. The proposed model is a client-side DOM scanner utilized on a subset of Google's websites. This DOM scanner has the ability to detect and report rogue ad elements. Through the scanner's client-side telemetry technique, the authors have discovered that over 5% of unique daily IP addresses accessing the Google websites during the time frame of the research have been impacted by ad injections via several vectors. Moreover, the authors have identified 50,870 Chrome extensions and 34,407 Windows binaries that have acted as unwanted ad injectors of which 38% and 17%, respectively, have been outright malicious.

To detect fake websites, Abbasi et al. [65] have introduced two categories of fake website detection tools: lookup systems and classifier systems. The lookup systems utilize a client-server architecture where the server-side keeps a blacklist of all known fake URLs, while the client-side tool examines the blacklist and alerts if a website poses a threat. In contrast, a classifier system is a client-side tool that applies a rule-based heuristic to a website's content or its DNS registration information. Classifier detection tools are independent of blacklists in detecting fake websites. They can provide better coverage than lookup systems for spoofed websites. Furthermore, in this work, the authors have proposed a support vector machine (SVM) classification model that utilizes a rich feature set to classify concocted and spoofed sites. Although the developed model appears to have outperformed the other comparable models, the findings of this work suggest that neither the proposed classifier nor the lookup system alone are an effective technique in combating various tactics employed by fraudsters. Instead, a hybrid system with regular/periodic updates of the classification model would be the most effective long-term solution.

8.2.2. Traffic Fraud Detection

The most widely used revenue models in digital advertising platforms, the pay-per-click model, is particularly susceptible to the previously discussed form of traffic fraud—click fraud.

In [83], Kantardzic et al. have introduced a multi-modal real-time detection and prevention system to address the problem of click fraud in the online ad system. The proposed model is based on Collaborative Click Fraud Detection and Prevention (CCFDP) system [84] involving a collaboration between client-side logs and server-side logs. In essence, CCFDP is designed to collect data about each click, including the data fusion between the client-side and server-side logs. CCFDP applies multi-level data to enhance the description of each click and obtain a better estimation of the click traffic quality. Kantardzic et al. have also performed analysis on the extended click records using three independent data mining modules: rule-based, outlier, and click map. The output of each of these modules is a probabilistic measure of evidence that an examined click is fraudulent. Based on the individual scores estimated by the three independent modules, a cumulative score is assigned to each click using the Dempster–Shafer evidence theory. The authors have examined version 1.0 (the initial version (version 1.0) of CCFDP was invented using a rule-based system, which closely matches most of the click fraud detection systems available today) and version 2.0 (the new CCFDP (version 2.0) has an outlier module and the click map module, and an improved rule-based system with additional click context information) of CCFDP systems with data from a real ad campaign. The obtained results have revealed that the use of multi-level data fusion can enhance the overall quality of click fraud analysis.

Haddadi [85] has proposed 'bluff' ads as an online click-fraud detection strategy to blacklist malicious publishers based on a predetermined threshold. The bluff ads are defined as sets of irrelevant ads that should never be clicked on and are displayed amongst a user's targeted ads. The underlying principle of Haddadi's model involves IP address monitoring, profile matching, threshold detection techniques and the use of bluff ads. One of the important objectives of this detection model is to make it more complicated for the botnet owners to train their software or a human operator on. The bluff ads contain irrelevant display text or highly relevant display text with irrelevant targeting information; thus, they work as a litmus test for the legitimacy of an individual's clicking on the ads. The bluff ads can also be seen as an approach to decrease the user's negative perceptions about user tracking by reducing the number of accurately targeted ads. It is worth mentioning that a 'side effect' of running bluff ads could lead to an increase in advertising budgets for advertisers.

Motivated by Haddadi's model, Dave et al. [86] have proposed a methodology that enables advertisers to independently measure and compare click spam ratios on their ads by creating fake ads. They also have developed an automated method for ad networks to differentiate between various click spam attacks in a proactive manner. The primary idea of this approach is that the users associated with click-spam are actually not interested in the displayed ads; consequently, they are less likely to make any extra effort to reach the target website than a legitimately interested user. The advertisers can measure this difference and apply it to estimate the click-spam fraction. Nevertheless, the authors also have taken into account the possibility that some legitimately interested users might not make the extra effort, while some uninterested users do make the extra work to reach the target website. Moreover, the authors propose the use of Bayesian techniques to effectively cancel out quantities that cannot be directly measured so as to reduce the number of false positives and false negatives. The effectiveness of the proposed approach is evaluated through a large-scale measurement study involving ten major ad networks (including Google, Bing, AdMob, and Facebook) and four types of ads (search and contextual advertising on mobile and non-mobile devices). Through this experimentation, the authors have also been able to perform an in-depth analysis of the following types of ad attacks: malware and badware, parked domains, and arbitrage. The results of this study have implied that click spam is a serious problem even for the largest ad network, and it is rampant in the mobile advertising context.

Nagaraja et al. [87] have introduced Clicktok, a statistical technique that detects click spam by identifying click traffic reuse. The underlying principle of Clicktok is based on modelling/measuring of timing properties of click traffic to support a technique capable of separating legitimate and fraudulent clicks. The proposed solution comprises two types of defenses: mimicry (passive defense), and bait-click (active defense). The mimicry defense technique is based on the assumption that 'organic click fraud' involves a reuse of legitimate click traffic, while 'non-organic click fraud' is based on the use of traffic synthesized using pseudo-random times. Accordingly, the organic click fraud can be detected by measuring it similarity to previously observed patterns of user behavior, while non-organic click fraud can be detected by measuring its traffic entropy which is generally lower than the entropy of legitimate user traffic. In the case of (active) bait-click defense, the ad network proactively injects bait clickstreams (with well-defined inter-click delay patterns) into legitimate user traffic. Any attempt (e.g., by a malicious publisher) to reuse these specific clickstream patterns will then be easily detected by the ad network. In this work, Non-negative Matrix Factorization (NMF) algorithm was the main approach used to partition click traffic in order to distinguish fraudulent clicks. According to the presented results, the proposed solution can reach an accuracy of 99.6%.

