IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 December 2023, accepted 28 December 2023, date of publication 5 January 2024,
date of current version 16 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3350444

TOPICAL REVIEW

Unveiling Vulnerabilities of Web Attacks Considering Man in the Middle Attack and Session Hijacking

MUTEEB BIN MUZAMMIL[1], MUHAMMAD BILAL[2,3], SAHAR AJMAL[4], SANDILE C. SHONGWE[5], AND YAZEED Y. GHADI[6]

[1]Department of Computing, Riphah International University, Faisalabad Campus, Islamabad 46000, Pakistan
[2]College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China
[3]Faculty of Computer Science and Information Technology, Superior University, Lahore 54000, Pakistan
[4]FAST School of Computing, Department of Software Engineering, National University of Computer and Emerging Sciences, Islamabad, Chiniot-Faisalabad Campus, Chiniot 35400, Pakistan
[5]Department of Mathematical Statistics and Actuarial Science, Faculty of Natural and Agricultural Sciences, University of the Free State, Bloemfontein 9301, South Africa
[6]Department of Computer Science/Software Engineering, Al Ain University, Abu Dhabi, United Arab Emirates

Corresponding author: Muhammad Bilal (mbilal@zju.edu.cn)

The work of Sandile C. Shongwe was supported by the University of the Free State, South Africa.

ABSTRACT The current era extensively utilizes the Internet, which uses data. Due to the apparent open-access Internet service, this data is highly vulnerable to attacks. Data privacy is affected by Web-based attacks. This Systematic Literature Review (SLR) focuses on two Web-based attacks: Man-In-The-Middle and session hijacking. It reviews about 30 studies from the years 2016-2023 that have been selected utilizing a proper study selection procedure. This SLR comprises three research questions. The first describes the overall trends in Man-In-The-Middle attacks and session hijacking studies. It shows that 7 articles were published in 2018, and the trend is decreasing to 4 articles by 2021. Moreover, 73% articles are published in conference venues, and India is the top contributor in this domain. Lastly, this question elaborated that IEEE is the top contributor as a publisher. The second addresses the sorts of attacks used by Man-In-The-Middle attacks and session hijacking on Transmission Control Protocol / Internet Protocol (TCP/IP). This demonstrates that Man-In-The-Middle attacks invade all layers and session hijacking attacks on only two, that is, the application and network layer. The third research question discusses the solutions provided by different studies to deal with Man-In-The-Middle attacks and session hijacking. In conclusion, this analysis highlights the need for stronger cybersecurity measures against Man-in-the-Middle and session hijacking assaults in the Internet era by revealing evolving trends, contributors, and solutions in data privacy.

INDEX TERMS Privacy, Man-In-The-Middle attack, session hijacking, hypertext transfer protocol (HTTP) hijacking.

I. INTRODUCTION

Due to the high Internet use, Web-based applications are widely used [1]. It enables communication among servers and clients through websites [2]. It is an essential part of daily activities in business, studies, banks, shopping marts, etc., to improve the quality of work. The Web is a hub of data repositories that holds private and confidential data of the users [3]. Due to the higher use of the Internet, websites are highly vulnerable. A software code defect, system configuration error, or other weakness in the website or web application or any of its parts and operations is referred to as a vulnerability. These vulnerabilities are distinct from other prevalent categories of vulnerabilities, like those related to networks or assets. They emerge from the necessity for online programs to communicate with numerous users over

The associate editor coordinating the review of this manuscript and approving it for publication was Petros Nicopolitidis.

FIGURE 1. Types of web-based attacks.

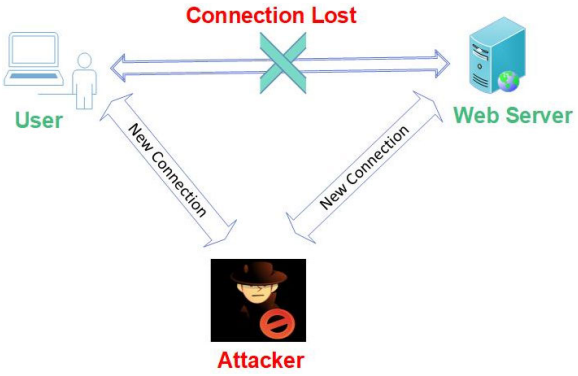


FIGURE 2. Working of Man-in-the-Middle attack.

FIGURE 3. Passive session hijacking state.

various networks, and hackers can readily exploit this degree of accessibility. Attackers can obtain unauthorized access to the organization's systems, procedures, and mission-critical assets through web application vulnerabilities. With this kind of access, attackers can plan attacks, commandeer apps, utilize privilege escalation to steal data, interrupt critical services on a massive scale, and more. Around 42% of websites are affected by cybercrimes [4]. Fig. 1 shows the types of web-based attacks. Packet sniffing is an attack that observes and gathers all the data transactions in the network [5]. SQL injection is a malicious activity that uses unauthorized backend code to access data packets flowing inside the network [6]. Furthermore, cross-site scripting (XSS) changes susceptible websites and compromises the data interaction on that web page [7]. Another attack, named path traversal, allows access to the web servers by navigating the trails of a user to gain access to the data [8]. Spooling is another method to gain access to the data by malicious users at input and output devices, from where data is originated and delivered [9]. Furthermore, Session Hijacking (SH) seizes the whole web session and gathers all the data [10]. Lastly, Man-In-The-Middle (MITM) is a kind of attack in which the attacker overhears the network without permission [11].

When it comes to finding holes in an organization's application security, it's crucial to explore beyond conventional vulnerability scanners because there are web application security solutions made especially for apps. Vulnerability management helps shield a company's brand and financial line from harm by averting data breaches and other security disasters. Vulnerability management can also help with compliance with different security requirements and standards.

