Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.19147971 **JSTE-10**

INVESTIGATION OF WEB ATTACK VULNERABILITIES MAN IN THE MIDDLE AND SESSION HIJACKING

[#1]J. SRINIVAS, ***Assistant Professor,***
[#2]AILAPURAM AKASH, ***B.Tech Student,***
[#3]GONE DHANUNJAY, ***B.Tech Student,***
[#4]BAKI VARUN, ***B.Tech Student,***
[#5]MOHAMMAD SHAHROZ KHAN, ***B.Tech Student,***
Department of Computer Science And Engineering,
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.

ABSTRACT: The online infrastructure is at risk from flaws in web security. Session hijacking and man-in-the-middle (MITM) assaults are two of the most dangerous dangers. Man-in-the-middle tactics enable attackers to intercept user-website conversations and manipulate or pilfer data. Attackers can gain access to another user's session and carry out harmful operations by using login tokens. The inquiry looks into the consequences, risks, and functionality of online apps. Many security techniques, including intrusion detection systems, private session management, and encryption, are now being investigated. Real-world case studies are used to demonstrate the issues and solutions. To improve safety procedures, a thorough understanding of these risks is required. The investigation focuses mostly on self-governing security systems. The principal aim of the research years will be to improve security by applying artificial intelligence.

Keywords:Web Security, Man-in-the-Middle (MITM) Attack, Session Hijacking, Cybersecurity ThreatsEncryption, Intrusion Detection

1. INTRODUCTION

The rapid expansion of web services has led to an increase in the number of online dangers. Because of this, maintaining internet security is crucial. Two of the most dangerous forms of cyberattack are session hacking and man-in-the-middle attacks (MITM). Because of holes in the identification and security measures of the network, attackers are able to steal or alter sensitive data for their personal benefit.Ensuring the safety of online activities and developing effective countermeasures requires a thorough understanding of these hazards.

It is called a "man-in-the-middle" attack when someone listens in on two parties' conversations without their knowledge or consent. Cybercriminals can hijack financial schemes and data breaches by eavesdropping on conversations, altering them, or inserting harmful content into online exchanges. Public Wi-Fi networks that fail to adhere to encryption standards are among the networks that are most commonly targeted by these types of assaults.

Another major hole in web security is session hijacking, which allows cybercriminals to take over a user's live experience. The most typical method that hackers employ for this is by obtaining verification codes or session cookies. This is due to the fact that without knowledge of the login credentials, hackers can utilize these approaches to access user accounts. This

This is an open access article under the creative commons license https://creativecommons.org/licenses/by-nc-nd/4.0/

attack is more likely to target websites that do not employ robust session management mechanisms, such as ensuring secure cookies and letting tokens expire.

To ensure the security of data while it is being transmitted, businesses should use strong encryption methods, such as Transport Layer Security (TLS). Some secure login methods that might reduce the likelihood of an unauthorized user accessing the system include multi-factor authentication (MFA) and secure cookie features. Implementing intrusion detection systems (IDS) and performing regular security audits can help network administrators identify and resolve potential security problems.

This paper examines the inner workings of session hacking and man-in-the-middle attacks, their effects, and methods for preventing them. The project intends to propose ways to make the internet safer by analyzing real-world scenarios and the best security procedures. To better defend against these new dangers, cybersecurity can benefit from future innovations like blockchain-based authentication and AI-driven threat tracking.

Mechanism of Session

Hijacking Session Creation and Initialization: The computer generates a new user ID whenever a user accesses a web application. This user ID is associated with the user's past experiences. For the most part, the session ID is stored in session cookies, which are tiny files that are transmitted from the server and saved in the user's browser.

Session Identification: Each time a user makes a request to the server while interacting with their preferred web app, their machine will transmit the session cookie back to the server. The server will use this session ID to keep track of the user's progress as they move between various tasks or websites.

Interception of Session Data:A malevolent actor can hijack a user's session on the internet the moment they link their computer to a website. A variety of methods, including packet eavesdropping, Man in the Middle attacks, and cross-site scripting (XSS), can be employed to gain access to the link.

