**Deep neural classifier model paper**

<https://journals.riverpublishers.com/index.php/JCSANDM/article/view/2263/5083>

**how attackers uses third-party cookie**

Attackers can use third-party cookies to track users' online behavior across multiple websites without their knowledge or consent. Here are some ways attackers can use third-party cookies:

1. Tracking: Attackers can use third-party cookies to track users' browsing habits across multiple websites. They can use this information to create detailed profiles of users and sell this information to advertisers or use it for malicious purposes.
2. Cross-site request forgery (CSRF) attacks: Attackers can use third-party cookies to carry out CSRF attacks, where they trick a user into unknowingly executing an action on a website they are logged into. For example, an attacker can inject a malicious script into a website that a user visits, which makes a request to another website where the user is logged in, using the third-party cookie to authenticate the request.
3. Session hijacking: Attackers can use third-party cookies to steal a user's session token and hijack their session. By stealing the session token, attackers can impersonate the user and perform actions on their behalf, such as making unauthorized purchases or accessing sensitive data.
4. Malvertising: Attackers can use third-party cookies to serve malicious ads on websites. When a user clicks on the ad, the attacker can use the third-party cookie to track their browsing activity or redirect them to a phishing or malware-infected website.

To protect against these attacks, it is important to use secure cookies that are encrypted and have secure flags set, to limit the scope of third-party cookies, and to use content security policies (CSPs) and other security measures to prevent cross-site scripting (XSS) attacks and other vulnerabilities.

**Checking if it is tracking third party cookie**

To check if a third-party cookie is a tracking cookie, you can follow these steps:

1. Check the domain of the cookie: Third-party cookies are set by a domain that is different from the domain of the website you are currently visiting. If the cookie is set by a domain that you do not recognize or have never visited, it could be a tracking cookie.
2. Check the cookie's purpose: Some third-party cookies are necessary for the proper functioning of a website, such as cookies used by a content delivery network (CDN) or advertising network. However, other third-party cookies are used for tracking and advertising purposes. You can check the purpose of the cookie by examining its name and value or by reading the cookie's documentation.
3. Check the cookie's expiration date: Some tracking cookies have a long expiration date, meaning they remain on your computer for an extended period. If a cookie has a long expiration date and is from a domain you do not recognize, it may be a tracking cookie.

XSS injection (attack)

**<script>**, **<iframe>**, **<object>**, **<embed>**, or **<meta>**