Identification of cloned websites

Srinithi M
126118030
BBA LLB (Hons)

Abstract:

This research paper primarily focuses on the concept of cloned websites and the methods used to identify them. A cloned website is often referred to as a fake website. Typically, cloned websites possess a misleading uniform resource locator, allowing browsers to access them and potentially be misled. Cloned websites often have URLs that closely resemble those of the originals. A URL consists of https:// - the protocol (indicating how the browser should access the resource), for instance, HTTP, HTTPS, or FTP; www.xyz.com, which is the domain name (the website's address); and ?user = 1, a query string (parameter sent to the server). To recognize cloned or impersonating websites, specialized tools are utilized for brand safeguarding, phishing detection, and image comparison. Some common tools include Red Points (which provides automated detection of clones and phishing as well as takedown services), Netcraft (which conducts extensive phishing and brand protection scans), BrandShield (an AI-driven service that monitors for similar domains, replicated web pages, and logos), ZeroFox (which keeps an eye out for domain typosquatting and phishing), and reverse-image tools like TinEye and Google Reverse Image Search that help spot duplicated product images or removed watermarks. These platforms employ HTML/content fingerprinting, domain/WHOIS indicators, image recognition, and automated removal strategies to detect and eliminate cloned websites. Upon discovering a cloned website, the first step is to collect evidence—take screenshots, record the domain, and note timestamps. Next, it's important to notify the hosting provider or domain registrar about the clone and request its immediate removal. Concurrently, it's advisable to inform search engines like Google to have the fraudulent site taken down from their listings. It is recommended to file a complaint with CERT-In (India) or the relevant cybercrime authorities to initiate legal action. Businesses often engage brand protection agencies to accelerate the removal process. Civil or criminal actions may be pursued if there is a violation of intellectual property or trademarks. Continuous monitoring is essential to prevent future occurrences and uphold user trust.

Keywords:

URL, domain name, query string, Red points, watermarks, Netcraft, Brand shield, zero fox, Tin Eye, Google reverse Image search.

Introduction:

In the era of digital globalization, the internet has become the foundation of commerce, communication, and social interaction. However, this rapid technological advancement has also created new avenues for cybercrimes, one of the most deceptive being the cloning of websites. Website cloning refers to the unauthorized replication of a legitimate website's design, content, or code, often with malicious intent to deceive users, steal sensitive data, or damage reputations. Such cloned or fake websites are meticulously crafted to resemble authentic ones, tricking unsuspecting users into believing they are interacting with a genuine source. This practice not only undermines digital trust but also raises serious concerns about data protection, intellectual property rights, and online security. The phenomenon of website cloning has become increasingly prevalent due to the ease of duplicating web content and the widespread use of open-source code. Attackers exploit vulnerabilities in website structures or take advantage of domain similarity—known as "typosquatting"—to host cloned sites that appear nearly identical to

their authentic counterparts. These replicas are often employed in phishing attacks, financial frauds, and identity theft, resulting in severe economic and reputational losses for individuals and organizations. With businesses increasingly relying on digital platforms for their operations, the need to identify and neutralize cloned websites has become an urgent cybersecurity priority. In India, the Information Technology Act, 2000 provides the legal framework to address offences involving cloned websites. Specifically, Section 66 penalizes acts performed dishonestly or fraudulently through electronic means, while Section 75 extends the Act's jurisdiction to offences committed outside India that affect computer systems or networks located within the country. Despite these provisions, enforcing cyber laws across borders remains a challenge due to the lack of international cooperation and the limited scope of Mutual Legal Assistance Treaties (MLATs). Many cloned websites are hosted on foreign servers, complicating evidence collection and prosecution. To combat these challenges, advanced technological tools such as Red Points, Netcraft, BrandShield, and ZeroFox have been developed to detect cloned websites using automated monitoring, AI-based domain analysis, and reverse image recognition. These platforms enable quicker identification and takedown of cloned sites while assisting in evidence collection for legal proceedings. Nonetheless, effective prevention requires a balanced integration of technology, law, and international collaboration. Therefore, this study explores the mechanisms and legal implications of identifying cloned websites, emphasizing the necessity of stronger cyber governance, global cooperation, and awareness to safeguard the digital ecosystem. Through this analysis, the paper aims to highlight the evolving intersection between technology and law in addressing one of the most sophisticated forms of online deception.