8.2.3. Action Fraud Detection

As mentioned earlier, action fraud targets users' online business activities. Because cost-per-action advertising typically involves less risk than other advertising pricing models (advertisers only pay when they make a profit or a sale), advertisers are intensely interested in using it to assess their advertising costs vs. revenue; therefore, action fraud can directly impact the ad pricing, campaign planning and other components of the ad ecosystem [1].

To detect fraudulent affiliates in ad ecosystems, Shekhter et al. [46] have introduced a method of monitoring transactions between the affiliate marketer(s) and their respective merchant website. The proposed model analyses patterns of activities to distinguish abnormal traffic from normal traffic. In particular, the detection process involves obtaining transaction data using an affiliate separation module in order to split up the transactions based on the affiliate source. The module then inspects each affiliate transaction to determine whether it matches a set of predefined parameters consistent with some known fraudulent activities. Subsequently, for each affiliate the detection model computes the percentage of suspicious transaction relative to all transactions, and the affiliate gets labelled 'suspicious' if the percentage of suspicious transactions exceeds a predetermined threshold.

To combat cookie stuffing-based affiliate fraud, Chachra et al. [61] have introduced AffTracker, a custom-built Chrome extension, to detect affiliate cookies and collect data from numerous crawled domains targeted by fraudulent affiliates. Using the detection module, they have been able to detect the merchants targeted by cookie stuffing fraud, and they have discovered a number of third-party affiliate networks implicated in stuffing scams. Particularly, they have found that large affiliate networks (such as CJ Affiliate—Commission Junction) provide a more significant opportunity for fraudulent affiliates to simultaneously target multiple merchants. The findings have also shown that in-house (in-house affiliate marketing refers to an affiliate program managed by a merchant using only an affiliate software alternative to an affiliate network. It allows the merchant to have a relationship with affiliates or to save on network commissions) affiliate programs are able to protect their affiliate programs better due to greater visibility into their activities and the revenue flow. Nevertheless, it should be acknowledged that running an in-house affiliate program requires additional investments.

A comprehensive summary of the aforementioned techniques of fraud detection and prevention is provided in Table 3.

Table 3. Comparison on Existing Detection and Prevention Proposal Methods in Digital Advertising System.

	Threat	Mitigation Strategy	Key Points	Ref.
Placement Fraud	Malvertising	MadTracer—Topology-based detection model	• MadTrace is capable of automatically generating detection rules to inspect ad delivery processes and discover malvertising activities. • It comprises two components: one to identify malvertising content-delivery paths through analysing a larger set of ad click-paths and their features. The second is an analyser that monitors the infected publisher pages to study cloaking techniques and expand the detection results.	[83]
	Ad Injection	A client-side DOM scanner	• The proposed detection model first scans the client-side DOM of visitors to Google websites in order to identify the side-effects of ad injection. • It then dynamically executes binaries (the model relies on Google's Safe Browsing infrastructure to dynamically scan binaries) and extensions in search of the same side-effects. • In the third step, the model executes ad injectors in a contained environment while visiting numerous web pages to harvest ad click chains and analyses the entities involved. • Using the proposed model, 192 deceptive Chrome extensions impacted 14 million users were detected.	[66]
	Fake Website/Phishing Attack	Ensemble model of Artificial Neural Network, K-Nearest Neighbours, and C4.5 with Random Forest Classifier (RFC)	• A novel ensemble model is introduced to detect phishing attack on a website. • It includes three machine learning classifiers: Artificial Neural Network (ANN), K-Nearest Neighbours (KNN), and Decision Tree (C4.5) to use in an ensemble method with Random Forest Classifier (RFC). • The ensemble of KNN and RFC detected phishing attacks with 97.33% accuracy.	[88]
	Phishing Website	Random Forest, Support Vector Machine, Neural Networks, Logistic Regression, Naïve Bayes	• Six new features are introduced to improve the detecting accuracy of phishing web pages. The features identify the relation between the page content and the URL of the web page. • Pattern matching algorithms are deployed to match the domain name of page resource elements with the domain name of the queried web page. • A web crawler is used to gather the website features automatically. • The model achieved relatively high accuracy in the detection of phishing websites—99.09%.	[89]

Table 3. *Cont.*

	Threat	Mitigation Strategy	Key Points	Ref.
Traffic Fraud	Click Fraud	CFXGB (Cascaded Forest and XGBoost), Feature transformation and classification.	• CFXGB is a combination of two learning models for feature transformation and classification. • The model consists of three stages: pre-processing, feature transformation based on Cascaded Forest and XGBoost model classification. • The two parameters Max Layers and Early Stopping Rounds (ESR) were used to limit the number of cascades/layers added to the model. • The XGBoost model is then trained on the transformed data, and the parameters are tuned based on Maximum Depths and Learning Rate. Upon completing the training step, the XGBoost model predicts whether a single click is fraudulent or not on all observations.	[90]
	Click fraud	Traffic analysis	• A statistical technique called Clicktok is introduced that detects click spam by identifying click traffic reuse. • It includes two click spam defences: the mimicry defence and the bait-click defence. • The Clicktok framework utilizes the Non-negative Matrix Factorization (NMF) algorithm to partition click traffic in order to identify fraudulent clicks. • Clicktok's FPR is 0.04%.	[87]
	Click Fraud	Multi-time-scale Time Series Analysis	• The proposed model forecasts click fraud behaviour in terms of seconds. It consists of seven stages: pre-processing, data smoothing, fraudulent pattern identification, homogenizing variance, normalizing auto-correlation, developing the AR (Autoregressive) and MA (Moving Average) models and fine tuning along with evaluation of the models. • The study shows the best model for forecasting fraudulent and non-fraudulent click behaviour was the Probability-based model approach compared with the Learning-based probabilistic estimator model.	[91]
	Impression Fraud	Ensemble Learning, Decision Tree classifier and Support Vector Machine	• Some new features (such as: *impressionToDelRatio/Site*—the ratio of impression count and delivery count, corresponding to a given site, and *imAvgDelay/IP*—the average delay between consecutive impressions caused by an IP address) are proposed and applied to the classifiers. • To support classification with a reduced dimension of features, PCA technique is applied. • The solution achieved 99.32% accuracy.	[92] (This study introduces a novel impression fraud detection model in mobile advertising. There is a lack of prior research studies on the topic.)

