International Journal of Electrical and Computer Engineering (IJECE)
Vol. 15, No. 6, December 2025, pp. 5792~5803
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i6.pp5792-5803

Exploring cookies vulnerabilities: awareness, privacy risks and exploitation

Nor Anisah Amir Hamzah, Anis Safiyyah Adnan, Norsaremah Salleh
Department of Computer Science, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur, Malaysia

Article Info

Article history:

Received Jan 4, 2025
Revised Aug 6, 2025
Accepted Sep 16, 2025

Keywords:

Awareness
Cookies
Exploitation
Online tracking
Privacy risks

ABSTRACT

This study investigates cookie vulnerabilities, focusing on awareness, privacy risks, and exploitation techniques. We used a mixed-method approach that combines insights from a survey study and a systematic mapping study of 27 papers from online databases to comprehensively address the research topic. The results show a moderate level of user awareness about cookie-related privacy risks, with significant concerns over user tracking and profiling, identified in 88% of the reviewed studies. Key risks include sensitive data exposure, privacy and consent issues, targeted advertising, ineffective mitigation measures, and cyberattacks. Tracking via cookies, and especially third-party cookies were found to pose the greatest risk to end-users. Their widespread use for cross-site tracking and extensive fingerprinting often occurred without users' awareness or explicit consent. These insights suggest the need for stricter privacy laws, better practices on cookies, and improved user awareness to mitigate concerning risks.

Corresponding Author:

Norsaremah Salleh
Department of Computer Science, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia
Gombak street, 53100 Kuala Lumpur, Malaysia
Email: norsaremah@iium.edu.my

1. INTRODUCTION

With the evolution of internet use to various aspects of daily life, privacy has become a greater concern in the digital era. Websites use cookies to track the user behavior, collect personal data and track them for personalization, analytics and other various purposes [1]. Cookies are a widely used technology, but they are also a subject of heated debate concerning their effect on user privacy. Online cookies, and more specifically third-party cookies, have raised concerns over what data they collect and how this data can be used.

Although cookies are widely used, users have a low understanding of privacy threats that may be posed by cookies. Third-party cookies are particularly invasive of users' privacy because they make it possible to track users across different sites, in the process of collecting sensitive data without users' direct consent. Even though cookie-related privacy threats have been researched in prior studies (*e.g.* [2], [3]), there is a significant gap in users' understanding of the associated privacy risks, especially in real-world contexts. The objective of this research is to study the level of awareness and to explore the privacy risks presented by cookies and exploitation techniques used related to cookies, especially in the context of online tracking. We have used a mixed-method research design consisting of survey and systematic mapping study to achieve the research objective.

The contributions of this study include raising awareness of online cookie risks among university students and identify knowledge gaps in security practices. It identifies the privacy risks cookies pose and explores the exploitation techniques, offering insights into where cybersecurity measures can be improved. These findings have practical implications for improving digital literacy through education, informing privacy-focused campaigns, and guiding policymakers and web administrators in enhancing cookie management and user data protection.

2. RELATED WORKS

There are various studies that have been conducted on third-party web tracking [4]. Although cookies are virus-free, tracking technologies use them as means of collecting and storing data, which is considered as problematic since the user's personal information is globally shared without their consent or knowledge, and allowing the trackers to build users' profiles according to their online activity [5]. Takata *et al.* [4] highlighted that cookies are key to several functionalities, such as keeping a user logged in, memorizing preferences, and gathering analytics data. However, the extensive usage of cookies, mainly third-party cookies, raised serious privacy issues since advertisers and analytics firms typically used them in order to monitor users' activities over multiple sites. This consequently facilitated the creation of fairly precise profiles about the user that often drew no explicit consent from the user and often heightened concerns over data privacy and misuse.

Previous studies analyzed third-party cookies, which are used to trace users and their behavior. According to Mayer and Mitchell [6], third-party cookies help invade privacy by leaking sensitive information, such as location, browsing history, and behavior patterns. Techniques like link decoration and Canonical Name (CNAME) cloaking have been implemented to bypass browser-imposed restrictions on cookie usage, as noted by Takata *et al.* [4] These evolving approaches highlight the inadequacy of the privacy measures in mitigating the risks posed by cookies.

In addition, Shuford *et al.* [7] emphasized how user data might be accidentally exposed through URL leaks and embedded content, which heightens worries about privacy violations made possible by cookies. Bhatraju *et al.* [8] investigated various cookie-based attacks, including cross-site request forgery (CSRF), cross-site scripting (XSS), and cookie poisoning. Their findings indicated that security measures and the enforcement of privacy regulations need to be greatly improved to reduce the risks posed by online tracking technologies. Further, the analysis by Pantelic *et al.* [9] highlights the need for a balanced approach to cookie usage and regulation by highlighting the dual role that cookies play in facilitating web functionality and increasing privacy threats. While existing studies have extensively examined third-party cookies, their functionalities, and associated privacy risks, none have specifically conducted a systematic mapping study to comprehensively assess the privacy risks posed by cookies. Our research fills this gap by systematically analyzing and categorizing privacy risks, offering a broader understanding of the implications of cookie usage.

3. METHOD

This study adopts a mixed-method approach [10], [11] by employing a survey and systematic literature map to study about cookie vulnerabilities more comprehensively. The survey aims to measure students' awareness of cookies and the associated privacy risks. A systematic mapping study (SMS) was performed to investigate the privacy risks exposed by cookies and the exploitation techniques mentioned in the literature regarding cookies' vulnerabilities. The SMS methodology was chosen because it offers a structured and transparent process for reviewing broad research areas, allowing the identification of trends, gaps, and classification of studies. In the next subsection, we will discuss the methodology for the survey and the SMS.

2.1. Survey

Survey research explores the connections between different variables and provides a quantitative description of particular characteristics within a population [12]. Creswell [11] mentioned that surveys are used mainly to assess the present characteristics, opinions, behaviors or attitudes of a defined population. In this study, the survey focuses on assessing the awareness and practices regarding cookie privacy risks among undergraduate students at International Islamic University Malaysia (IIUM). The survey aims to answer following research question:

RQ1: To what extent are students aware of potential security risks when allowing cookies on online websites?