Literature Review :

1) Sharma (2020) – "Cross-Border Cyber Jurisdiction: Challenges under Section 75 of IT Act, 2000". Sharma analyzed India's extraterritorial jurisdiction in cyberspace and discussed how lack of MLATs restricts evidence collection from foreign servers.
2) Chatterjee (2021) – "Phishing, Website Cloning and Legal Responses in India". Chatterjee linked website cloning with phishing attacks and discussed Indian cases like Anish Bajaj.
3) Liu & Zhao (2022) – "International Cooperation in Cybercrime Investigations". MLATS agreement improves prosecution of cyber offenders.

Hypothesis Statement:

The effective identification and prosecution of cloned websites under Section 75 of the Information Technology Act, 2000, are significantly hindered by the lack of international cooperation and limited applicability of Mutual Legal Assistance Treaties (MLATs) in cross-border data hosting disputes.

Explanation:

This hypothesis assumes that while India possesses legal provisions for extraterritorial jurisdiction, including Section 75 of the IT Act, their enforcement in cross-border scenarios remains practically weak. The hypothesis will be tested by analyzing cases involving cloned websites hosted on foreign servers, assessing delays or failures in data retrieval, and evaluating the role of MLATs in such cases. It is expected that the study will reveal that jurisdictional conflicts, absence of timely cooperation between countries, and technological loopholes collectively contribute to ineffective cybercrime prosecution. Consequently, strengthening MLAT networks and creating a global cyber law coordination framework could enhance India's ability to identify and penalize offenders responsible for website cloning and other cross-border cybercrimes.

Legal provision of cloned website:

Cloning of a website falls under section 66 of IT Act 2000 which states that If any person , dishonestly or fraudulently does any act, he shall be punished with imprisonment for term which may extend to to three years or with fine which may extend to five lakh rupees or with both.[1]

Different elements of cloning of website :

Website cloning fundamentally involves producing a duplicate, frequently a closely resembling version, of a current website. This duplication can focus on different elements:

Design Duplication: Reproducing the visual arrangement, color palette, font styles, graphic components, and general appearance and atmosphere.

Content Duplication: Reproducing text, articles, blog entries, images, videos, product narratives, or other written or visual content.

Functionality Duplication: Reproducing particular characteristics, engaging components, user processes, or even foundational business principles.

Code Duplication: Directly replicating the source code (HTML, CSS, JavaScript, backend scripts such as PHP or Python) that drives the website.

It's essential to differentiate cloning from simply taking inspiration. Examining rivals or appreciating a website's layout for inspiration is common practice. Cloning, on the other hand, entails directly reproducing or generating a replica so alike that it is nearly indistinguishable or obviously derived without permission. Malicious cloning, commonly employed in phishing, seeks to achieve exact replication to mislead users.[2]

The process of duplicating websites and the simplicity of replication :

As your website achieves greater success, its visibility increases, drawing in a higher amount of traffic. Yet, as your website gains popularity, it turns into a key target for harmful individuals looking to take advantage of your brand, reputation, and status, resulting in increased susceptibility to numerous attacks, such as website cloning.

Regrettably, website cloning is sometimes simpler than expected and can happen through multiple approaches.

Here’s a straightforward description of how it occurs:

Duplicating code: Numerous websites utilize open-source code, allowing individuals to easily access and replicate it. With fundamental coding skills, an individual can recreate the layout and design of your website.

Content scraping: As we are aware, certain tools can automatically extract content from websites. These tools are capable of duplicating text, images, and other media from a specific website and displaying them in other locations.

Website downloading: There are applications available that enable users to download complete websites for offline access. Though this can serve valid needs, it also facilitates cloning by offering an easy method to duplicate a website's layout and material.

Domain hijacking and cybersquatting: Occasionally, attackers might unlawfully acquire a website's domain name or register a closely resembling domain name to impersonate the authentic site. This can enable website duplication by offering a foundation for the duplicated site to function.