Table 3. *Cont.*

	Threat	Mitigation Strategy	Key Points	Ref.
Action Fraud	Cookie-stuffing	Tracker—A custom-built Chrome extension	• AffTracker, detects affiliate cookies and collects data from numerous crawled domains targeted by fraudulent affiliates. • The model proved its capability of detecting the merchants targeted by cookie stuffing fraud and a number of third-party affiliate networks implicated in stuffing scams.	[61]
	Cookie-stuffing	Decision-tree based technique	• An automated approach is proposed capable of detecting fraud in affiliate marketing programs with 93.3% accuracy based on HTTP request logs. • The honest and fraudulent activity of 166 affiliate marketing programs across six affiliates is measured. • The study shows more than one-third of publishers in affiliate marketing programs use fraudulent cookie-stuffing techniques to claim credit from online retailers for illicit referrals.	[93]

8.3. Prevention of Digital Advertising Fraud

Desiderius Erasmus has said: "Prevention is better than cure". To effectively prevent fraud in a digital advertising environment, a comprehensive across-the-board endeavor is required to force all parties to follow proper advertising strategies and increase public awareness of the unethical motivators that bring fraud into the ad ecosystem. One of the preliminary steps in avoiding fraud in ad-serving platforms is to study ad banner viewability and arrange web pages in a way that is easy to identify potential placemen vulnerabilities fraudsters seek after. Additionally, Google AdSense [94] suggests placing ads closer to the contents of the host web page; however, ads should be completely distinguishable from the main web page contents so as not to misguide users. It is also mentioned in [95] that putting many ad placements on one single page increases the possibility of stuffing and stacking fraud. Google AdMob [95] recommends not placing ads in areas that can be easily clicked on by accident.

A prevention procedure proposed by Jakobsson et al. [96] aims to avoid click inflation fraud conducted by the publisher. The study expresses the importance of verifying the publishers' identification before making any decision (such as signing them up in the ad network). The AdSense-like syndicate ads program may already reject registering a publisher due to its invalid identification. It should be stressed that nefarious publishers constantly attempt to sign up with invalid, fraudulent names to hide their identities and mislead the other parties in the ad system.

Fou et al. [97] suggest that advertisers should focus more on users' actions than just a raw number of impressions provided by publishers. In fact, advertisers should go beyond the viewability and demand a full transparency about the source of each ad impression. The researchers also advocate for a novel reverse proxy approach innovated by Distil Networks, which inspects each HTTP request in real-time and determines if it is generated by a bot or not.

ANA/WhiteOps [98] encourages all parties in the ad ecosystem to combat fraud by frequently updating and deploying IP blacklisting so as to prevent displaying of ads to those IPs. Namely, entities behind blacklisted IPs would likely produce fraudulent impressions, clicks or other more involved actions.

In addition to the above straightforward recommendation, the more comprehensive solutions for the prevention of fraud in ad platforms can be classified into the following four categories [1,99]: honeypot-based, signature-based, anomaly-based, and credential-based prevention.

- Honeypot-based prevention approach (i.e., bluff ads) is a mechanism that allows advertisers to serve some small, unrecognizable bluff or honeypot ads in order to detect fraudulent activities in the ad system. The different conversion rates between the bluff-ads and the legitimate-ads can be used as an indicator to detect ongoing fraudulent activities.
- Signature-based method refers to identifying and preventing malicious traffic and bogus impressions by hunting specific patterns or features in the traffic. This mechanism uses a predefined pattern (signature) to decide if traffic is valid or not. For example, a typical signature is click count on published ads in order to detect duplicate clicks.
- Anomaly-based prevention technique applies statistical analysis and historical data to identify patterns of fraudulent behavior, and then use those patterns in order to detect suspicious ad placements and/or abnormal traffic.
- Credential-based prevention mechanism (also known as Website Popularity or Page Ranking) refers to the task of assessing the creditability of a publisher or an advertiser in order to discover the authenticity of their web page contents or the number of impressions they generate. The reverse crawling (reverse engineering is the process of understanding the functioning and structure of a website and its information [100]. For example, to evaluate a publisher's credentials, DSPs and advertisers can use reverse engineering/crawling to find the content of web pages and verify that the

content matches the tags associated with the impression when bidding) method and trusted website ranking are the most common approach in that endeavor.

Stone-Gross et al. [99] have expanded the above classification by introducing a Performance-based Pricing approach. Namely, they believe that the Return on Investment (ROI) revenue model is a better alternative to the impression-based methods commonly used in the ad ecosystem. In the case of ROI model, advertisers are not concerned with the number of impressions but rather focus on how much return on investment they can get from a publisher. This type of revenue model can disincentivize impression fraud and eliminate ineffective advertising.

9. Conclusions and Future Trends

Online advertising fraud aims to exfiltrate money from the ad ecosystem by conducting various types of fraudulent actions. This survey has provided a comprehensive study of online digital advertising platforms, their key components and the most popular revenue models. Additionally, various techniques to collect data on users' online activities and their behavioral patterns have also been reviewed. More importantly, the present work adds to the existing literature in this field by focusing on the categorization of ad fraud based on the main human actors—executors vs. victims—and providing illustrative real-world examples of different types of advertising fraud; this essential practical perspective makes it different from previous studies such as [4,5]. Most existing works have discussed advertising fraud in very generic ways. They focused on issues relating to privacy threats and protection mechanisms [5,101], marketing perspective [102–104] and analytical assessment on challenges in online advertising [105,106].