Among these web attacks, Man-in-the-middle assaults, phishing, and session hijacking are the most prevalent kinds of online attacks. Man-In-The-Middle (MITM) [11] and session hijacking [10] is a type of invasion that includes an attacker who tries to breach the privacy of the user. The Web-based application depends upon Hypertext Transfer Protocol Secure (HTTPS) to ensure privacy and security during user communication [12]. The communication between users depends upon Transmission Control Protocol / Internet Protocol (TCP/IP) [13]. Even due to heavy security, the attacker finds a way to breach the secrecy of the user.

The MITM is a type of security invasion in which the attacker even drops the communication among users or users with a Web page. This attack occurs between two legally interconnecting hosts that allow the invader to snoop on communication that is not legal to listen [8]. In this attack, the attacker sits between the sender and receiver, thus known as a Man-In-The-Middle attack. It destroys the original connection between the user and the website and creates a new relationship where the attacker continuously overhears each conversation [15]. Fig. 2 shows the MITM attack.

In passive hijacking, the attacker sits inside the network. The attacker then sends the data to users masquerading as legitimate users in the network. Thus, in this way, it hijacks the system [10]. Fig. 3 shows passive session hijacking. In an active hijacking, the attacker attacks the already established session among users [10]. The attacker performs a DOS attack and sniffs the session during that process. In this, the attacker does not invade the connection between the user and the Web page but sniffs their session. Fig. 4 shows active session hijacking. Due to the high rate of attacks in the current era, it is important to discuss Blockchain technology. Blockchain is a kind of shared database that keeps data in blocks connected by cryptography, which sets it apart from conventional databases. It has a wide range of possible uses.

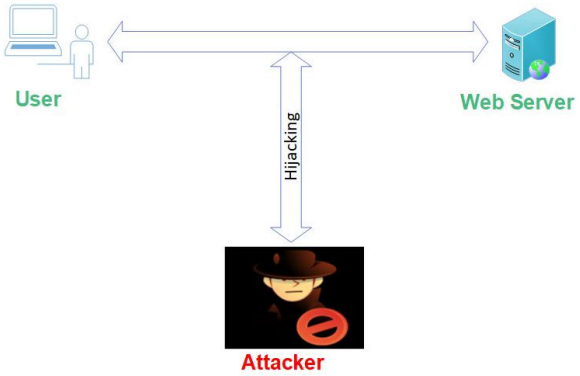


FIGURE 4. Active session hijacking state.

Because it has the power to completely transform financial transactions by facilitating safe, open, and international payments. Ethereum and Bitcoin are two popular examples of cryptocurrencies used for this purpose. Blockchain improves efficiency and transparency in the supply chain by tracking the flow of assets and goods. Self-executing contracts that are coupled with blockchain technology can automate agreements and transactions, reducing costs and eliminating middlemen. This technology speeds up processes like document management and identity verification by providing safe and verifiable digital identities. Blockchain technology protects patient privacy by facilitating easier information sharing between authorized parties and securely handling and storing sensitive healthcare data.

To sum up, this technology has become a revolutionary force that is changing several industries and influencing how people will connect digitally in the future. Because it is secure and decentralized, it has enormous potential to improve transparency, streamline procedures, and build trust in the digital sphere. There is no denying that it can improve security, transparency, and trust. The digital world will probably be shaped by blockchain to a greater extent as technology advances and obstacles are overcome [14], [15], [16].

It is imperative to deploy strong security measures to prevent the dangers associated with web attacks. Many tactics have been documented in different literature studies. Businesses can greatly lessen their susceptibility to MITM attacks, session hijacking, and other web-based risks by putting these tactics into practice and remaining aware of new dangers. We made an effort to gather this information to use it to inform both the development of new techniques to address these online vulnerabilities and the application of these tactics for preventing web attacks, especially Man-in-the-Middle and session hijacking attacks.

This article comprises three research questions that will help identify year-wise distribution, country-wise contribution, publication type, article publishers, the ratio of attacks, and the proposed solution for MITM and session hijacking. We compared Man-In-the-Middle (MITM) and Session Hijacking (SH), Web Accessibility, and SH-MITM variables/parameters from several research studies to manipulate data for our experiment. This quantitative study is carried out methodically using pertinent MITM and session hijacking web assaults. Secondly, we collected information from conference papers and publications. IEEE, ACM, and Science Direct are the primary sources of data. Thirdly, we analyzed the primary vulnerabilities identified in this research, which include phony server links, HTTPS application layers, unauthorized user access, and unexplored upgraded technologies.

II. LITERATURE REVIEW

There are a lot of different surveys conducted in the field of MITM and session hijacking independently, such as a survey on the prevention of session hijacking [2] on Secure Socket Layer / Transport Layer Protocol (SSL/TLP). Its scope is limited to SSL/TLP. Furthermore, another survey discusses the state-of-the-art methodology of session hijacking [10]. This only discusses session hijacking in banking systems. A survey related to MITM attacks [11] shows the classification of attacks and the countermeasures to deal with the attacker. Another review article is performed on MITM in wireless and computing networks [17]. It categorizes the MITM attacks and shows possible prevention methods. Another survey [18] is related to Web accessibility and people with disabilities but does not deal with the issue of security. This paper [19] does not explicitly focus on matters like MITM attacks or session hijacking. Furthermore, another article deals with Web accessibility but does not deal with the security issues of session hijacking and MITM. By analyzing [2], [10], [11], [17], [18], [19], it is extracted that no study focuses on both session hijacking and MITM at a single platform. Table 1 shows the research gap, which identifies a need for SLR that focuses on MITM and Session Hijacking (MITM-SH). This SLR aims to work on a comparison and analysis of SH and MITM collectively.