Session Impersonation: Anyone can impersonate the intended recipient of data if they have access to a session cookie or session ID. Once an attacker gains unauthorized access to a victim's account, they can log the user's session by making requests using a stolen session ID.

Unauthorized Actions: Attackers will impersonate legitimate users once they obtain their login details. Someone could be able to access sensitive information, alter account settings, initiate financial transactions, or even steal one's identity in some cases.

Covering Tracks: Some malevolent actors, after committing an act, will take further measures to avoid detection, such as logging the user out of their session or destroying it.

2. REVIEW OF LITERATURE

Ravie Lakshmanan2025: When it comes to secure networking, the OpenSSH suite of tools has two holes that must be filled. Active denial-of-service (DoS) and Man-in-the-Middle (MitM) attacks can be launched using these vulnerabilities if specific criteria are satisfied. In order to draw attention to the potential risks that OpenSSH client versions 6.8p1 through 9.9p1 may present, particularly with the VerifyHostKeyDNS option enabled, the Qualys Threat Research Unit (TRU) discovered these vulnerabilities. With this function, bad guys can pose as trustworthy servers while the client is online.

This is an open access article under the creative commons license https://creativecommons.org/licenses/by-nc-nd/4.0/

Zoran Cekerevac, 2025: In this essay, we talk about man-in-the-middle (MITM) invasions in great length, including topics like how they work, some historical examples, the damage they cause to businesses, and what managers can do to stop them. Not only does the study take a look at the issues plaguing currently used security protocols like Transport Layer Security and Secure Sockets Layer, but it also investigates the Internet as a whole and the challenges in establishing confidence in both directions.

Wil Liam Teng, Kasper Rasmussen2024: This research looks into the Signal protocol, which is widely used to send encrypted data, and how vulnerable it is to active man-in-the-middle assaults. The authors provide an automated, band-independent key testing technique that eliminates the need for user input or the utilization of extraneous channels. To prevent man-in-the-middle attacks, the server monitors key fingerprint changes that occur during ratcheting. A more secure setting for user activities will be the result of these modifications.

Lily Hay Newman2024: From November 2023 to July 2024, the Russian hacking group APT29, alias Cozy Bear, launched many "watering hole" attacks on vulnerable machines that were visiting compromised government websites in Mongolia. Hackers exploited previously patched vulnerabilities in Apple's iOS and Google's Android by taking advantage of holes created by commercial spyware businesses. Patches for these vulnerabilities were already in place. This study's findings demonstrate unethical government actors employing commercial surveillance equipment without a license, and assaults on watering holes continue to make use of advanced exploits.

Shampa Banik, Trapa Banik, S. M. Mostaq Hossain, Sohag Kumar Saha2023: The goal of this research is to evaluate cyber-physical technologies that can detect smart grid network weak spots in real-time. This research delves into the idea that electricity systems could be vulnerable to man-in-the-middle attacks that exploit holes in the Modbus protocol. In order to protect smart grid systems from possible weaknesses, the results are expected to assist individuals in developing effective cybersecurity strategies and remedies.

Fabian Bäumer,2023: Downgrade attacks can be carried out through the Terrapin attack, a cryptographic vulnerability in the SSH protocol, by eavesdropping on messages as they are transmitted. We talk about this defect in this piece. Because the vulnerability alters sequence numbers during feature negotiation, attackers can sneakily insert or remove messages without the service provider or client noticing. The survey results showed that the majority of SSH implementations are out of date, which highlights the urgency of applying security updates immediately.

Hamidreza Fereidouni, The article delves into the implications of the Internet of Things (IoT), specifically highlighting the concept of man-in-the-middle security risks. It investigates the barriers to detection and prevention in IoT networks, the reasons for these incursions, and potential solutions. This study does more than just look at the state of IoT security; it also investigates possible solutions that can improve systems' ability to detect and prevent man-in-the-middle attacks.