Through this study, the following observations have been made:

There has been a major shift in the academic circles towards the use of machine learning (ML) and artificial intelligence (AI) solutions—some of these works are surveyed in this paper. The shift towards ML/AI solutions is observed in the industry as well. This shift stems from the well-established capabilities of ML/AI to effectively analyze users' needs, interests, and preferences—in real-time and from large volumes of multisensory data—ultimately producing comprehensive consumer insights. In particular, as described in [107,108], ML/AI based speech recognition, natural language processing, and the help of computer vision technologies are very useful for understanding consumer insights into online advertising. Additionally, the studies presented in [109–112] describe the broader use of intelligent advertising in practice for advertising creativity with diverse consumers and as sponsored recommendations on retail platforms. As real-world examples of ML/AI deployment, Facebook, Google, and Amazon—the biggest names in the digital advertising industry—have begun investing in ML/AI solutions in their online advertising platforms [113,114]. The Google Assistant, introduced in 2016, can pull data from any Google app (e.g., Gmail, Search, Maps, Shopping, Photos, Calendar, Contacts, . . .) after only a single sign-in by the user. It then uses AI technologies, such as natural language processing and machine learning, to perform various tasks responding to voice requests or user keyboard input [115].

However, Hairong Li in [115] has claimed that although intelligent advertising seems to be driven by big data, algorithms, and cloud computing, its ultimate future may depend on other factors, such as industry innovation, investment in AI technologies, government regulation, and business and consumer acceptance [116,117].

On the other hand, in the report by the Juniper research group [118], it is stated that the publishers' ad media inventory grows faster than advertisers' demand. This gap provides an exclusive opportunity for fraudsters to fill this unused inventory with fraudulent ads through advanced techniques such as spoofed advertising networks and fabricated ad clicks.

To address the problem of sophisticated ad fraud, we believe marketers should embrace a holistic approach to data analysis. This involves connecting the data dots across networks, browsers, and devices as well as user behavior to complete view of the entire ad ecosystem. Using big data to distinguish between genuine and fraudulent ad requests, the new generation of machine learning techniques (i.e., Deep Reinforcement Learning [119])—which combines artificial neural networks with a reinforcement learning architecture—can be deployed. Reinforcement learning or goal-oriented algorithms learn how to achieve a complicated goal or maximize an objective along a given dimension over many steps. For example, DRL can be used to analyze and identify sophisticated click bots behavior—those that mimic the random movement of a human and engage in humanlike patterns—in digital advertising.

Finally, to stay ahead of the ever-increasing threat landscape requires more advanced and complex defensive capabilities. To acquire these capabilities, we need more datasets of real-world ad requests, extensive experimentation with state-of-the-art methods, and continuous knowledge exchange between the academic and industrial communities. Most systems from commercial companies for fraud detection are black boxes, and the systems developed in academia follow the fast-growing trend of machine learning techniques. Nevertheless, from the investigations we conducted, there is a lack of viable solutions to address the problem of ad fraud in some areas. Moreover, there likely exist some possible research solutions that have not been applied yet. Consequently, it is expected to witness a more extensive interconnection between academia and industry based on the persuasive evidence provided by this study.

Author Contributions: Conceptualization, S.S. and N.V.; methodology, S.S.; validation, S.S. and N.V.; writing—original draft preparation, S.S.; writing—review and editing, S.S. and N.V.; supervision, N.V.; project administration, N.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zhu, X.; Tao, H.; Wu, Z.; Cao, J.; Kalish, K.; Kayne, J. *Fraud Prevention in Online Digital Advertising*; Springer: Berlin/Heidelberg, Germany, 2017.
2. Digital Ad Industry Will Gain $8.2 Billion By Eliminating Fraud and Flaws in Internet Supply Chain, IAB & EY Study Shows. Available online: https://www.iab.com/news/digital-ad-industry-will-gain-8-2-billion-by-eliminating-fraud-and-flaws-in-internet-supply-chain-iab-ey-study-shows (accessed on 4 November 2021).
3. Ad Fraud Stats. 2021. Available online: https://www.businessofapps.com/research/ad-fraud-statistics/ (accessed on 4 November 2021).
4. Pooranian, Z.; Conti, M.; Haddadi, H.; Tafazolli, R. Online advertising security: Issues, taxonomy, and future directions. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2494–2524. [CrossRef]
5. Cai, Y.; Yee, G.O.; Gu, Y.X.; Lung, C.-H. Threats to online advertising and countermeasures: A technical survey. *Digit. Threats Res. Pract.* **2020**, *1*, 1–27. [CrossRef]
6. Estrada-Jiménez, J.; Parra-Arnau, J.; Rodríguez-Hoyos, A.; Forné, J. Online advertising: Analysis of privacy threats and protection approaches. *Comput. Commun.* **2017**, *100*, 32–51. [CrossRef]
7. What Is an Ad Network and How Does It Work?—Clearcode Blog. 2021. Available online: https://clearcode.cc/blog/what-is-an-ad-network-and-how-does-it-work/ (accessed on 4 November 2021).
8. Dave, K.; Varma, V. Computational advertising: Techniques for targeting relevant ads found. *Trends Inform. Retr.* **2014**, *8*, 263–418. [CrossRef]
9. Cook, K. A Brief History of Online Advertising. 2021. Available online: https://blog.hubspot.com/marketing/history-of-online-advertising (accessed on 4 November 2021).
10. Panwar, A.; Onut, I.-V.; Miller, J. Towards real time contextual advertising. In *International Conference on Web Information Systems Engineering*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 445–459.
11. Boerman, S.C.; Kruikemeier, S.; Zuiderveen Borgesius, F.J. Online behavioral advertising: A literature review and research agenda. *J. Advert.* **2017**, *46*, 363–376. [CrossRef]