The following steps were taken to ensure comprehensive and accurate data collection and analysis:

a. Defining objectives: The survey aims to discover the level of awareness among students about privacy risks related to cookies and their management practices.
b. Identify population: We used purposeful sampling targeting students from various faculty at IIUM.

c. Develop questionnaire: A questionnaire that encompasses awareness of cookies, privacy risks and cookie management practices was developed using a Google Form.
d. Identify key variables: The key variable is the level of awareness of privacy risks posed by cookies among students.
e. Survey distribution: The surveys were distributed via group WhatsApp, Instagram, and Telegram.
f. Plan statistical analysis: We conducted descriptive analysis on the survey data to identify students' awareness and attitudes on cookies.
g. Address ethical issues: We provided informed consent, confidentiality, and anonymity for all participants before they complete the survey.
h. Survey analysis: Analyze the data to assess student's awareness of cookie privacy concerns.

2.2. Systematic mapping study

Based on the insight obtained from the survey, we conducted an SMS in order to provide a structured overview of the current knowledge on cookie vulnerabilities, privacy risks, and exploitation techniques. We followed guidelines by [11], [13]. The main objectives of the SMS were to classify and synthesize existing studies, identify trends and explore research gaps. The SMS aims to address the following research questions:

RQ2: What do we know about the risks to user privacy posed by online cookies?
RQ3: What exploitation techniques regarding cookie vulnerabilities are identified in the literature?

As shown in Figure 1, the mapping study was executed in three key phases: planning, execution, and reporting. The planning phase involved developing the research questions, a review protocol and defining the inclusion/exclusion criteria. In the execution phase, literature search was conducted, the criteria were applied to select relevant studies, data were extracted, and the findings were categorized based on a classification scheme. The final phase involved reporting the findings from the studies included.

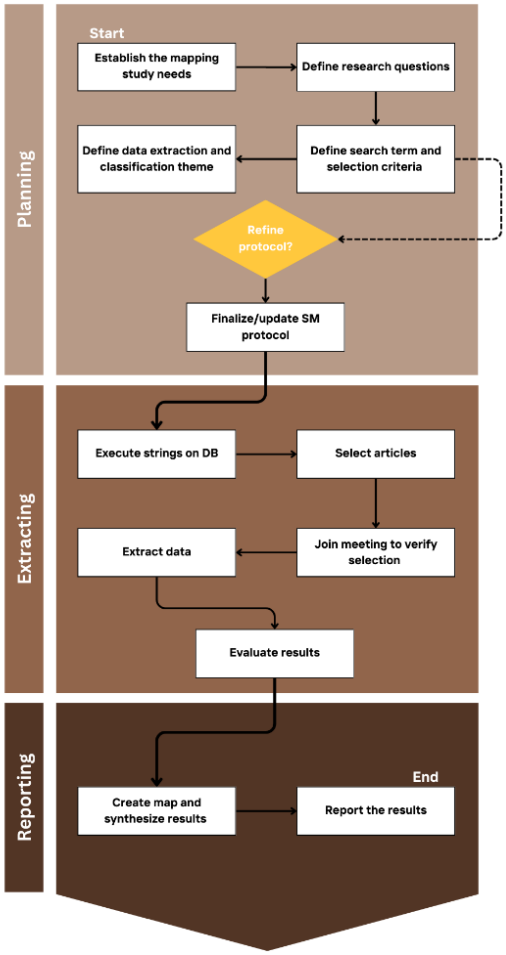

Figure 1. Systematic mapping process

2.2.1. Phase 1 - planning

The coverage of the mapping study was established to focus on cookie vulnerabilities, privacy risks and exploitation techniques. During this stage, two research questions were developed to guide the mapping process. Based on the research questions, the search string constructed was ("Cookies" AND "Privacy" AND "Risks"). This string was carefully constructed based on the following strategy:

a. The keyword "Cookies": It will focus on the main subject, exploring their types and purposes.
b. The keyword "Privacy": It will address concerns related to user data protection.
c. The keyword "Risks": It will highlight potential vulnerabilities and security issues associated with cookies.

To ensure relevance to the research topic, the inclusion criteria required that studies explicitly discuss cookie vulnerabilities or risks to user privacy as shown in Table 1. A protocol was designed to extract and classify data consistently. This included predefined categories for publication years, publication venues, and dependent topics.

Table 1. Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
IC 01 – The title and/or abstract and/or keywords do(es) explicitly mention(s) cookies, privacy, and risks to users	EC 01 – Papers that investigated cookies but not related to privacy or risk.
IC 02 – Fully refereed journal and conference papers, and book chapters	EC 02 – Articles where the full text is not accessible.
IC 03 – Full-text articles accessible through IIUM library subscriptions.	EC 03 – Articles are not written in English.
IC 04 – Articles/chapters must be written in English language.	

2.2.2. Phase 2 - execution

During this phase, the searching of studies was performed to retrieve studies published up until 2024. Selection of studies was conducted based on the inclusion and exclusion criteria. Titles, abstracts, and keywords were used to filter the articles. Further review of introductions and conclusions was conducted for ambiguous cases. Finally, data extraction activity was conducted based on selected studies.

2.2.3. Phase 3 - reporting

During this phase, extracted data were synthesized into a systematic map to identify trends, and key insights related to privacy risks and exploitation techniques. Findings were documented to address RQ2 and RQ3, highlighting privacy risks and exploitation techniques related to cookie vulnerabilities. To create a map of studies on cookie vulnerabilities, privacy risks and exploitation techniques, we used topic-independent (generic) classification and topic-dependent classification. In terms of general classification, studies were organized according to publication year as shown in Table 2.

For topic-dependent classification, we selected categories based on the main themes of cookie vulnerabilities. These included two main dimensions: the type of risks and the exploitation techniques reported in the existing studies. The risks can be categorized based on privacy risks, such as user tracking and profiling, privacy and consent issues, sensitive data exposure, ineffective mitigation measures, and data integrity issues. The second category focuses on the various techniques used to exploit cookie vulnerabilities such as cookie tracking, session hijacking and navigational phishing. This dual classification methodology ensured a comprehensive framework for analyzing and synthesizing the literature. It enabled us to map out previous studies in a methodical manner and identify study gaps related to cookies, privacy threats, and exploitation strategies.