III. RESEARCH METHODOLOGY

This SLR is based on the guidelines by Kitchenham et al. [20]. A proper mechanism is followed to select the appropriate articles for the SLR. It has 3 phases: planning, guiding, and reporting an SLR [21].

A. PLANNING AN SLR

Planning an SLR is an essential and foremost task. The complete base of SLR depends upon the planning.

1) RECOGNIZING SLR NEED

It is analyzed from studies [2], [10], [11], [17], [18], [19] that there exists a research gap in the comparison of MITM and session hijacking. So, there is a need for a systematic review that discusses and compares MITM with session hijacking.

TABLE 1. Research gap for MITM-SH.

Ref.	Type	Year	SH	MITM	Web Accessibility	MITM-SH with Web Accessibility
[10]	Survey	2016	✓	x	x	x
[11]	Survey	2016	x	✓	x	x
[17]	Survey	2017	x	✓	x	x
[2]	Survey	2018	✓	x	x	x
[18]	Survey	2021	x	x	✓	✓
[19]	Survey	2021	x	x	✓	✓
MITM-SH	SLR	2023	✓	✓	✓	✓

TABLE 2. Research questions for MITM-SH.

ID	Research Questions
RQ1	What are the year-by-year analysis, demographic progress, and publisher details for MITM and session hijacking?
RQ2	Which Layers of TCP/IP are affected by MITM and session hijacking?
RQ3	What are solutions provided by articles to deal with MITM and Session Hijacking?

TABLE 3. Electronic databases for SLR.

ID	Database	URL
ED1	IEEE	https://ieeexplore.ieee.org
ED2	ACM	https://dl.acm.org
ED3	Science Direct	https://www.sciencedirect.com
ED4	MDPI	https://www.mdpi.com

2) IDENTIFYING RESEARCH QUESTIONS

The Research Questions (RQs) are an integral part of an SLR. All the findings and results are based on the RQ. This study focuses on three RQs that are stated in Table 2.

3) SPECIFYING ELECTRONIC DATABASES

The identification and specification of Electronic Databases (ED) are essential because the articles are only extracted from those sources; Table 3 shows the EDs used in this SLR for digging out research articles.

B. GUIDING AN SLR

During the process of SLR, a query is designed that is related to the topic to extract data from specified ED's. The question comprises all the components and meanings to gather information about the domain. The query used for MITM-SH is shown in Fig. 5. The specified query is run on different ED's, elaborated in Table 3. Table 4 shows the format of the question applied to different EDs.

1) STUDY SECTION PROCESS

The article selection procedure comprises four phases. It is a process through which the studies are extracted to perform analysis based on RQs. The first step is the identification phase in which articles are removed based on the query. This SLR focuses on three ED's; their applied query is shown in Table 4. The next process is screening, in which articles are filtered based on title and abstract. Furthermore, eligibility is considered based on quality metrics. Lastly, selected studies

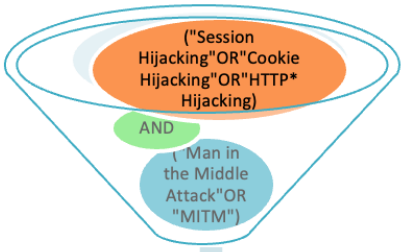


FIGURE 5. Query for MITM-SH.

TABLE 4. Query on different EDs.

ID	ED's	Query
ED1	IEEE	("All Metadata": Man in the Middle Attack OR "All Metadata": MITM) AND ("All Metadata": Session Hijacking OR "All Metadata": Cookie Hijacking OR "All Metadata": HTTP* hijacking)
ED2	ACM	[[All: "man in the middle"] OR [All: "mitm"]] AND [[All: "session hijacking"] OR [All: "cookie hijacking"] OR [All: "HTTP* hijacking"]] AND [Publication Date: (01/01/2016 TO 31/12/2023)]
ED3	Science Direct	("Man in the Middle Attack" OR"MITM") AND ("Session Hijacking" OR "Cookie Hijacking" OR"HTTP hijacking" OR "HTTPS hijacking")
ED4	MDPI	("Man in the Middle Attack" OR"MITM") AND ("Session Hijacking" OR "Cookie Hijacking" OR"HTTP hijacking" OR "HTTPS hijacking")

are elaborated by considering the inclusion-exclusion criteria. The study selection process of MITM-SH is shown in Fig. 6, which shows that the final 30 studies are selected for analysis.

2) FINDING AND SELECTING PRIMARY STUDIES

The identification and screening are the first two phases of the study selection process. In the third phase, the eligibility of selected primary studies is identified, but inclusion, exclusion, and quality criteria are established for this purpose. Based on these criteria, the articles on which SLR will be performed are selected. The inclusion criteria and exclusion criteria are shown in Tables 5 and 6, respectively, whereas the quality evaluation criteria are in Table 7.

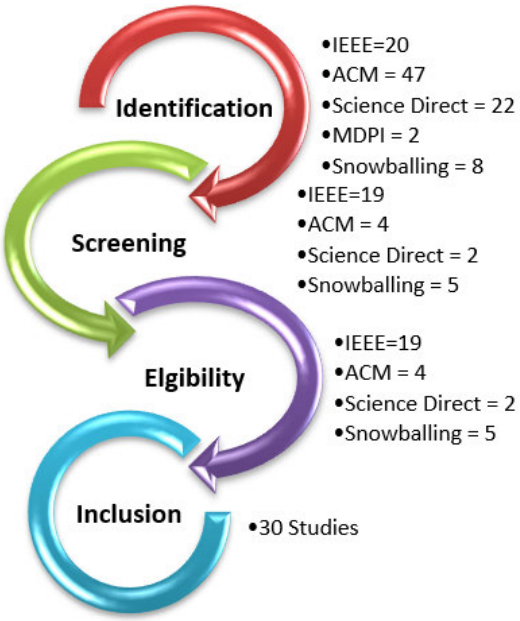


FIGURE 6. Study selection process.