12. Types Of Online Advertising. 2020. Available online: https://www.adskills.com/blog/7-types-of-online-advertising/ (accessed on 4 November 2021).
13. Understanding RTB, Programmatic Direct, and PMP—Clearcode Blog. 2021. Available online: https://clearcode.cc/blog/rtb-programmatic-direct-pmp/ (accessed on 4 November 2021).
14. Wang, J.; Zhang, W.; Yuan, S. Display advertising with Real-Time Bidding (RTB) and behavioural targeting. *Found. Trends®Inf. Retr.* **2017**, *11*, 297–435. [CrossRef]
15. Ultimate Guide to the Private Marketplace for Publishers | Publift. 2020. Available online: https://www.publift.com//adteach/ultimate-guide-to-the-private-marketplace-for-publishers (accessed on 4 November 2021).
16. DeBlasio, J.; Guha, S.; Voelker, G.M.; Snoeren, A.C. Exploring the dynamics of search advertiser fraud. In Proceedings of the 2017 Internet Measurement Conference, London, UK, 1–3 November 2017; pp. 157–170.
17. Wilbur, K.C.; Zhu, Y. Click Fraud. *Market. Sci.* **2009**, *28*, 293–308. [CrossRef]
18. Cufoglu, A. User Profiling-a Short Review. *Int. J. Comput. Appl.* **2014**, *108*, 3. [CrossRef]
19. Haveliwala, T.H.; Jeh, G.M.; Kamvar, S.D. Targeted Advertisements Based on User Profiles and Page Profile. 27 November 2012. Available online: https://patents.google.com/patent/US8321278B2/en (accessed on 4 December 2021).
20. Fleuren, M.C.W. User Profiling Techniques: A Comparative Study in the Context of e-Commerce Websites. Bachelor's Thesis, Utrecht University, Utrecht, The Netherlands, 2012.
21. Degeling, M.; Herrmann, T. Your interests according to google-a profile-centered analysis for obfuscation of online tracking profiles. *arXiv* **2016**, arXiv:1601.06371.
22. Google Data Collection Research. 2018. Available online: https://digitalcontentnext.org/blog/2018/08/21/google-data-collection-research/ (accessed on 4 November 2021).
23. Dennis, W.L.; Erwin, A.; Galinium, M. Data mining approach for user profile generation on advertisement serving. In Proceedings of the 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, Indonesia, 5–6 October 2016; pp. 1–6.
24. Bujlow, T.; Carela-Espanol, V.; Lee, B.-R.; Barlet-Ros, P. A Survey on web tracking: Mechanisms, implications, and defenses. *Proc. IEEE* **2017**, *105*, 1476–1510. [CrossRef]
25. Schmucker, N. Web Tracking. *In SNET2 Seminar Paper-Summer Term*. Citeseer. 2011. Available online: https://www.semanticscholar.org/paper/Web-Tracking-SNET-2-Seminar-Paper-Summer-Term-2011-Schm%C3%BCcker/304bb388a1e4e74a2109f39ff8ae0b6f66f0dd02 (accessed on 4 December 2021).
26. What Is a Session ID? Available online: https://www.ionos.ca/digitalguide/hosting/technical-matters/what-is-a-session-id/ (accessed on 4 December 2021).
27. Alaca, F. Strengthening Password-Based Web Authentication through Multiple Supplementary Mechanisms. Ph.D. Thesis, Carleton University, Ottawa, ON, Canada, 2018. [CrossRef]
28. Session Management—OWASP Cheat Sheet Series. Available online: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html (accessed on 4 December 2021).
29. HTTP Cookie. Wikipedia. 2021. Available online: https://en.wikipedia.org/wiki/HTTP_cookie#window.name (accessed on 4 December 2021).
30. DOM Standard. Available online: https://dom.spec.whatwg.org/ (accessed on 4 December 2021).
31. Tracking Cookies—How to Limit Third-Party Data Collection. Comparitech. 2021. Available online: https://www.comparitech.com/blog/information-security/tracking-cookies/ (accessed on 4 December 2021).
32. Nasir, M. *Tracking and Identifying Individual Users in a Web Surfing Session*; Computer and Network Security, Middlesex University: London, UK, 2014.
33. Web Caching Basics: Terminology, HTTP Headers, and Caching Strategies. Available online: https://www.digitalocean.com/community/tutorials/web-caching-basics-terminology-http-headers-and-caching-strategies (accessed on 4 December 2021).
34. Klein, A.; Pinkas, B. DNS Cache-Based User Tracking. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2019, San Diego, CA, USA, 24–27 February 2019. [CrossRef]
35. HTTP Caching—HTTP | MDN. Available online: https://developer.mozilla.org/en-US/docs/Web/HTTP/Caching (accessed on 4 December 2021).
36. Sánchez, P.M.S.; Valero, J.M.J.; Celdrán, A.H.; Bovet, G.; Pérez, M.G.; Pérez, G.M. A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1048–1077. [CrossRef]
37. Kaur, N.; Azam, S.; Kannoorpatti, K.; Yeo, K.C.; Shanmugam, B. Browser fingerprinting as user tracking technology. In Proceedings of the 2017 11th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 5–6 January 2017; pp. 103–111.
38. Iqbal, U.; Englehardt, S.; Shafiq, Z. Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May 2021; pp. 1143–1161. [CrossRef]
39. OS and Application Fingerprinting Techniques | SANS Institute. Available online: https://www.sans.org/white-papers/32923/ (accessed on 4 December 2021).
40. Al-Shehari, T.; Shahzad, F. Improving operating system fingerprinting using machine learning techniques. *Int. J. Comput. Theory Eng.* **2014**, 57–62. [CrossRef]