Kailash Gogineni, 2022: In this post, we will go over the novel server authentication approach called Verify-Pro. It makes use of a variety of communication protocols. Modifying the system's settings and features dynamically allows Verify-Pro to generate unique fingerprints that can be used to identify information sources. Session hijacking and man-in-

This is an open access article under the creative commons license https://creativecommons.org/licenses/by-nc-nd/4.0/

the-middle attacks are both mitigated by this method. Machine learning ensures robust authentication by augmenting the system with new languages for each request. It has been demonstrated through testing that it can be utilized in real life with minimal more work.

ManeshThankappan, 2022: In this particular instance, investigators are looking into Multi-Channel MITM (MC-MitM) assaults on WPA Wi-Fi networks. Cryptographic downgrades, key reinstallation attacks (KRACK), fragment attacks, and denial of service attacks are among the assaults that have been carried out. Studying IoT-connected systems in particular, the research delves into MC-MitM's potential, the practical challenges of implementing countermeasures, and the many existing defenses. Also included are recommendations regarding the way future studies should go.

Stefano Calzavara, Riccardo Focardi, Niklas Grimm, Matteo Maffei, Mauro Tempesta2020: While session management is essential for online activities, ensuring its security could be challenging. This essay will examine the first security solution developed to safeguard session security on a fundamental model of web applications, with an emphasis on server-side code. To demonstrate the pliability of their type system, the writers examine the session management logic of well-known systems such as HotCRP, Moodle, and phpMyAdmin. Even though programmers are aware of existing security holes, they discover new ones.

3. RELATED WORKS

Several aspects of session hijacking are now being investigated by researchers and security experts. This is because session hijacking is one of the most serious cybersecurity risks. This literature review will include both comparable and dissimilar case studies and conference papers, allowing us to compare and contrast their salient characteristics.

Session security in web applications: Session security issues can only be understood after extensive investigation. When seeking to take over platforms, cybercriminals use complex strategies such as plotting attacks and, if successful, conducting in-depth species research. Although this paper provides a general outline of platform dangers, our essay focuses on specific strategies. An investigation into the phenomenon known as "Reducing Session Hijacking Attacks in Online Banking Systems" is central to this study. This exemplifies the unique issues that arise within the banking sector. By providing a more comprehensive view, this item enhances the previous effort. Advanced techniques like session scheduling, cross-site scripting, and man-in-the-middle assaults are covered. The variety of approaches used by criminals in various contexts is demonstrated by these ways. Research on session management strategies employed by online stores is known as session management in e-commerce. This study does a good job of covering some ground, but our work covers more ground by looking at session hijacking avoidance strategies. The use of encryption software and trained operators is crucial to these tactics. Machine learning and session security can be improved by utilizing it to detect session hacking. Both can be improved in this way. This technical study backs up our claims and demonstrates how important it is to prevent session hijacking by using secure code, encryption, and top-tier machine learning techniques.

Flaws in Assembly Systems: When it comes to assembly systems, Threats and Countermeasures analyses them thoroughly to identify specific issues and potential solutions.

This is an open access article under the creative commons license https://creativecommons.org/licenses/by-nc-nd/4.0/

Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.19147971 **JSTE-10**

We gain a more complete picture and learn more as a result of our research when we merge conference design into bigger conferences on conference abduction.

4. TECHNIQUES OF SESSION HIJACKING

Threats Posed by a Third Party Intermediary (MitM):

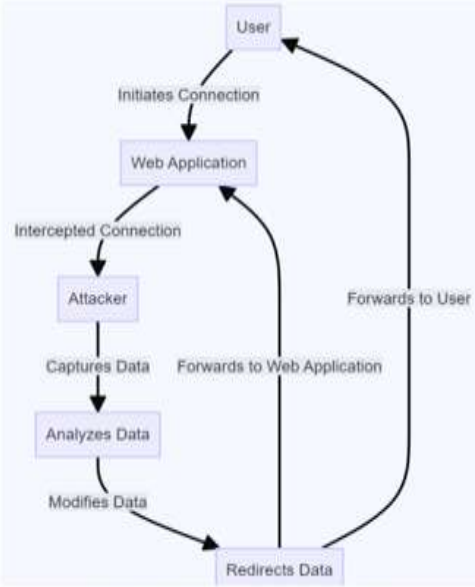

Figure 1: MitM Flowchart

A man-in-the-middle assault can only work if two individuals are listening in on each other's talks. An attacker can prevent session data delivery to a user's server by using fake ARP or DNS records or by monitoring Wi-Fi traffic.