TABLE 5. Inclusion criteria.

ID	Inclusion Criteria
IC1	Articles published in the range of 2016 to 2023.
IC2	Only peer-reviewed articles.
IC3	Articles that complement research questions.
IC4	Only full-text articles should be included.
IC5	In case of improvement in some articles, the latest version should be considered.
IC6	Only conference or journal papers.

TABLE 6. Exclusion criteria.

ID	Exclusion Criteria
EC1	Non-English articles.
EC2	Articles other than conference or journal paper.
EC3	Articles with no validation or results.

TABLE 7. Quality criteria.

ID	Quality Criteria
QC1	Articles should have perfect goals and objectives.
QC2	The article properly demonstrates the experiments.
QC3	Articles that mention the limitations are explicitly declared.

3) EXTRACTION OF DATA

The study selection process of MITM-SH shows that a final 30 studies are extracted on which further procedures will be performed. For this purpose, the data needs to be extracted based on certain factors that will help in answering the research questions. The following are the factors that will be extracted to perform this SLR:

- Year of Publication.
- Country of author or conference.
- Type of publication.
- Publisher.

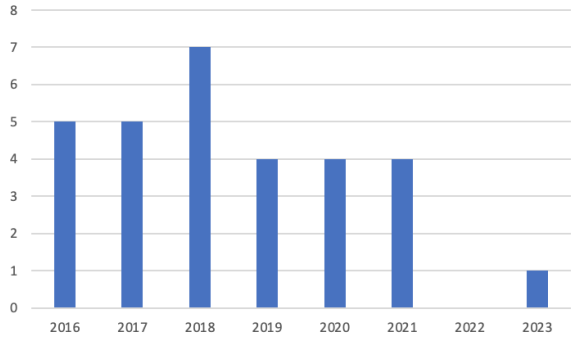


FIGURE 7. Year-wise analysis of MITM-SH.

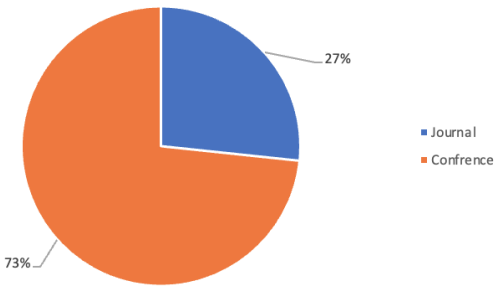


FIGURE 8. Conference vs Journal publication type in MITM-SH.

- Type of Attack.
- Domain of Attack.
- Attack point in the network.
- Countermeasures to attacks.

IV. RESULTS

This section will show the results and answers of each RQ with proper facts and figures in a systematic way. The questions are divided into the following subsections.

A. RESEARCH TRENDS

RQ1: What are the year-by-year analysis, demographic progress, and publisher details for MITM and session hijacking?

This RQ focuses on research trends in the domain of MITM-SH, including publication type, year of publication, country of publication, and publisher details. The complete detail of the selected studies is shown in Table 8. Fig. 7 shows the year of publications. It is analyzed that the research trend of MITM-SH was at its peak in 2018, and 7 articles were published; however, the second peak was in 2016. Lastly, the trend continues with 4 publications in 2021. From facts, it is analyzed that 22 selected articles were conference papers, and 8 were journal papers. Their percentage is shown in Fig. 8. However, the research trend based on geographical facts states that India is the highest contributor to research on MITM-SH with 8 articles. Whereas the United States of America (USA) contributes 6 articles and China contributes 3 articles. This shows that most of the work in the field of MITM-SH is done by Indians. Fig. 9 shows all contributor

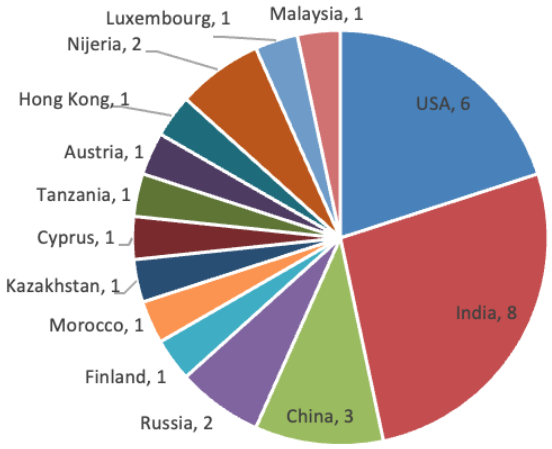


FIGURE 9. Geographical contribution to MITM-SH.

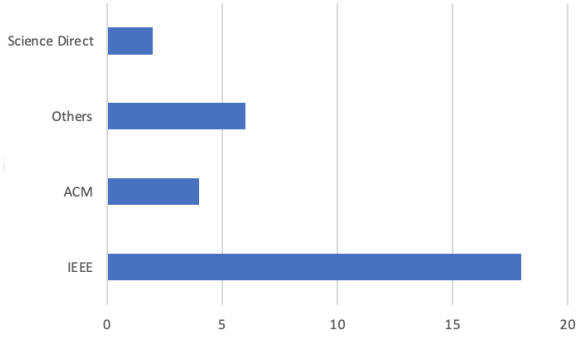


FIGURE 10. Publishers in the field of MITM-SH.

countries in MITM-SH. Lastly, it is analyzed that most of the publishers belong to IEEE, which has 18 publication, whereas ACM provides 4 articles, Science Direct with 2 articles, and the rest are other venues. Fig. 10 shows the analysis of publishers in MITM-SH.