41. Geradin, D.; Katsifis, D.; Karanikioti, T. Google as a de Facto Privacy Regulator: Analyzing Chrome's Removal of Third-Party Cookies from an Antitrust Perspective. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3738107# (accessed on 4 December 2021).
42. Thomas, I. Planning for a cookie-less future: How browser and mobile privacy changes will impact marketing, targeting and analytics. *Appl. Market. Anal.* **2021**, *7*, 6–16.
43. Wilander, J. Intelligent Tracking Prevention. WebKit. 2017. Available online: https://webkit.org/blog/7675/intelligent-tracking-prevention/ (accessed on 4 December 2021).
44. Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default | The Mozilla Blog. Available online: https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/ (accessed on 4 December 2021).
45. The Privacy Sandbox—The Chromium Projects. Available online: https://www.chromium.org/Home/chromium-privacy/privacy-sandbox (accessed on 4 December 2021).
46. Bogna, J. What Is Google's FLoC, and How Will It Track You Online? Available online: https://www.howtogeek.com/724441/what-is-googles-floc-and-how-will-it-track-you-online/ (accessed on 4 December 2021).
47. Chrome is Removing Third-Party Data. What's Next? Available online: https://www.match2one.com/blog/how-removal-of-third-party-cookies-affects-digital-marketers/ (accessed on 4 December 2021).
48. Sood, A.K.; Enbody, R.J. Malvertising–exploiting web advertising. *Comput. Fraud Secur.* **2011**, *2011*, 11–16. [CrossRef]
49. Edelman, B. Accountable? The problems and solutions of online ad optimization. *IEEE Secur. Priv. Mag.* **2014**, *12*, 102–107. [CrossRef]
50. What Is Ad Fraud and How to Prevent It? | CLICKTRUST. We Are CLICKTRUST. 2020. Available online: https://clicktrust.be/en/blog/ppc/what-is-ad-fraud-and-how-to-counter-it/ (accessed on 4 December 2021).
51. Ads.txt: A White Ops Perspective. 2018. Available online: https://www.humansecurity.com/blog/ads.txt-a-white-ops-perspective-1 (accessed on 4 November 2021).
52. Vidakovic, R. The Beginner's Guide to Digital Ad Fraud. AdProfs. Available online: https://adprofs.co/beginners-guide-to-digital-ad-fraud/ (accessed on 4 December 2021).
53. Comcast Wi-Fi Serving Self-Promotional Ads via JavaScript Injection | Ars Technica. Available online: https://arstechnica.com/tech-policy/2014/09/why-comcasts-javascript-ad-injections-threaten-security-net-neutrality/ (accessed on 4 November 2021).
54. Springborn, K.; Barford, P. Impression fraud in on-line advertising via pay-per-view networks. In Proceedings of the 22nd USENIX Security Symposium (USENIX Security 13), Washington, DC, USA, 14–16 August 2013; pp. 211–226.
55. Dr. Augustine Fou—Independent Ad Fraud Researcher. Ad Fraud Ecosystem 2017 Update, 11:52:29 UTC. Available online: https://www.slideshare.net/augustinefou/ad-fraud-ecosystem-2017-update (accessed on 4 December 2021).
56. What Is Retargeting and Which Problems Might Be Damaging Your Campaign? 2020. Available online: https://www.cheq.ai/retargeting (accessed on 4 November 2021).
57. Dwivedi, Y.K.; Rana, N.P.; Alryalat, M.A.A. Affiliate marketing: An overview and analysis of emerging literature. *Mark. Rev.* **2017**, *17*, 33–50. [CrossRef]
58. Adware—What Is It & How to Remove It? Available online: https://www.malwarebytes.com/adware (accessed on 4 November 2021).
59. Dam, T.; Klausner, L.D.; Schrittwieser, S. Typosquatting for fun and profit: Cross-country analysis of pop-up scam. *J. Cyber Secur. Mobil.* **2020**, 265–300. [CrossRef]
60. Szurdi, J.; Kocso, B.; Cseh, G.; Spring, J.; Felegyhazi, M.; Kanich, C. The long "taile" of typosquatting domain names. In Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, 20–22 August 2014; pp. 191–206.
61. Chachra, N.; Savage, S.; Voelker, G.M. Affiliate crookies: Characterizing affiliate marketing abuse. In Proceedings of the 2015 Internet Measurement Conference, IMC'15, Association for Computing Machinery, New York, NY, USA, 28–30 October 2015; pp. 41–47.
62. Daswani, N.; Mysen, C.; Rao, V.; Weis, S.; Gharachorloo, K.; Ghosemajumder, S. Online Advertising Fraud. In *Crimeware: Understanding New Attacks and Defenses*; Addison-Wesley Professional: Boston, MA, USA, 2008; Volume 40, pp. 1–28.
63. Zheng, Y.; Jeon, B.; Xu, D.; Wu, Q.M.; Zhang, H. Image segmentation by generalized hierarchical fuzzy C-means algorithm. *J. Intel. Fuzzy Syst.* **2015**, *28*, 961–973. [CrossRef]
64. Zhang, Y.; Egelman, S.; Cranor, L.; Hong, J. *Phinding Phish: Evaluating Anti-Phishing Tools*; Carnegie Mellon University: Pittsburgh, PA, USA, 2007.
65. Abbasi, A.; Chen, H. A Comparison of tools for detecting fake websites. *Computer* **2009**, *42*, 78–86. [CrossRef]
66. Thomas, K.; Bursztein, E.; Grier, C.; Ho, G.; Jagpal, N.; Kapravelos, A.; Mccoy, D.; Nappa, A.; Paxson, V.; Pearce, P.; et al. Ad injection at scale: Assessing deceptive advertisement modifications. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015; pp. 151–167. [CrossRef]
67. Almahmoud, S.; Hammo, B.; Al-Shboul, B.; Obeid, N. A Hybrid Approach for Identifying Non-Human Traffic in Online Digital Advertising. *Multimed. Tools Appl.* **2021**, 1–34. [CrossRef]
68. Neal, A.; Kouwenhoven, S.; Sa, O. *Quantifying Online Advertising Fraud: Ad-Click Bots vs. Humans*; Oxford Bio Chronometrics: London, UK, 2015.