The simplicity of duplicating websites is exacerbated by weak security protocols, obsolete software, and flaws in website platforms. Furthermore, these worsen the issue by facilitating deception of visitors and exploitation of brands by attackers.[3]

[1] https://share.google/wfzwi2c1OgoGF0XKP

[2] https://webxloo.com/blog/cloned-website-understanding-the-benefits-pitfalls-and-critical-legal-issues-2025-guide.html

[3] https://www.smartprotection.com/articles/my-website-was-cloned-what-can-i-do-about-it

Who could be responsible for website cloning and what are their motivations?
The individuals responsible for website cloning can differ, but they typically belong to a few groups:
Fraudsters: Fraudsters and online criminals might replicate your website to deceive users into sharing personal or financial details.
Cybercriminals: Cybercriminals might replicate a website to spread malware or participate in phishing schemes.
Competitors: While it is less common, rivals might replicate a website to capture traffic, customers, or concepts.[4]

Eliminate a duplicated website in 4 Steps

If you discover that your website has been duplicated, follow these steps:
Verify that the site is truly a replica of yours. Here are a few suggestions:
Identify resemblances in design, content, arrangement, and features. Focus on specifics like the logo, branding components, written content, visuals, and navigation bars.
Examine URLs, page titles, meta descriptions, and additional metadata for any inconsistencies or indications of alteration.
Examine earlier iterations of your website alongside the alleged copy.Collect proof, recording the resemblances between the clone and your site. Capture screenshots or recordings of both your original site and the replicated version, emphasizing the similarities.Create a comprehensive report detailing the exact components that have been replicated or mimicked without permission.Maintain documentation of any past encounters with the alleged infringer or occurrences of intellectual property violations.Reach out to the hosting provider, notify them about the duplicated website, and ask for its deletion. Here's a method to achieve this:
Determine the hosting provider of the cloned site by conducting a WHOIS lookup or utilizing online tools.
Compose a formal grievance or removal request directed to the hosting provider. Present definitive proof of the cloning and clarify how it infringes upon your intellectual property rights.
Incorporate pertinent legal citations like the Digital Millennium Copyright Act (DMCA) or relevant intellectual property regulations in your area.
Send the complaint via the hosting provider's specified methods, which can consist of online forms, email, or postal mail.[5]

Website cloning Techniques :
Reverse Engineering and Code Duplication: Attackers can analyze and duplicate website code in order to create a copycat site. This cloned site is then used to deceive visitors, steal information or distribute malware.
Content. Reproduction: Content scraping involves automatically extracting information from websites. Attackers use this scraped content to create cloned sites that appear genuine but are actually controlled by them.
Content Management System (CMS) Cloning: Some attackers employ tools that allow them to clone websites built on CMS platforms. These cloned sites serve as channels for phishing attempts, fraud or other malicious activity.[6]

Instances of Actual Cyber-attacks Related to Cloning:
Spear phishing attacks frequently utilize imitation emails that focus on specific individuals or organizations.
Cybercriminals design imitation websites that closely mirror banking sites, resulting in financial deception.

[4] https://www.ccslearningacademy.com/what-is-cloning-in-cybersecurity/
[5] https://www.ccslearningacademy.com/what-is-cloning-in-cybersecurity/

[6] https://www.ccslearningacademy.com/what-is-cloning-in-cybersecurity/

Concealed malware is frequently spread via applications, which compromise users' devices.[7]

Safeguarding Your Business Against Cloning Attacks:
Deploy Strong Security Protocols: Utilize firewalls, encryption methods, and additional strong security tools to enhance your protection against cloning efforts.
Train Employees: Consistently offer training sessions on the dangers of cloning and methods to avert it. This will enable your employees to recognize threats and react appropriately.
Observe and React: Ongoing surveillance and a clearly outlined incident response strategy can aid in quickly identifying and addressing cloning attacks.[8]