Cross-Site Scripting (XSS):

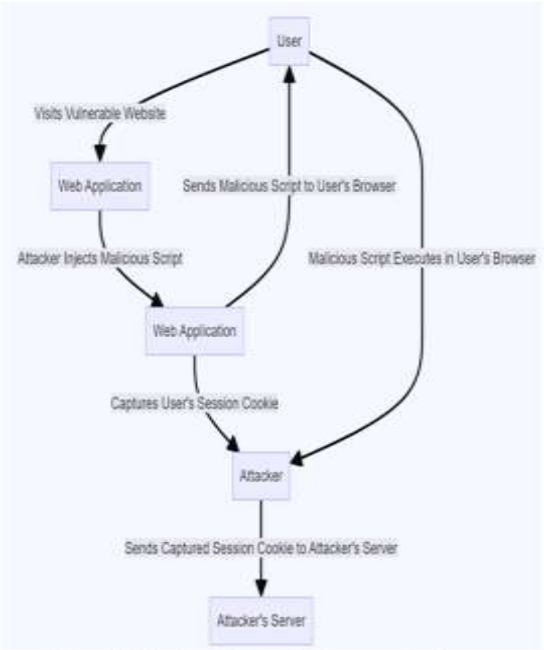

Figure 2:Flowchart of Cross-Site Scripting Attack

This is an open access article under the creative commons license https://creativecommons.org/licenses/by-nc-nd/4.0/

Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.19147971 **JSTE-10**

Users' current web pages could be inadvertently compromised due to the XSS vulnerability. Attackers can steal session cookies and utilize them on other websites the moment a user runs these scripts in their browser.

Session Fixation:

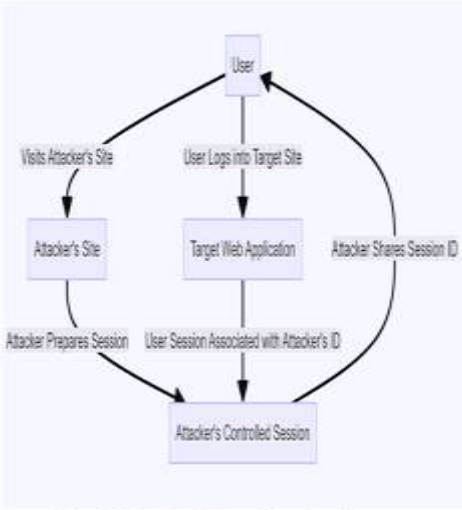

Figure 3:Flowchart of Session Fixation Attack

Once an attacker has guessed the session's subject, they can take control by altering the user's session ID to a known number. This type of assault is known as a session fixation attack. This is a potential consequence of a cyberattack in which a user is deceived into entering a specific session ID.

Consequences of Session Hijacking: Identity theft, unauthorized access to private information, financial loss, and brand damage are all outcomes of session hijacking, a scenario that is extremely detrimental to both people and organizations.

Preventive Measures

Users need to know the hazards of encryption and secure coding approaches in order to prevent session hijacking.

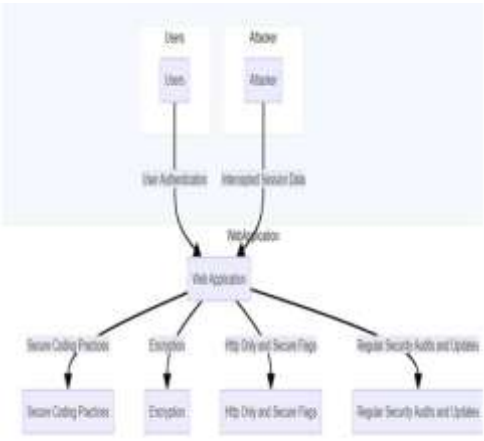

Figure 4:Session Hijacking Preventive Measures

Secure Coding Practice: Developers must adhere to secure coding principles. Some examples of this kind of thinking are secure session management, input validation, and output encoding. One way to reduce risks is to create processes that can handle assembly security on their own.