Table 2. Classification schemes

General classification	Topic-dependent classification
Publication year	Type of risks
	Exploitation techniques

4. RESULTS AND DISCUSSION

4.1. Answering research question 1

We have collected responses from a total of 60 students through social media platforms and other online channels. Among the respondents, 21 were male, and 39 were female. Most of the respondents (61.67%) aware of the security risk of online cookies. On the other hand, 35% are either unsure or do not know what these risks are, demonstrating a relatively poor understanding of the privacy implications of cookies.

In terms of awareness of security risks, the results showed that 68.33% of the respondents understand the meaning of cookies in relation to the internet browser, 25% are not sure what they mean, and 6.67% do not understand the meaning at all. This indicates an overall decent level of awareness, although not every student appears to have a solid understanding of how cookies actually work. This could be the reason they face such issues with cookies, as a large number of the respondents usually use online websites (83.33%), according to the survey.

Respondents are presented with cookie pop-ups the most, and the majority (41.67% always and 53.33% sometimes) accept the cookie pop-up. However, only a small number of respondents (5%) never accepts cookies, indicating a common practice of data bypass or ignoring privacy settings for convenience. The majority (43.33%) see the potential consequences of accepting cookies as tracking their online activity, collecting personal information and showing targeted ads, while smaller groups see the potential consequences as tracking their activity or only collecting personal information. While many students recognize the security risks, their follow-up actions differ as only 40% are moderately concerned with privacy issues, 20% are not concerned, and a very small number (13.33%) are strongly concerned. It is important to note that 95% of the respondents use third-party cookie detectors or blockers, which shows that they are taking control of their own online privacy. It was also common among them to use security measures like clearing out cookies and history regularly, disabling third-party cookies and avoiding unclear links or ads. Overall, the survey results indicate that there is a relatively high level of awareness among students about the potential security risks they face with cookies, but there is still a need for better education and understanding of the best practices for handling cookies in order to fully understand the risks and implications of this technology. However, without fully grasping the potential implications, students still easily accept cookies, indicating an inconsistency between the awareness and action spheres when it comes to managing their online activities.

3.2. Demographics data from SMS

The results from Table 3 shows that a total of 75 studies were retrieved from online databases subscribed by International Islamic University Malaysia (IIUM) library. Out of 75 studies, 61 were retrieved from Scopus and 14 from IEEEXplore. Upon filtering based on the inclusion and the exclusion criteria, we included 27 studies, in which 81% were from Scopus and 19% from IEEEXplore.

The bar chart in Figure 2 shows the number of studies over a specified period, highlighting a significant peak in 2022. The data reveals a sharp increase in publications during this year, reaching a maximum of six (6) papers, compared to two (2) in the preceding year (2021) and four (4) in the subsequent year (2023). The trend demonstrates sustained level of academic interest in the subject in the last several years.

Table 3. Search results

Database	Retrieved	Excluded	Included
Scopus	61	39	22
IEEEXplore	14	9	5
TOTAL	75	48	27

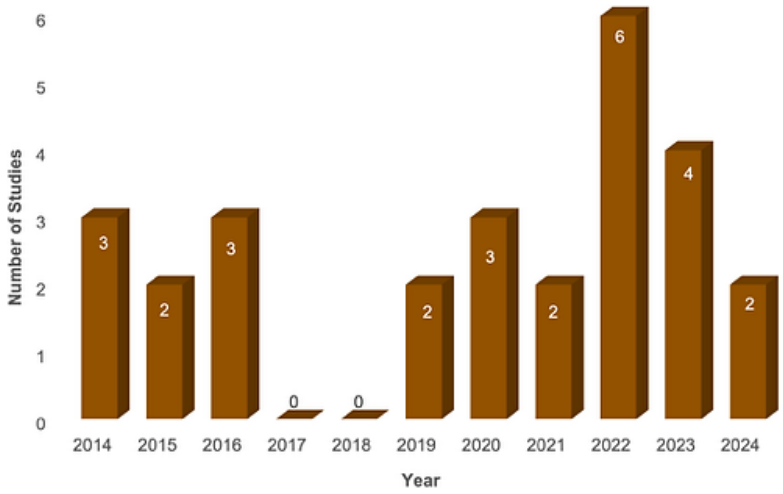

Figure 2. Number of studies published per year

3.3. Answering research question 2

To answer this question, we reviewed from a mapping study a total of 27 studies that investigate the diverse privacy risks associated with online cookies. The papers identified various vulnerabilities and possible threats, raising awareness in this area and the need for mitigation techniques to improve user privacy. Key risks identified in the literature include user tracking, sensitive data exposure, targeted advertising, privacy and consent issues, poor mitigation measures, cyberattacks, data integrity issues, and privacy policy failures. Collectively, these risks contribute to the decline of user privacy in the context of online cookies. Table 4 provides the list of the types of risks available in existing studies and the total number of studies.

Table 4. Types of risk

Type of risk	Paper references	Total
User tracking and profiling	[2]–[4], [8], [14]–[19] [20]–[29] [30]–[33]	24
Sensitive data exposure	[2], [14], [19], [22], [26], [28], [29], [31]–[33] [34]	11
Privacy and consent issues	[2], [3], [8], [17], [18], [26], [28], [32], [34], [35]	10
Targeted advertising	[2], [3], [14], [18], [27], [29], [30], [32], [36]	9
Ineffective mitigation measures	[3], [4], [20], [22], [28]	5
Data integrity Issues	[2], [16], [21], [25]	4
Cyber attacks	[3], [22], [32]	3
Privacy policy failures	[20], [33]	2

Results show that the most worrying privacy risk is user tracking and profiling, which have been studied in 24 out of 27 studies (88.88%). All of the 24 articles in Table 4 explicitly emphasized that cookies or commonly referred to as unique identifiers, including third-party cookies, are vital in enabling websites to track user activity and perform cross-site tracking with the involvement of third-party websites. This tracking capability is essential in building detailed user profiles based on browsing behavior and interactions, exposing users to privacy threats and raising concerns about user privacy. This is because it makes it easier for third-party advertisers and websites to gather and exploit personal data without user knowledge or consent.