69. Zhang, L.; Guan, Y. Detecting click fraud in pay-per-click streams of online advertising networks. In Proceedings of the 2008 28th International Conference on Distributed Computing Systems, Washington, DC, USA, 17–20 June 2008; pp. 77–84.
70. Stitelman, O.; Perlich, C.; Dalessandro, B.; Hook, R.; Raeder, T.; Provost, F. Using Co-Visitation networks for detecting large scale online display advertising exchange fraud. In Proceedings of the 19th ACM Sigkdd International Conference on Knowledge Discovery and Data Mining, Association for Computing Machinery, New York, NY, USA, 11–14 August 2013; pp. 1240–1248.
71. Tian, T.; Zhu, J.; Xia, F.; Zhuang, X.; Zhang, T. Crowd fraud detection in internet advertising. In Proceedings of the 24th International Conference on World Wide Web, WWW'15, International World Wide Web Conferences Steering Committee, Geneva, Switzerland, 18–22 May 2015; pp. 1100–1110.
72. Shekhter, H. System and Method for Detecting Fraudulent Affiliate Marketing in an Online Environment. U.S. Patent 20110251869A1, 13 October 2011.
73. Budak, C.; Goel, S.; Rao, J.; Zervas, G. Understanding Emerging Threats to Online Advertising. In Proceedings of the 2016 ACM Conference on Economics and Computation, Maastricht, The Netherlands, 24–28 July 2016; pp. 561–578.
74. Fight Ad Fraud with SecureAd. Fight Digital Fraud with Oxford BioChronometrics. Available online: https://oxford-biochron.com/fight-ad-fraud-with-securead/ (accessed on 4 November 2021).
75. DoubleVerify—DoubleVerify Authenticates the Quality of Digital Media for the World's Largest Brands Ensuring Viewable, Fraud-Free, Brand-Safe Ads. Available online: https://doubleverify.com/company/ (accessed on 4 November 2021).
76. HUMAN. HUMAN | Bot Mitigation | Know Who's Real. Available online: https://www.humansecurity.com (accessed on 4 November 2021).
77. Integral Ad Science | Digital ad Tech & Verification. Available online: https://integralads.com/uk/ (accessed on 4 November 2021).
78. Limited, C. © 2021 P. E. Pixalate—Ad Fraud Protection, Privacy, and Compliance Platform (CTV). Available online: https://www.pixalate.com (accessed on 4 November 2021).
79. Ad Fraud Protect & Monitor: Stop Affiliate, Influencer Fraud. Available online: https://impact.com/protect-monitor/ (accessed on 4 November 2021).
80. ClickGUARDTM | Leading Click Fraud Protection Software. Available online: https://www.clickguard.com/ (accessed on 12 November 2021).
81. Measurement, Analytics, & Brand Safety | Moat by Oracle Data Cloud. Available online: https://www.moat.com/ (accessed on 4 November 2021).
82. Li, Z.; Zhang, K.; Xie, Y.; Yu, F.; Wang, X. Knowing your enemy: Understanding and detecting malicious web advertising. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS '12, Association for Computing Machinery, New York, NY, USA, 16–18 October 2012; pp. 674–686.
83. Kantardzic, M.; Walgampaya, C.; Yampolskiy, R.; Woo, R.J. Click Fraud Prevention via multimodal evidence fusion by Dempster-Shafer theory. In Proceedings of the 2010 IEEE Conference on Multisensor Fusion and Integration, Salt Lake City, UT, USA, 5–7 September 2010; pp. 26–31. [CrossRef]
84. Ge, L.; King, D.; Kantardzic, M. Collaborative Click Fraud Detection and Prevention System (CCFDP) Improves Monitoring of Software-Based Click Fraud. 2005.E-COMMERCE 2005, 34. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.420.8672&rep=rep1&type=pdf#page=53 (accessed on 12 November 2021).
85. Haddadi, H. Fighting online click-fraud using bluff ads. *ACM SIGCOMM Comput. Commun. Rev.* **2010**, *40*, 21–25. [CrossRef]
86. Dave, V.; Guha, S.; Zhang, Y. Measuring and fingerprinting click-spam in ad networks. In Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Association for Computing Machinery, New York, NY, USA, 13–17 August 2012; pp. 175–186.
87. Nagaraja, S.; Shah, R. Clicktok: Click Fraud Detection Using Traffic Analysis. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '19, Association for Computing Machinery, New York, NY, USA, 15–17 May 2019; pp. 105–116.
88. Basit, A.; Zafar, M.; Javed, A.R.; Jalil, Z. A Novel Ensemble Machine Learning Method to Detect Phishing Attack. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; pp. 1–5. [CrossRef]
89. Jain, A.K.; Gupta, B.B. Towards detection of phishing websites on client-side using machine learning based approach. *Telecommun. Syst.* **2017**, *68*, 687–700. [CrossRef]
90. Thejas, G.S.; Dheeshjith, S.; Iyengar, S.S.; Sunitha, N.R.; Badrinath, P. A hybrid and effective learning approach for Click Fraud detection. *Mach. Learn. Appl.* **2020**, *3*, 100016. [CrossRef]
91. Thejas, G.S.; Soni, J.; Boroojeni, K.G.; Iyengar, S.S.; Srivastava, K.; Badrinath, P.; Sunitha, N.R.; Prabakar, N.; Upadhyay, H. A multi-time-scale time series analysis for click fraud forecasting using binary labeled imbalanced dataset. In Proceedings of the 2019 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS), Bengaluru, India, 20–21 December 2019; Volume 4, pp. 1–8.
92. Haider, C.M.R.; Iqbal, A.; Rahman, A.H.; Rahman, M.S. An ensemble learning based approach for impression fraud detection in mobile advertising. *J. Netw. Comput. Appl.* **2018**, *112*, 126–141. [CrossRef]
93. Snyder, P.; Kanich, C. No Please, After You: Detecting Fraud in Affiliate Marketing Networks. In *WEIS*; 2015. Available online: https://www2.cs.uic.edu/~{}ckanich/papers/snyder2015noplease.pdf (accessed on 12 November 2021).