Addressing Cloning Incidents: Response Actions and Recovery Steps:
During a cloning attack, it is vital to react swiftly. Organizations ought to possess an incident response plan that includes the following steps:
Recognition and Evaluation: Rapidly determine the type and extent of the assault.
Containment and Elimination: Seclude impacted systems and eliminate harmful components.
Recovery and Reinstatement: Reestablish impacted systems and adopt further security protocols to avert future assaults.
Reporting and Compliance: Adhere to legal and regulatory obligations, including informing impacted individuals when needed.[9]

Dangers and Outcomes:
Within the field of cybersecurity, the dangers linked to cloning are extensive and complex. The repercussions of cloning can be serious and harmful, ranging from unauthorized access to financial deceit.
Here's a summary of several main risks:
Unauthorized Access to Systems and Networks: Cloning enables individuals to circumvent security protocols and infiltrate systems and networks, leading to data leaks and other negative consequences.
Data Breaches and Privacy Violations: Replicated identities or gadgets might be employed to capture information, resulting in data breaches and privacy violations. Confidential, financial, or business information could be at risk.
Deceptive Actions and Monetary Damages: Cloning can enable various activities, including credit card fraud, identity theft, or corporate intelligence theft. Such actions may lead to losses for both individuals and organizations.[10]

The Function of Cloning in Cyber-attacks:
Perpetrators utilize cloning as a method to trick, influence, and take advantage of weaknesses. Cloning serves a multifaceted purpose in cyber attacks, whether it entails duplicating a device to capture communications or replicating an email for phishing schemes.[11]

Tactics Employed by Cybercriminals to Avoid Detection:
They utilize cloning methods to replicate entities, complicating the detection of their actions.

[7] https://www.ccslearningacademy.com/what-is-cloning-in-cybersecurity/
[8] https://www.ccslearningacademy.com/what-is-cloning-in-cybersecurity/

[9] https://www.ccslearningacademy.com/what-is-cloning-in-cybersecurity/
[10] https://www.ccslearningacademy.com/what-is-cloning-in-cybersecurity/
[11] https://www.ccslearningacademy.com/what-is-cloning-in-cybersecurity/

These offenders persistently. Advance their cloning techniques to remain a step ahead of security protocols and detection systems.
They merge cloning with attack vectors to develop complex cyber assaults.

Preventive Strategies and Optimal Techniques:
In the continuing struggle against cloning and various cybersecurity risks, it is crucial to embrace proactive and watchful measures.
Here are several essential measures that both individuals and organizations can implement to improve their security stance:
Consistently refresh software and security systems to guarantee they possess the necessary protections.
Be careful with emails and links from unknown sources.
Employ multi-factor authentication as an additional security measure to prevent unauthorized access.

Enhanced Safeguards and Tactics to Combat Cloning:
To improve protection against cloning attacks, it is recommended to implement the following strategies.
Deploy security measures like intrusion detection systems and threat intelligence platforms.
Work closely with cybersecurity specialists who can evaluate your weaknesses and apply tailored security solutions.
Inform both staff and users about the dangers linked to cloning, promoting a culture of awareness in your organization.
Acknowledge the contribution of cybersecurity experts and services in detecting, reducing, and averting cloning attacks. Their knowledge enables them to create customized security plans that effectively address the threats associated with cloning.
Utilizing these strategies can greatly enhance your protection against cloning attacks while fostering a supportive atmosphere for your organization[12]

The Research problem:

Many online platforms and cloud service providers host data in multiple jurisdictions. On the occurrence of an alleged act, there is always an ambiguity in the principle of comity of nations and conflict of laws to crossborder data hosting disputes in the regime of IT Act 2000.

The preceding statement is detailed in Section 75, which applies to individuals who have committed offenses outside India, regardless of their nationality, when the act of the offense involves a computer system, computer, or computer network located within India. Given that the offense committed by an individual, regardless of nationality, involves a cloned computer, computer system, or computer network, this pertains to a website on a foreign server. Consequently, numerous cloned websites are located on foreign servers. The implementation of section 75 to detect cloned websites concerning foreign servers is restricted due to insufficient international collaboration, as numerous countries lack cybercrime cooperation treaties like MLATs. Consequently, Indian authorities are unable to retrieve data from foreign servers such as IP logs or server details. Hence, this complicates the process of penalizing the offenders.