The second most common privacy risk mentioned in the literature is sensitive data exposure, which is discussed in a total of 11 studies. Two articles [2], [34] highlighted that browsing habits reveal personal details like gender, age, and political beliefs. One of the studies [22] stated that encrypted traffic allows attackers to hijack the session cookies and passwords. Two studies [25], [28] noted that misconfigured cookies can leak user data. Cookies store sensitive data such as IP addresses and geolocation which can be exploited for specific ads according to three studies [29], [32], [33]. Three studies [19], [31], [34] pointed out the sharing of personal data to third-party trackers and one more [31] showed that major advertisers are capable of tracking over 90% of user's browsing histories, rendering users susceptible to privacy violations. These results emphasize severe privacy risks in cookie management.

Next, privacy and consent issues were identified as the third most studied risk, addressed in ten (10) studies. Users typically have no control over shadowy data harvesting activities [2], and impulsiveness or social norms can expose them to privacy threats [35]. Only 28% of the websites allow users to get rid of their data [17]. Users often incorrectly assume that privacy policies prevent sharing data with third parties or that cookies cannot track behavior without asking for explicit consent from the users [18], [26]. Cookie banners usually fail to ensure informed consent [34], and data continues to be collected through third-party cookies despite users' choice of opting out [28], [32]. Even the efforts of disabling or filtering cookies do not prevent tracking, most cookies are sent without specific opt-in consent, resulting in unintentional sharing of the data [3], [8], [32]. This gap in expectations further emphasizes the lack of transparency regarding how cookies are used and the need for more responsible and open practices when it comes to data collection and usage.

The fourth most discussed privacy risk is targeted advertising, which is mentioned in a total of nine studies. Several studies highlighted how online tracking and cookies are used for personalized ads. For example, one article [2] explained that user's browsing habits are tracked and used to target users with specific ads, raising privacy concerns. Another study [36] noted that cookies track users' activities to help advertisers serve targeted ads. Retargeted ads, which show users products they previously browsed, were also mentioned as a significant concern [18]. Tracking mechanisms, as highlighted in one study [30], create detailed behavioral profiles that can be sold to third parties. Advertising cookies are used to collect users' online activity data and customize advertisements [29], [32]. These findings show how targeted advertising practices not only compromise user privacy but also sustain a system of commercial surveillance.

The fifth risk is ineffective mitigation measures, which are mentioned in five studies. Two out of five studies highlighted that the lack of secure network protocols like HTTPS and vulnerabilities in cookie

management expose users to privacy threats, especially in sensitive situations [20], [22]. For example, SameSite cookies were not fully protected due to CNAME cloaking, which bypassed security features like the HttpOnly attribute [4]. Other studies noted that major cookie-blocking browsers like Edge and Firefox do not block all third-party cookies by default, allowing trackers to retain cookies despite opt-out actions [28]. Additionally, techniques like disabling third-party cookies or using filter lists were found insufficient to prevent tracking effectively [3]. These findings emphasize that existing mitigation measures are insufficient in fully protecting users' privacy. They underline the need for stronger, more effective strategies to manage cookies securely, particularly in an era where data privacy concerns are escalating. These findings suggest a clear need for improved browser settings, more robust privacy tools, and better user awareness of how cookies function and how to control them effectively.

Data integrity issues were identified in four studies, highlighting the concern about the persistence and misuse of cookies. One study [2] discussed how Flash cookies can regenerate deleted normal cookies, preserving sensitive information. Another study [16] noted the European Union's response to privacy concerns by introducing consent requirements in the e-privacy directive to address third-party tracking. Additionally, one article [21] pointed out the power imbalance between consumers and website operators, who control the collection of private information. Cookies that retain user data for extended periods can increase the risk of misuse if not managed properly, potentially allowing unauthorized access to sensitive data and violating privacy regulations such as in the general data protection regulation (GDPR) by the European Union [25]. This shows the importance of not only ensuring that cookies are securely managed but also that users are educated about the risks associated with long-term cookie storage. Proper cookie management and awareness of how cookies can affect data integrity are crucial to maintaining user privacy in an increasingly data-driven world.

Three studies pointed out Cyber Attacks as a privacy risk, emphasizing the risk associated with cookies vulnerabilities like Cross-Site Scripting (XSS) [4], [22], [32]. XSS attacks can be used to steal user credentials, alter website behavior, or make a site unusable, allowing attackers to hijack user sessions or launch phishing attacks [22]. Additionally, cookies can be leaked through XSS or network vulnerabilities, exposing users to risks such as session hijacking and CSRF attacks [4]. One study also highlighted how XSS and CSRF attacks can compromise website availability and steal sensitive data by exploiting cookies [32]. These cyber-attack risks underscore the importance of strong security measures in cookie management, such as using secure and HttpOnly flags for cookies, implementing encryption for sensitive data, and enforcing strong session management practices to prevent unauthorized access.

Privacy policy failures, discussed in two studies, highlight the significant gaps in user information regarding data handling. One study [20] revealed that only 16% of websites had accessible privacy policies, and just 4% provided a cookie consent banner, leaving users uninformed about how their data is managed. Another study [33] found that only 32% of websites provided privacy policies, with most failing to disclose tracking or data retention practices, leading to uncertainty and potential misuse of user data. These privacy policy failures highlight the need for stronger regulations and better practices to ensure that websites provide clear, accessible, and comprehensive information about their use of cookies and data collection methods.

The bubble plot in Figure 3 highlights the number of papers mentioning cookie-related privacy risks per year. User Tracking and Profiling is the most frequently discussed risk; reaches it peaks at five mentions in 2022. Sensitive data exposure and privacy and consent issues also show significant attention, especially in recent years. Targeted advertising remains consistently mentioned, with a peak in 2022. Less frequently addressed risks, such as ineffective mitigation measures, data integrity issues, and cyber-attacks, appear sporadically. Privacy policy Failures receive minimal focus. Overall, user tracking and profiling dominate the discussion, reflecting its central role in privacy concerns.