94. Best Practices for Ad Placement—Google AdSense Help. Available online: https://support.google.com/adsense/answer/1282097?hl=en (accessed on 4 November 2021).
95. About Confirmed Click—Google AdMob Help. Available online: https://support.google.com/admob/answer/10094971?hl=en#zippy=%2Chow-can-i-fix-accidental-clicks-on-my-ad-units (accessed on 4 November 2021).
96. Jakobsson, M.; Ramzan, Z. *Crimeware: Understanding New Attacks and Defenses*; Addison-Wesley Professional: Boston, MA, USA, 2008.
97. A Digital Publisher s Guide to Measuring and Mitigating Non-Human Traffic—PDF Free Download. Available online: https://businessdocbox.com/Advertising/74441712-A-digital-publisher-s-guide-to-measuring-and-mitigating-non-human-traffic.html (accessed on 4 November 2021).
98. Bot Baseline: Fraud in Digital Advertising. Available online: https://www.ana.net/miccontent/show/id/rr-2019-bot-baseline (accessed on 4 November 2021).
99. Stone-Gross, B.; Stevens, R.; Zarras, A.; Kemmerer, R.; Kruegel, C.; Vigna, G. Understanding fraudulent activities in online ad exchanges. In Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, Association for Computing Machinery, New York, NY, USA, 15–19 August 2011; pp. 279–294.
100. Kienle, H.M.; German, D.; Muller, H. Legal concerns of web site reverse engineering. In Proceedings of the Sixth IEEE International Workshop on Web Site Evolution Proceedings, Chicago, IL, USA, 11 September 2004; pp. 41–50.
101. Chen, G.; Cox, J.H.; Uluagac, A.S.; Copeland, J.A. In-depth survey of digital advertising technologies. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 2124–2148. [CrossRef]
102. Dörnyei, K.R. Marketing professionals' views on online advertising fraud. *J. Curr. Issues Res. Advert.* **2020**, *42*, 156–174. [CrossRef]
103. Fulgoni, G.M. Fraud in digital advertising: A multibillion-dollar black hole: How marketers can minimize losses caused by bogus web traffic. *J. Advert. Res.* **2016**, *56*, 122. [CrossRef]
104. Kshetri, N.; Voas, J. Online advertising fraud. *Computer* **2019**, *52*, 58–61. [CrossRef]
105. Gordon, B.R.; Jerath, K.; Katona, Z.; Narayanan, S.; Shin, J.; Wilbur, K.C. Inefficiencies in digital advertising markets. *J. Mark.* **2020**, *85*, 7–25. [CrossRef]
106. Kanei, F.; Chiba, D.; Hato, K.; Yoshioka, K.; Matsumoto, T.; Akiyama, M. Detecting and understanding online advertising fraud in the wild. *IEICE Trans. Inf. Syst.* **2020**, *E103*, 1512–1523. [CrossRef]
107. Lee, H.; Cho, C.-H. Digital advertising: Present and future prospects. *Int. J. Advert.* **2019**, *39*, 332–341. [CrossRef]
108. Kietzmann, J.; Paschen, J.; Treen, E. Artificial intelligence in advertising: How marketers can leverage artificial intelligence along the consumer journey. *J. Advert. Res.* **2018**, *58*, 263–267. [CrossRef]
109. Qin, X.; Jiang, Z. The impact of AI on the advertising process: The chinese experience. *J. Advert.* **2019**, *48*, 338–346. [CrossRef]
110. Chen, G.; Xie, P.; Dong, J.; Wang, T. Understanding programmatic creative: The role of AI. *J. Advert.* **2019**, *48*, 347–355. [CrossRef]
111. Deng, S.; Tan, C.-W.; Wang, W.; Pan, Y. Smart Generation system of personalized advertising copy and its application to advertising practice and research. *J. Advert.* **2019**, *48*, 356–365. [CrossRef]
112. Malthouse, E.C.; Hessary, Y.K.; Vakeel, K.A.; Burke, R.; Fudurić, M. An algorithm for allocating sponsored recommendations and content: Unifying programmatic advertising and recommender systems. *J. Advert.* **2019**, *48*, 366–379. [CrossRef]
113. Alcantara, C.; Schaul, K.; Vynck, G.D.; Albergotti, R. How Big Tech Got So Big: Hundreds of Acquisitions. Available online: https://www.washingtonpost.com/technology/interactive/2021/amazon-apple-facebook-google-acquisitions/ (accessed on 4 November 2021).
114. Lai, Z. Research on advertising core business reformation driven by artificial intelligence. *J. Physics Conf. Ser.* **2021**, *1757*, 012018. [CrossRef]
115. Li, H. Special section introduction: Artificial intelligence and advertising. *J. Advert.* **2019**, *48*, 333–337. [CrossRef]
116. Manheim, K.; Kaplan, L. Artificial intelligence: Risks to privacy and democracy. *Yale JL Tech.* **2019**, *21*, 106.
117. Vlačić, B.; Corbo, L.; Costa e Silva, S.; Dabić, M. The evolving role of artificial intelligence in marketing: A review and research agenda. *J. Bus. Res.* **2021**, *128*, 187–203. [CrossRef]
118. Juniper Research: Advertising Fraud Losses to Reach $42 Billion in 2019, Driven by Evolving Tactics by Fraudsters. 2019. Available online: https://www.businesswire.com/news/home/20190520005650/en/Juniper-Research-Advertising-Fraud-Losses-to-Reach-42-Billion-in-2019-Driven-by-Evolving-Tactics-by-Fraudsters (accessed on 4 November 2021).
119. Li, Y. Deep reinforcement learning: An overview. *arXiv* **2017**, arXiv:1701.07274.