This is an open access article under the creative commons license https://creativecommons.org/licenses/by-nc-nd/4.0/

Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.19147971 **JSTE-10**

Encryption and HTTPS: Through the use of encryption, HTTPS guarantees that the data transfer remains private as it travels from the user's computer to the website. These SSL/TLS certificates not only protect hackers from accessing links, but they also provide evidence that the host is who they claim to be.

Http Only and Secure Flags: If the "HTTP Only" configuration is in place, session cookies cannot be subjected to an XSS attack. This results in a ban on JavaScript access. Another reason cookies are better than other forms of data transfer is that the secure mark ensures they are sent via encrypted HTTPS connections.

Regular safety audits and updates: To identify potential security holes in the system, security checks are executed often. This way, developers can address them promptly. Making sure all tools, software, and websites are kept up to date is essential for patching the detected security vulnerabilities.

5. CONCLUSION

Attacks like Man-in-the-Middle (MITM) and Session Hijacking have made the internet far less secure. Hackers can eavesdrop on and manipulate user-computer conversations through Man-in-the-Middle (MITM) attacks. Data can be altered or stolen by them. Similar to this, session hijacking is a method of gaining unauthorized access to specific sessions by taking advantage of inadequate security mechanisms. Due to the increase in users of public Wi-Fi networks and the lack of adequate security protocol strengthening, these vulnerabilities are becoming increasingly severe. Protect yourself from these threats by implementing measures such as secure session management, multi-factor authentication, and robust encryption protocols like HTTPS and TLS. To achieve a greater degree of web security, it is necessary to implement strategies for intrusion monitoring, vulnerability assessments, and ongoing security enhancement. Encouraging the usage of VPNs and warning users against connecting to networks they do not trust is another important part of security. In order to safeguard confidential information and online applications, businesses must separately implement robust security protocols. In order to successfully handle emerging cyberthreats, cybersecurity research must be continuous and new approaches must be developed.

REFERENCES

1. Ravie Lakshmanan. (2025). Security vulnerabilities in OpenSSH: Risks of MitM and DoS attacks. Qualys Threat Research Unit Journal.
2. Zoran Cekerevac. (2025). A comprehensive analysis of Man-in-the-Middle (MitM) attacks: Technology, history, and mitigation strategies. Journal of Cybersecurity and Internet Governance.
3. Wil Liam Teng, Kasper Rasmussen. (2024). Mitigating MitM attacks in the Signal protocol through automated key confirmation. Lily Hay Newman. (2024). APT29's watering hole attacks: The proliferation of state-sponsored surveillance exploits. Journal of Advanced Cyber Threats and Intelligence.
4. Shampa Banik, Trapa Banik, S. M. Mostaq Hossain, Sohag Kumar Saha. (2023). MitM attack vulnerabilities in smart grids using Modbus protocol. Journal of Cyber-Physical System Security.

This is an open access article under the creative commons license https://creativecommons.org/licenses/by-nc-nd/4.0/

ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.19147971 **JSTE-10**

5. Fabian Bäumer. (2023). The Terrapin attack: A cryptographic vulnerability in SSH enabling downgrade attacks. Journal of Applied Cryptography and Network Security.
6. Hamidreza Fereidouni, Olga Fadeitcheva, Mehdi Zalai. (2023). MitM attacks in IoT: Causes, challenges, and prevention mechanisms.
7. Kailash Gogineni. (2022). Verify-Pro: A dynamic fingerprinting approach for preventing MitM attacks. Journal of Secure Communication Protocols and Machine Learning Applications.
8. ManeshThankappan. (2022). Multi-Channel MitM (MC-MitM) attacks in WPA Wi-Fi networks: Vulnerabilities and defense strategies. Journal of Wireless Security and Cryptanalysis.
9. Stefano Calzavara, Riccardo Focardi, Niklas Grimm, Matteo Maffei, Mauro Tempesta. (2020). A security type system for enforcing session security in web applications. Journal of Web Application Security and Privacy.

This is an open access article under the creative commons license https://creativecommons.org/licenses/by-nc-nd/4.0/