3.4. Answering research question 3

To answer this research question, we examined 27 papers to find and classify exploitation techniques of cookie vulnerabilities and identified 14 articles that either mentioned or discussed these exploitation techniques. A cookie is an essential part of web functionality, enabling stateful interactions between clients and servers [37]. However, their misuse or vulnerabilities can lead to severe security and privacy risks [5]. Our approach focused on identifying exploitation techniques on cookies from the papers, such as cookie synchronization, session hijacking, and CSRF attacks. Table 5 provides the list of exploitation techniques available in existing studies included in this mapping study. The analysis identified exploitation techniques in 14 studies out of the 27 studies (51.9%), while the remaining 13 studies (48.1%) did not explicitly mention any exploitation techniques [3], [14]–[17], [21], [23]–[25], [29] [34]–[36]. Out of 14 studies, the discussion on the techniques varied. Some of the studies discussed more than one exploitation techniques such as in [4], [19]. There are studies that briefly mention cookies in the exploitation technique

discussion, but they are still considered in this research because the exploitation conducted had cookies being implemented.

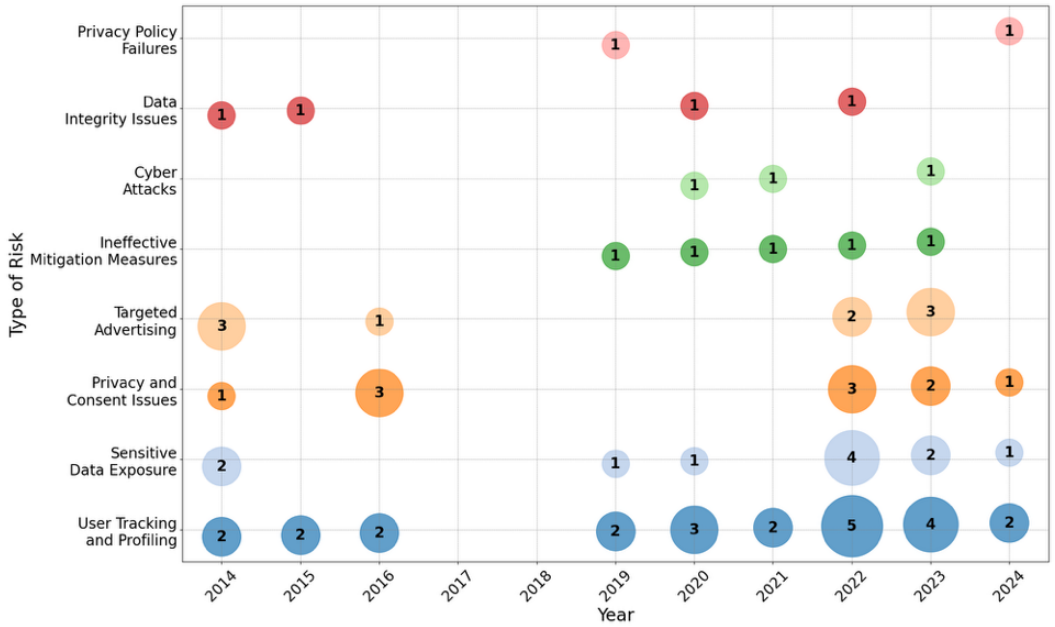

Figure 3. Number of papers mentioning type of risk per year

Table 5. Exploitation techniques

Exploitation technique	Paper references	Total
Cookie tracking (third-party and first-party cookies)	[2], [15], [18], [19], [27], [28], [30], [31]	8
Fingerprinting	[19], [20], [28], [30], [33]	5
Cross-site request forgery (CSRF)	[4], [8], [26], [32]	4
Session Hijacking	[4], [30], [32]	3
HTTP respawning, flash cookie respawning	[28], [33]	2
Cookie synchronization	[18], [20]	2
Cross-site scripting (XSS) attack	[22]	1
CNAME cloaking for cookie sharing	[4]	1
Cross-origin state inference (COSI)	[26]	1
Cookie poisoning and tampering	[32]	1
Man-in-the-middle (MITM) attacks	[32]	1
Navigation-based phishing	[22]	1

With the highest count of papers, eight studies (29.6%) [2], [15], [18], [19], [27], [28], [30], [31], highlighted Cookie Tracking involving either third-party or first-party cookies as the most common exploitation technique where cookies are used to track users across multiple websites. To fully understand cookie tracking, we must first understand first-party and third-party cookies. First-party cookies are used when users visit a website for tasks such as storing login details or items in the shopping cart. Third-party cookies, on the other hand, are set by external domains (*e.g.* advertisers) to track users across websites to build personalization for targeted advertising [31]. As noted by Nikiforakis *et al.* [2], advertisers and analytics organizations can track users' visits to website to identify recurring users and monitor the status of a particular session. Cookie tracking functions when a third party sets a cookie with a unique ID on the user's browser to track the browsing activity every time that third-party services are used, even on different websites [31]. However, privacy tools, ad blockers, and anti-tracking extensions (*e.g.* Privacy Badger and Adblock Plus) are able to block known tracking domains and they can be used to mitigate cookie tracking and cookies [19]. There are some preventive measures mentioned in [25], such as user consent mechanisms, including comprehensive cookie consent tools that have been designed to meet GDPR requirements.

The second most used exploitation technique is fingerprinting, which is a stateless tracking technique that recognizes and tracks users without the browser's storage utilization [38]. For example, when a user visits a webpage with a fingerprinting script, various data points from the user's browser and device can be collected, which consequently form a unique fingerprint that can be used to recognize the user across

different website and sessions [33]. WebGL fingerprinting was mentioned in [19], [30], demonstrating how advanced methods allowed for user tracking without being blocked or detected by conventional cookie management programs. These methods demonstrate how tracking technologies are becoming more complex and the privacy mechanisms in place seem to be inadequate to successfully counteract them [24].

Third, CSRF is another prevalent method which has been studied in four papers (14.8%). In this method, attackers exploit session cookies to trick users into performing unintended actions on authenticated websites [26]. CSRF exploits session cookies by deceiving users into performing unintended actions on authenticated websites such as transferring funds or altering account settings [8], [32]. Takata *et al.* [4] discussed how CSRF attacks manipulate cookies to execute unauthorized activities, while Khodayari and Pellegrino [26] highlight the exploitation of HTTP requests in these attacks. These findings underscore the need for robust anti-CSRF measures, such as a proper configuration of the SameSite attribute [32]. In order to mitigate these risks effectively, the proper implementation of the SameSite attribute can limit the inclusion of cookies in cross-site requests [19].