B. AFFECT ON TCP/IP LAYERS

RQ2: Which Layers of TCP/IP are affected by MITM and session hijacking?

The attack by a hacker is performed on some layer of the TCP/IP model, depending upon the nature of the attack. Table 9 shows the summary of articles focusing on MITM and session hijacking. The MITM attack can happen on any TCP/IP model, depending on the attacker's way of exploiting the network [12]. The spoofing-based MITM is an attack in which the attacker bugs the conversation among users and websites without their knowledge [15]. The spoofing includes Domain Name Server (DNS) spoofing, which is an attack on devices that lie between the website and is on the application layer [27], [42], [43], whereas Address Resolution Protocol (ARP) based spoofing is a direct attack to the hand-held devices of users and it attacks data link layer [22], [25], [33], [44]. The Secure Socket Layer / Transport Layer Protocol (SSL/TLS) on MITM is an attack on the transport layer where the attacker involves itself among

TABLE 8. Research trends in MITM-SH.

Ref.	Publisher	Publication Type	Year of Publication	Country
[22]	IEEE	Conference	2018	USA
[23]	IEEE	Conference	2016	India
[24]	IEEE	Conference	2016	Cyprus
[25]	ACM	Conference	2016	USA
[26]	ACM	Conference	2016	USA
[27]	Others	Journal	2016	Hong Kong
[28]	Others	Journal	2016	Nigeria
[29]	IEEE	Conference	2017	USA
[30]	IEEE	Conference	2017	Malaysia
[31]	Science Direct	Conference	2017	India
[32]	IEEE	Conference	2017	Russia
[33]	IEEE	Conference	2017	India
[34]	IEEE	Conference	2018	Russia
[35]	IEEE	Conference	2018	Morocco
[36]	IEEE	Conference	2018	Kazakhstan
[37]	Science Direct	Journal	2018	India
[38]	Others	Journal	2018	India
[39]	IEEE	Conference	2018	Luxembourg
[40]	IEEE	Conference	2019	USA
[41]	IEEE	Journal	2019	China
[42]	Others	Conference	2019	India
[43]	IEEE	Journal	2020	China
[44]	ACM	Conference	2020	USA
[45]	ACM	Conference	2020	Austria
[46]	Others	Journal	2020	Nigeria
[47]	IEEE	Conference	2021	India
[48]	IEEE	Conference	2021	India
[49]	IEEE	Conference	2021	Finland
[50]	IEEE	Conference	2021	Tanzania
[51]	Others	Journal	2023	China

TABLE 9. Categorization of MITM-SH.

Attack Domain	References
MITM	[22], [25], [26], [27], [28], [29], [31], [32], [33], [34], [35], [37], [41], [42], [43], [44], [45]
Session Hijacking	[23], [24], [26], [30], [31], [34], [35], [36], [37], [38], [39], [40], [46], [47], [48], [49], [50], [51]

TABLE 10. MITM-SH attack on TCP/IP model.

References	Attack Type	Attack on TCP/IP Layer
[22]	SSL stripping	Application
[27], [42], [43]	DNS Spoofing	Application
[37],[41]	phishing attack	Transport
[26], [29], [31], [32], [34], [35]	IP Spoofing	Network
[37], [45]	TLS	Network
[28]	BGP	Network
[22], [25], [33], [44]	ARP poisoning	Datalink

browsers and Web servers [22], [28], [37], [45]. It furthermore creates its connection with the user, works as a mediator among user-website links without consent, and sometimes modifies data. The IP spoofing attack occurs on the transport and network layer, where the attacker takes the IP address and delivers data to its autonomous station, where it can be altered [26], [29], [31], [32], [34], [35]. Table 10 shows the summary of MITM attacks on TCP/IP layers. Whereas Fig. 11 shows the categorization of attacks that can occur in the TCP/IP model.

The session hijacking occurs on two layers of TCP/IP only: an application and network layer. In the application

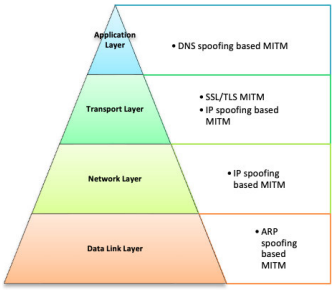


FIGURE 11. MITM types on networking model.

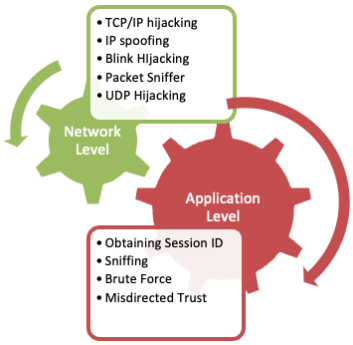


FIGURE 12. Session hijacking types on networking model.

layer, hijacking occurs during the HTTP session when the user gets its ID, whereas in-network layer interception occurs during TCP and User Datagram Protocol (UDP) sessions [48]. Fig. 12 shows the details of the network layer and application-layer attacks.

Following are the hijacking attacks that occur on the network layer.

1) In TCP hijacking, the attacker formulates an environment where the communicating users cannot communicate or share data. The attacker here duplicates the data coming from both ends and thus captures the whole network session [40].
2) The IP spoofing takes the mask of an original user by masking its IP address and communicating over a network, therefore trying to gain access in an unauthorized manner [24], [26], [31], [34], [35], [46].
3) In a packet sniffer, the attacker uses an interface among the users to look at the interchanging data [47].
4) In UDP hijacking, the attacker replies to the UDP request as a legitimate user before the server responds [48].

Following are the hijacking attacks that occur on the application layer.

1) The application-level hijacking obtains the ID of the session through HTTP requests and then exploits it but intimidates other users, thus illegally performing tasks on their behalf [36], [38], [39], [49].
2) Whereas sniffing is the activity of observing and catching the data that are communicating over the network [23].