[12] https://www.ccslearningacademy.com/what-is-cloning-in-cybersecurity/

Avnish Bajaj v State (NCT Of Delhi) 2005 Bazee.com case[13]

Facts :

A video clip of obscene material was listed for sale on Bazee.com by a foreign server located in the US, Bazee.com is an Indian e-commerce platform.

Issue:

Whether Indian courts could take action when severe and part of operation . were outside India.

Court observation:

Collecting evidence and tracing data from US based servers required international cooperation which was slow and limited. The website 's server is abroad; the offence affects Indian users and thus falls under Indian Jurisdiction.

Court Judgement:

As the cloned website is made by an offender of Foreign Server which affected the Indian server therefore, the offender is liable for the offence of cyber crime under section 75 of ITAct 2000.

S.M.C. Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra (Delhi High Court, 2002)[14]

Facts:

The defendant, an employee of S.M.C. Pneumatics, sent defamatory, obscene, and abusive emails to the company and its associates.These emails were sent from a location outside India, but they affected the reputation and functioning of the company within India.The issue was whether Indian courts had jurisdiction when the origin of the communication was outside India.

Issue:

Whether the Indian courts could assume jurisdiction for an act committed outside India (cross-border electronic communication), under the provisions of the IT Act, 2000 — specifically Section 75?

Court's Observation:

The Delhi High Court recognized that cyber defamation or offences committed through electronic means have extraterritorial effects.

The Court emphasized that since the harm and impact of the act occurred within India, Indian courts could rightly assume jurisdiction.

The decision was guided by Section 75 of the IT Act, 2000, which empowers Indian law to apply to offences involving computer systems located in India.

Judgment:

The Court granted an injunction restraining the defendant from sending such emails or making defamatory statements online.

This became one of the first Indian cases recognizing extraterritorial jurisdiction under the IT Act, 2000.

[13] (2005) 3 CompLJ 364 (Del).

[14] (2002) 108 DLT 659 (Delhi High Court)

Suggestions:

1. Strengthen International Cooperation Mechanisms:

India should actively negotiate and expand Mutual Legal Assistance Treaties (MLATs) and bilateral data-sharing agreements to identify the cloned websites from foreign servers.

2. Enhance Enforcement under Section 75 of the IT Act, 2000:

The government must update procedural frameworks and jurisdictional guidelines to ensure effective extraterritorial application of Section 75 in cyber offences involving cloned websites.

3. Use Softwares:

Encourage the adoption of AI-based detection tools such as Red Points, Netcraft, and BrandShield for identifying cloned or fraudulent websites through automated content and domain analysis.

Conclusion:

Website cloning represents one of the most alarming forms of cybercrime, posing risks to both individuals and organizations. With the globalized nature of cloud computing, data and servers are often distributed across multiple jurisdictions, creating serious enforcement challenges. The Indian legal framework, particularly Section 75 of the IT Act, 2000, aims to provide extraterritorial jurisdiction to address offences committed outside India that affect systems within the country. However, the practical enforcement of this section remains limited due to jurisdictional ambiguity and lack of effective international cooperation. Case laws such as Avnish Bajaj v. State (NCT of Delhi, 2005) and S.M.C. Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra (2002) illustrates the judiciary's evolving stance on cyber offences with cross-border implications. In both cases, the courts recognized the principle that if the impact of an offence occurs in India, Indian courts have jurisdiction. Despite this recognition, enforcement agencies face obstacles in gathering digital evidence located on foreign servers because not all nations are signatories to Mutual Legal Assistance Treaties (MLATs). This leads to delays and gaps in investigation and prosecution.The identification of cloned websites today largely depends on advanced technological tools such as Red Points, Netcraft, and BrandShield, which use AI-driven detection techniques. Yet, technology alone cannot replace strong legal collaboration. Hence, strengthening India's international cybercrime cooperation mechanisms, establishing direct data-sharing agreements, and modernizing Section 75 enforcement procedures are crucial. A combination of technological vigilance, legal modernization, and cross-border alliances will ensure that offenders cannot escape liability merely because of jurisdictional limitations. Therefore, the future of cyber law enforcement must rest on a harmonized international legal ecosystem supported by technological precision.