Next, with a total of three studies that mentioned the cookies exploitation technique, Session hijacking happens when attackers intercept or predict session cookies to impersonate users and gain unauthorized access to accounts [30]. The technique mentioned in [30] utilizes shared resources and timestamps to track and recreate users' browsing history (e.g. the synchronized browsing history of users might be exposed when archived articles are accessed directly). The importance of security flags is highlighted in [4], [32], where the Secure flag will ensure the transmission is sent through a secure SSL channel, improving cookie security. Additionally, cookie synchronization is mentioned in two studies [18], [20]. This technique allows third-party services to share user identifiers across websites, which could build many user profiles. This technique is also called "cookie matching" [18]. It is vital in real-time bidding (RTB) auctions since supply-side platforms (SSPs) and demand-site platforms (DSPs) share user information through this technique. For instance, this happens via HTTP redirects, where the SSP deliver its cookie ID to the DSP, which will connect it with its own cookie ID and identify users [18]. Similarly, HTTP Respawning and Flash Cookie Respawning were discussed in two studies [28], [33]. This technique involves regenerating deleted cookies through HTTP headers or flash local shared objects, undermining user efforts to block or delete cookies. As mentioned in [33], HTTP respawning restores tracking cookies, enabling continued monitoring of user activity even after cookies are cleared.

Subsequentially, another six exploitation techniques from Table 5 were analyzed, and each has one (1) study (3.7%) that mentioned the techniques. First, XSS is a technique that involves the injection of malicious scripts into trusted websites to steal users' cookies or other data [22]. In order to mitigate XSS, Chen *et al.* (2023) [32] suggested turning on the HTTPOnly flag, blocking client-side scripts like JavaScript from accessing the user's cookie. CNAME cloaking for cookie sharing was mentioned in one study [4]. This technique works by disguising third-party cookies as first-party cookies to pass the security mechanisms easily, similar to the SameSite attribute. This allows trackers to exploit and acquire users' sensitive information without authorization.

Furthermore, COSI, which leaks sensitive user information such as login status and account type, was addressed in one study [26]. Chen *et al.* (2023) reported technique known as cookie poisoning and tampering and man-in-the-middle (MITM) attacks [32]. MITM attack is one of the most commonly used methods to damage a system. The attacker will work as an interceptor and manipulator between two users and it usually exploits vulnerabilities in protocols such as the address resolution protocol (ARP) [39]. Lastly, navigation-based phishing was mentioned in one study [22]. This technique happens when attackers are able to trick users into vulnerable websites using meta tags or scripts. This enables them to steal cookies to launch phishing attacks or access user accounts without permission.

To summarize, cookie tracking persists as the most common exploitation method. It is also closely related to the privacy risk of user tracking and profiling, which was the main concern in RQ2. CSRF and fingerprinting demonstrated the evolution of complex exploitation methods that go around conventional cookie protections, while cookie synchronization and hijacking sessions reveal session and cross-domain data management flaws. These results showed the essentials for a development in privacy regulations in order to promote safer environment on the internet. Figure 4 displayed the visualization of exploitation techniques on cookies mentioned in the papers included in our mapping study. Each bubble represents the occurrence or number of papers of a specific technique, in which the larger the bubble reflected the increasing counts. Hence, some techniques, such as cookie tracking and fingerprinting, have received more attention throughout the years. Results also showed that some techniques such as COSI, navigation-based phishing, CNAME cloaking for cookie sharing, cookie poisoning and tampering, XSS attacks, and cookie matching were only mentioned in 1 paper in the duration of 10 years, suggesting a research gap in addressing these vulnerabilities in web environments. The following subsection will discuss the limitations and strengths we had encountered in the research.

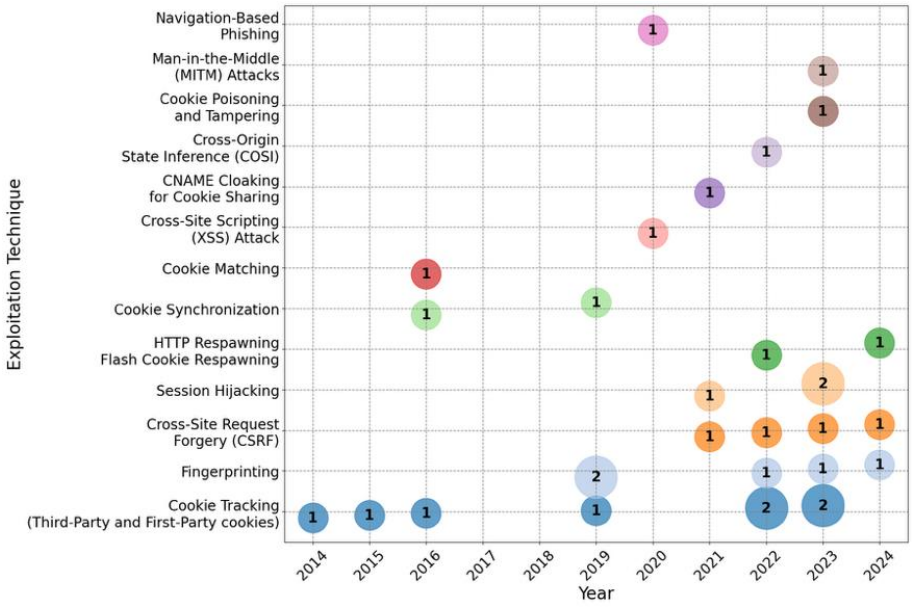

Figure 4. Number of papers mentioning exploitation technique

5. CONCLUSION

This research highlights the pressing need to address the vulnerabilities associated with cookies, particularly those that pose risks to user privacy. While cookies serve useful functions in enhancing user experience, third-party cookies, in particular, raise significant concerns due to their ability to track users across multiple sites. Despite their utility, these cookies often operate without users' full awareness or consent, making them a critical focus for privacy protection efforts. Our survey results revealed that while 68.33% of IIUM students understand the concept of cookies, only 40% are moderately concerned about privacy issues, with a smaller proportion taking effective actions to manage their cookie settings. From the literature review, 88.88% of the studies pointed out user tracking and profiling as the most frequent privacy risk, and the second most frequent risk was sensitive data exposure (40.74%). Although not all papers described the exploitation techniques, this study found several of them: cookie tracking was reported by 29.6% of the papers, fingerprinting by 18.5%, and CSRF attacks by 14.8%, illustrating the complexity and variety of risks.