TABLE 11. Session hijacking attacks on TCP/IP model.

References	Attack Type	Attack on TCP/IP Layer
[23]	HTTP Hijacking	Application
[36], [38], [39], [49]	Application-Level Hijacking	Application
[50]	Brute Force Attack	Application
[51]	Misdirecting Interest	Application
[24], [26], [31], [34], [35], [46]	IP Spoofing	Network
[30]	ARP Spoofing	Network
[31]	IP Spoofing	Network
[37]	Phishing	Network
[40]	TCP Hijacking	Network
[47]	Packet Sniffer	Network
[48]	UDP Hijacking	Network

3) A way to hijack the network is the brute force method in which the hit-and-trial process overtakes login data, encryption keys, and other private information [50].
4) Lastly, misdirecting interest works by diverting users' interest to other websites, thus gaining, and attaining their private information [51].

Table 11 summarizes all the session hijacking attacks that occur on the application and network layer of the TCP/IP model.

A brief comparison between MITM and session hijacking is shown in Table 12.

C. EXPLORING SOLUTIONS FOR MITIGATING ATTACKS

RQ3: What are solutions provided by articles to deal with MITM and Session Hijacking?

MITM and session hijacking are unethical activities that must be mitigated efficiently to secure a network. There are different solutions provided by articles depending upon the nature of the problem. Table 13 shows the types of attacks and their possible solutions.

V. DISCUSSION AND FUTURE DIRECTIONS

There are still many unanswered questions regarding Man-in-the-Middle (MITM) attacks and session hijacking. It is still a key problem to adapt to the ever-changing world of cyber threats, which calls for the creation of dynamic defense mechanisms to fend off novel and sophisticated attack methods. A recurring concern is user knowledge and education regarding the risks involved with MITM attacks and session hijacking, necessitating measures to ensure safe and educated online behavior. The continuous challenge of achieving seamless interoperability amongst varied cybersecurity methods highlights the necessity of integrated defense strategies. Research on privacy-preserving techniques is necessary since it might be difficult to balance increased security with user privacy when developing mitigation solutions. Global cybersecurity initiatives must prioritize the establishment of international coordination and standardized practices for

TABLE 12. Comparison between MITM and session hijacking.

Techniques	Sit between the User and the Web page	Hijack Session from outside	Application Layer	Transport Layer	Network Layer	Datalink Layer
MITM	✓	x	✓	✓	✓	✓
SH	✓	✓	✓	x	✓	x

TABLE 13. Proposed solution of MITM-SH.

References	Solutions/Claims about Solution
[22]	Rerouting of information over the network
[23]	Uses secondary cache system on Internet control management protocol (ICMP) for ensuring a set of IP-MAC.
[24]	Promotes awareness against attacks.
[25]	It is challenging to manage session hijacking and leakage of information in a network.
[26]	Newton's tool identifies stones from Web portals and authenticates them according to the list.
[27]	It uses a combination of SHA-256 hashing and the Elliptic Curve Digital Signature Algorithm (ECDSA) to authenticate the data.
[28]	Identify attacks on a real-time basis using a rule line algorithm on Web-based systems.
[29]	Introduce a co-hijacking monitor in the network.
[30]	Uses auto-detection of attacks based on hashing function for data cataloging to avoid unauthorized access.
[31]	It uses a sum chain algorithm to deal with attacks.
[32]	It uses DNS witch to deal with attacks.
[33]	It uses a DHCP server to detect the attack and prevent the network from being attacked.
[34]	It uses a prototype Software-defined Internet Exchange (SDX) to detect an attack and prevent the network from being attacked.
[35]	It uses a private key in CoMP over the network to deal with attacks over the system.
[36]	It uses local area network security to maintain privacy, integrity, and validation.
[37]	It uses a secure authentication method against attacks by using Bluetooth for authentication.
[38]	It uses a database to control and save the system from attackers.
[39]	It checks the network from endpoints, senses the attack, and mitigates it.
[40]	It detects the attack using the Hidden Markov Model and Linear Regression pointing devices.
[41]	It uses a POX controller to detect and prevent attacks.
[42]	It uses a tool that deals with attacks by analyzing the network traffic.
[43]	It uses shared keys to detect authenticated users and avoid third-party users.
[44]	It uses the HTTPS ecosystem for the mitigation of attacks.
[45]	It uses Hacksaw incorporation with Web applications to deal with attacks and prevent user privacy.
[46]	It uses an online service that saves records from attackers.
[47]	It uses authenticated systems that generate and manage only authenticated users over the network.
[48]	It restricts the cookies so the attacker cannot access the information through the network.
[49]	Promotes awareness against attacks.
[50]	It uses a private key to secure the network communication.
[51]	It uses packet-level features and a trained classifier of machine learning for the detection and prevention of attacks.

reducing MITM attacks and session hijacking. Emerging technologies like artificial intelligence and quantum-resistant encryption present opportunities and challenges that need to be investigated when they are integrated. Furthermore, it is still difficult to handle moral and legal issues in the context of cybersecurity and to choose the right frameworks for looking into and prosecuting offenders. Managing these complex issues demands ongoing investigation, teamwork, and flexibility to successfully combat the changing threat environment. Following can be future directions considering attacks in a network.

A. ADVANCED CRYPTOGRAPHIC PROTOCOLS

To strengthen web systems against Man-in-the-Middle attacks and Session Hijacking, future research can concentrate on creating and implementing advanced cryptographic protocols. Investigating post-quantum cryptography is one way to be resilient to the advances in quantum computing. Furthermore, studies can focus on cutting-edge encryption strategies that surpass conventional approaches and improve communication and data transmission security.

B. BEHAVIORAL ANALYTICS INTEGRATION

Future research into incorporating behavioral analytics into cybersecurity measures is quite promising. Real-time anomalies suggest compromised sessions or unauthorized access can be identified by examining user behavior patterns. To provide an adaptable layer of defense against potential risks related to Man-in-the-Middle assaults and Session Hijacking, research efforts should focus on improving and tailoring behavioral analytics models.

C. MACHINE LEARNING FOR THREAT DETECTION AND PREVENTION

Leveraging machine learning algorithms for dynamic threat detection and prevention is a crucial direction for future research. Systems can autonomously identify patterns and anomalies by training models on historical data related to web attacks, including Man-in-the-Middle incidents and Session Hijacking. This enables the proactive mitigation of threats, enhancing the overall security posture of web applications. Continuous refinement and adaptation of machine learning models will be essential to keep pace with evolving attack strategies.

TABLE 14. Abbreviations.

Abbreviation	Full Form
SLR	Systematic Literature Review
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
TCP/IP	Transfer Control Protocol / Internet Protocol
XSS	Cross-Site Scripting
SQL	Structured Query Language
MITM	Man-In-The-Middle
SH	Session Hijacking
DOS	Denial of Service
ED	Electronic Databases
RQ	Research Questions
IC	Inclusion Criteria
EC	Exclusion Criteria
QC	Quality Criteria
SSL/TLP	Secure Socket Layer / Transport Layer Protocol
MITM-SH	MITM and Session Hijacking
USA	United States of America
IEEE	Institute of Electrical and Electronics Engineers
ACM	Association for Computing Machinery
DNS	Domain Name Server
ARP	Address Resolution Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
ICMP	Internet Control Management Protocol
MAC	Media Access Control Address
ECDSA	Elliptic Curve Digital Signature Algorithm
SDX	Software-defined Internet Exchange
coMP	Coordinated Multipoint Transmission
POX	A Python-based SDN controller platform geared towards research and education

In summary, future directions should encompass machine learning to bolster the resilience of web systems against the ever-evolving challenges posed by Man-in-the-Middle attacks and Session Hijacking [52]. Future research must utilize machine learning algorithms for dynamic threat identification and prevention. Systems can autonomously detect trends and anomalies by training models on past data about web attacks, such as Man-in-the-Middle occurrences and Session Hijacking incidents. This enables proactively mitigating risks, and improving web applications' overall security posture. Machine learning models must be continuously improved and adjusted to stay up with changing assault tactics.

To put it briefly, future directions should investigate more sophisticated cryptography methods, incorporate behavioral analytics for real-time threat detection, and use machine learning to make web systems more resilient to the constantly changing threats posed by Man-in-the-Middle attacks and Session Hijacking.

VI. CONCLUSION

Web-based applications are widely used over the Internet and face different attacks. MITM and session hijacking are two different types of attacks on websites. It is evaluated that the research trend was highest in 2018 with 7 publications; moreover, India is the highest contributor in the domain of MITM-SH with 8 out of 30 articles. Most of the articles are conference papers; 73% of selected publications are conference articles. Furthermore, it is evaluated from the studies that MITM attacks can happen on all the five layers of TCP/IP protocol, whereas session hijacking occurs only on application and network layers. Moreover, in MITM, the attacker sits between the user and the Web portal, whereas, in session hijacking, the attacker only hijacks the system and saves a copy at its place without sitting between the user and the Web page. Lastly, solutions to MITM-SH are provided to detect, prevent, and mitigate the attacks.

APPENDIX

The Table 14 shows the abbreviations shown in the article.

REFERENCES

[1] O. B. Al-Khurafi and M. A. Al-Ahmad, "Survey of web application vulnerability attacks," in *Proc. 4th Int. Conf. Adv. Comput. Sci. Appl. Technol. (ACSAT)*, Dec. 2015, pp. 154–158.

[2] M. S. Hossain, A. Paul, M. H. Islam, and M. Atiquzzaman, "Survey of the protection mechanisms to the SSL-based session hijacking attacks," *Netw. Protocols Algorithms*, vol. 10, no. 1, pp. 83–108, Apr. 2018.

[3] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, "Ethical dilemmas and privacy issues in emerging technologies: A review," *Sensors*, vol. 23, no. 3, p. 1151, Jan. 2023.

[4] H. Corrigan-Gibbs, A. Henzinger, and D. Kogan, "Single-server private information retrieval with sublinear amortized time," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Trondheim, Norway: Springer, 2022, pp. 3–33.

[5] D. Glăvan, C. Răcuciu, R. Moinescu, and S. Eftimie, "Sniffing attacks on computer networks," *Sci. Bull. Mircea cel Batran Naval Academy*, vol. 23, no. 1, pp. 202–207, 2020.

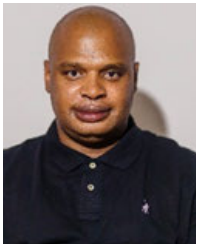
[6] M. Nasereddin, A. ALKhamaiseh, M. Qasaimeh, and R. Al-Qassas, "A systematic review of detection and prevention techniques of SQL injection attacks," *Inf. Secur. J., Global Perspective*, vol. 32, no. 4, pp. 252–265, Jul. 2023.