Trends in research publications demonstrate increased scholarly attention to cookie vulnerabilities, with notable growth since 2019 and a peak in 2022. Thus, it is crucial to improve privacy knowledge, establish more effective rules and regulations, and implement advanced technologies. This paper provides insight in terms of recommendations for future works, highlighting the need to explore advanced exploitation techniques and enhanced cookie management practices. Based on findings from the survey and the mapping study, future work should focus on developing a robust mitigation strategy to address the privacy risks of user tracking and sensitive data exposure, as these were identified as the most important issues in existing research.

ACKNOWLEDGEMENTS

We would like to thank all respondents who participated in our survey conducted in International Islamic University Malaysia.

REFERENCES

[1] A. Cahn, S. Alfeld, P. Barford, and S. Muthukrishnan, "An empirical study of web cookies," in *25th International World Wide Web Conference, WWW 2016*, 2016, pp. 891–901, doi: 10.1145/2872427.2882991.

[2] N. Nikiforakis, G. Acar, and D. Saelinger, "Browse at your own risk," *IEEE Spectrum*, vol. 51, no. 8, pp. 30–35, 2014, doi: 10.1109/MSPEC.2014.6866435.

[3] R. Khandelwal, A. Nayak, H. Harkous, and K. Fawaz, "Automated cookie notice analysis and enforcement," in *32nd USENIX Security Symposium, USENIX Security 2023*, 2023, vol. 2, pp. 1109–1126.

[4] Y. Takata, D. Ito, H. Kumagai, and M. Kamizono, "Risk analysis of cookie sharing by link decoration and CNAME cloaking," *Journal of Information Processing*, vol. 29, pp. 649–656, 2021, doi: 10.2197/IPSJJIP.29.649.

[5] M. Wheeler, S. Saka, and S. Das, "User perception and actions through risk analysis concerning cookies," *arXiv*, 2022,

doi: arXiv:2211.07366.
[6] J. R. Mayer and J. C. Mitchell, "Third-party web tracking: policy and technology," in *2012 IEEE Symposium on Security and Privacy*, May 2012, pp. 413–427, doi: 10.1109/SP.2012.47.
[7] E. Shuford, T. Kavanaugh, B. Ralph, E. Ceesay, and P. Watters, "Measuring personal privacy breaches using third-party trackers," in *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, Sep. 2018, pp. 1615–1618, doi: 10.1109/TrustCom/BigDataSE.2018.00236.
[8] G. P. Bhatraju, C. Vikas, and G. Saranya, "Cookie analysis using web crawling and web scraping," in *Proceedings of the 14th International Conference on Cloud Computing, Data Science and Engineering, Confluence 2024*, 2024, pp. 148–153, doi: 10.1109/Confluence60223.2024.10463260.
[9] O. Pantelic, K. Jovic, and S. Krstovic, "Cookies implementation analysis and the impact on user privacy regarding GDPR and CCPA regulations," *Sustainability (Switzerland)*, vol. 14, no. 9, May 2022, doi: 10.3390/su14095015.
[10] S. O. Migiro and B. a Magangi, "Mixed methods : A review of literature and the future of the new research paradigm," *African Journal of Business Management*, vol. 5, no. 10, pp. 3757–3764, 2011, doi: 10.5897/AJBM09.082.
[11] J. W. Creswell, *Research design : qualitative, quantitative, and mixed methods approaches*, 6th ed. SAGE Publications Inc., 2017.
[12] P. A. Glasow, "Fundamentals of survey research methodology," MITRE, Washington C3 Center, McLean, Virginia, 2005.
[13] N. Salleh, F. Mendes, and E. Mendes, "A systematic mapping study of value-based software engineering," in *Proceedings - 45th Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2019*, Aug. 2019, pp. 404–411, doi: 10.1109/SEAA.2019.00067.
[14] C. Romero-Tris, J. Castellà-Roca, and A. Viejo, "Distributed system for private web search with untrusted partners," *Computer Networks*, vol. 67, pp. 26–42, Jul. 2014, doi: 10.1016/j.comnet.2014.03.022.
[15] A. Aleyasen, O. Starov, A. P. Au, A. Schiffman, and J. Shrager, "On the privacy practices of just plain sites," in *WPES 2015 - Proceedings of the 2015 ACM Workshop on Privacy in the Electronic Society, co-located with CCS 2015*, Oct. 2015, pp. 1–10, doi: 10.1145/2808138.2808140.
[16] H. Marreiros, R. Gomer, M. Vlassopoulos, M. Tonin, and M. C. Schraefel, "Exploring user perceptions of online privacy disclosures," in *Proceedings of the 14th International Conference WWW/Internet 2015*, 2015, pp. 19–26.
[17] D. H. Charbonneau, "Privacy practices of health social networking sites: Implications for privacy and data security in online cancer communities," *CIN - Computers Informatics Nursing*, vol. 34, no. 8, pp. 355–359, 2016, doi: 10.1097/CIN.0000000000000249.
[18] M. A. Bashir, S. Arshad, W. Robertson, and C. Wilson, "Tracing information flows between ad exchanges using retargeted Ads," in *Proceedings of the 25th USENIX Security Symposium*, 2016, pp. 481–496.
[19] S. Ali, T. Osman, M. Mannan, and A. Youssef, "On privacy risks of public Wi-Fi captive portals," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, vol. 11737 LNCS, pp. 80–98, doi: 10.1007/978-3-030-31500-9_6.
[20] P. Vallina, Á. Feal, J. Gamba, N. Vallina-Rodriguez, and A. F. Anta, "Tales from the porn: A comprehensive privacy analysis of the web porn ecosystem," in *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, Oct. 2019, pp. 245–258, doi: 10.1145/3355369.3355583.
[21] R. Bornschein, L. Schmidt, and E. Maier, "The effect of consumers' perceived power and risk in digital information privacy: the example of cookie notices," *Journal of Public Policy and Marketing*, vol. 39, no. 2, pp. 135–154, 2020, doi: 10.1177/0743915620902143.
[22] B. Eriksson and A. Sabelfeld, "AutoNav: evaluation and automatization of web navigation policies," in *The Web Conference 2020 - Proceedings of the World Wide Web Conference, WWW 2020*, 2020, pp. 1320–1331, doi: 10.1145/3366423.3380207.
[23] V. L. Nabbosa, "Me too: value creation by digitalization and data privacy," in *ACM International Conference Proceeding Series*, 2020, pp. 20–24, doi: 10.1145/3404649.3404650.
[24] I. Thomas, "Planning for a cookie-less future: How browser and mobile privacy changes will impact marketing, targeting and analytics," *Applied Marketing Analytics*, vol. 7, no. 1, pp. 6–16, 2021, doi: 10.69554/ejua3389.
[25] G. Reynolds and S. Dowling, "An analysis of Ireland's homecare companies' cookie practices in terms of GDPR compliance," in *2022 Cyber Research Conference - Ireland, Cyber-RCI 2022*, 2022, pp. 1–7, doi: 10.1109/Cyber-RCI55324.2022.10032677.
[26] S. Khodayari and G. Pellegrino, "The state of the SameSite: studying the usage, effectiveness, and adequacy of SameSite cookies," in *Proceedings - IEEE Symposium on Security and Privacy*, 2022, vol. 2022-May, pp. 1590–1607, doi: 10.1109/SP46214.2022.9833637.
[27] A. Berke and D. Calacci, "Privacy limitations of interest-based advertising on the web: a post-mortem empirical analysis of Google's FLoC," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2022, pp. 337–349, doi: 10.1145/3548606.3560626.
[28] D. Bui, B. Tang, and K. G. Shin, "Do opt-outs really opt me out?," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2022, pp. 425–439, doi: 10.1145/3548606.3560574.
[29] N. Waheed, M. Ikram, S. S. Hashmi, X. He, and P. Nanda, "An empirical assessment of security and privacy risks of web-based chatbots," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13724 LNCS, R. Chbeir, H. Huang, F. Silvestri, Y. Manolopoulos, and Y. Zhang, Eds. Springer, Cham, 2022, pp. 325–339.
[30] P. Ioannou and E. Athanasopoulos, "Been Here Already? Detecting Synchronized Browsers in the Wild," in *Proceedings - 8th IEEE European Symposium on Security and Privacy, Euro S and P 2023*, 2023, pp. 913–927, doi: 10.1109/EuroSP57164.2023.00058.
[31] M. S. Alvim, N. Fernandes, A. McIver, and G. H. Nunes, "A quantitative information flow analysis of the topics API," in *WPES 2023 - Proceedings of the 22nd Workshop on Privacy in the Electronic Society*, 2023, pp. 123–127, doi: 10.1145/3603216.3624959.
[32] S. Chen, J. McCracken, K. Lu, T. Wang, and T. Hou, "Taking a look into the cookie jar: a comprehensive study towards the security of web cookies," in *Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2023, pp. 474–479, doi: 10.1145/3565287.3617625.
[33] H. Qayyum, M. Ikram, M. A. Kaafar, and G. Tyson, "Measuring, characterizing, and analyzing the free web games ecosystem," *IEEE Transactions on Games*, vol. 17, no. 1, pp. 88–101, 2025, doi: 10.1109/TG.2024.3383838.
[34] E. Ma and E. Birrell, "Prospective consent: the effect of framing on cookie consent decisions," *Association for Computing Machinery*, New York, NY, USA, 2022, doi: 10.1145/3491101.3519687.
[35] L. M. Coventry, D. Jeske, J. M. Blythe, J. Turland, and P. Briggs, "Personality and social framing in privacy decision-making: A study on cookie acceptance," *Frontiers in Psychology*, vol. 7, no. SEP, 2016, doi: 10.3389/fpsyg.2016.01341.
[36] P. Makakaba, "The supreme court of appeal's judgement on online casino gambling: a means to an end," *International Journal of Private Law*, vol. 7, no. 1, pp. 53–68, 2014, doi: 10.1504/IJPL.2014.059073.

[37] J. S. Park and R. Sandhu, "Secure cookies on the web," *IEEE Internet Computing*, vol. 4, no. 4, pp. 36–44, 2000, doi: 10.1109/4236.865085.
[38] I. Fouad, C. Santos, A. Legout, and N. Bielova, "Did I delete my cookies? Cookies respawning with browser fingerprinting," *arXiv:2105.04381*, 2021.
[39] E. N. Yrlmaz, H. H. Sayan, F. Üstünsoy, S. Gönen, and G. Karacayilmaz, "Cyber security analysis of DoS and MitM attacks against PLCs used in smart grids," in *7th International Istanbul Smart Grids and Cities Congress and Fair, ICSG 2019 - Proceedings*, 2019, pp. 36–40, doi: 10.1109/SGCF.2019.8782313.

BIOGRAPHIES OF AUTHORS

Nor Anisah Amir Hamzah is a final-year Computer Science student specializing in Network and Security at the International Islamic University Malaysia. She is currently working on her final year project, focusing on cookies' vulnerabilities, privacy risks, and exploitation. She can be contacted at email: anisah.amir@live.iium.edu.my.

Anis Safiyyah Adnan is a final-year computer science student specializing in network and security at the International Islamic University Malaysia (IIUM). She is currently working on her final year project, focusing on cookies' vulnerabilities, privacy risks, and exploitation. She can be contacted at email: safiyyah.adnan@live.iium.edu.my.

Norsaremah Salleh is a professor in the Department of Computer Science at the International Islamic University Malaysia. She has over 20 years of academic experience and academic administrative at IIUM. Her research interests include empirical software engineering, and human and social aspects of SE. Salleh holds a PhD in computer science from the University of Auckland, New Zealand. She can be contacted at email: norsaremah@iium.edu.my.