[7] V. Nithya, S. L. Pandian, and C. Malarvizhi, "A survey on detection and prevention of cross-site scripting attack," *Int. J. Secur. Appl.*, vol. 9, no. 3, pp. 139–152, Mar. 2015.
[8] A. Bernal, O. Parra, and R. Díaz, "Man in the middle attack: Prevention in wireless LAN," *Int. J. Appl. Eng. Res.*, vol. 13, no. 7, pp. 4671–4672, 2018.
[9] H. Fadhil and A. R. Hakim, "Classification model of web application attacks," in *Proc. 6th Int. Workshop Big Data Inf. Secur. (IWBIS)*, Oct. 2021, pp. 87–90.
[10] P. Kamal, "State of the art survey on session hijacking," *Global J. Comput. Sci. Technol.*, vol. 16, no. 1, pp. 39–49, Mar. 2016.
[11] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2027–2051, 3rd Quart., 2016.
[12] D. Glăvan, C. Răcuciu, R. Moinescu, and S. Eftimie, "Man in the middle attack on HTTPS protocol," *Sci. Bull. Mircea cel Batran Naval Academy*, vol. 23, no. 1, pp. 199–201, 2020.
[13] A. A. Mohammadi, R. Hussain, A. Oracevic, S. M. A. R. Kazmi, F. Hussain, M. Aloqaily, and J. Son, "A novel TCP/IP header hijacking attack on SDN," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2022, pp. 1–2.
[14] N. S. Alghamdi and M. A. Khan, "Energy-efficient and blockchain-enabled model for Internet of Things (IoT) in smart cities," *Comput., Mater. Continua*, vol. 66, no. 3, pp. 2509–2524, 2021.
[15] F. Algarni, M. A. Khan, W. Alawad, and N. B. Halima, "P3S: Pertinent privacy-preserving scheme for remotely sensed environmental data in smart cities," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 16, pp. 5905–5918, 2023.
[16] M. A. Khan, "A formal method for privacy-preservation in cognitive smart cities," *Expert Syst.*, vol. 39, no. 5, p. e12855, Jun. 2022.
[17] B. Bhushan, G. Sahoo, and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking—A review," in *Proc. 3rd Int. Conf. Adv. Comput., Commun. Autom. (ICACCA)*, Sep. 2017, pp. 1–6.
[18] T. C. P. B. Pichiliani and E. B. Pizzolato, "Cognitive disabilities and web accessibility: A survey into the Brazilian web development community," *J. Interact. Syst.*, vol. 12, no. 1, pp. 308–327, Dec. 2021.
[19] P. Teixeira, C. Eusébio, and L. Teixeira, "Diversity of web accessibility in tourism: Evidence based on a literature review," *Technol. Disability*, vol. 33, no. 4, pp. 253–272, Nov. 2021.
[20] B. Kitchenham, L. Madeyski, and D. Budgen, "How should software engineering secondary studies include grey material?" *IEEE Trans. Softw. Eng.*, vol. 49, no. 2, pp. 872–882, Feb. 2023.
[21] S. Ajmal and M. B. Muzammil, "PVRS: Publication venue recommendation system a systematic literature review," in *Proc. 5th Int. Conf. Comput. Eng. Design (ICCED)*, Apr. 2019, pp. 1–6.
[22] A. R. Chordiya, S. Majumder, and A. Y. Javaid, "Man-in-the-middle (MITM) attack based hijacking of HTTP traffic using open source tools," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, May 2018, pp. 0438–0443.
[23] D. R. Rupal, D. Satasiya, H. Kumar, and A. Agrawal, "Detection and prevention of ARP poisoning in dynamic IP configuration," in *Proc. IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2016, pp. 1240–1244.
[24] S. Al-Sharif, F. Iqbal, T. Baker, and A. Khattack, "White-hat hacking framework for promoting security awareness," in *Proc. 8th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Nov. 2016, pp. 1–6.
[25] S. Sivakorn, A. D. Keromytis, and J. Polakis, "That's the way the cookie crumbles: Evaluating HTTPS enforcing mechanisms," in *Proc. ACM Workshop Privacy Electron. Soc.*, Oct. 2016, pp. 71–81.
[26] Y. Mundada, N. Feamster, and B. Krishnamurthy, "Half-baked cookies: Hardening cookie-based authentication for the modern web," in *Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, May 2016, pp. 675–685.
[27] M. Alwazzeh, S. Karaman, and M. N. Shamma, "Man in the middle attacks against SSL/TLS: Mitigation and defeat," *J. Cyber Secur. Mobility*, vol. 9, pp. 449–468, 2020.
[28] F. I. Onah, "IP-spoofing vulnerability protection software for data communication network operators," *IUP J. Inf. Technol.*, vol. 12, no. 1, pp. 7–28, 2016.
[29] P. Wang and X. Chen, "Co_Hijacking monitor: Collaborative detecting and locating mechanism for HTTP spectral hijacking," in *Proc. IEEE 15th Int. Conf. Dependable, Autonomic Secure Comput., 15th Int. Conf. Pervasive Intell. Comput., 3rd Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech)*, Nov. 2017, pp. 61–67.
[30] T. Islam, R. F. Olanrewaju, and O. O. Khalifa, "MotionSure: A cloud-based algorithm for detection of injected object in data in motion," in *Proc. IEEE 4th Int. Conf. Smart Instrum., Meas. Appl. (ICSIMA)*, Nov. 2017, pp. 1–6.
[31] A. Krishnan, P. Amritha, and M. Sethumadhavan, "Sum chain based approach against session hijacking in MPTCP," *Proc. Comput. Sci.*, vol. 115, pp. 794–803, Jan. 2017.
[32] A. A. Maksutov, I. A. Cherepanov, and M. S. Alekseev, "Detection and prevention of DNS spoofing attacks," in *Proc. Siberian Symp. Data Sci. Eng. (SSDSE)*, Apr. 2017, pp. 84–87.
[33] N. Tripathi, M. Swarnkar, and N. Hubballi, "DNS spoofing in local networks made easy," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2017, pp. 1–6.
[34] R. R. Brooks, K.-C. Wang, L. Yu, G. Barrineau, Q. Wang, and J. Oakley, "Traffic analysis countermeasures using software-defined Internet exchanges," in *Proc. Int. Sci. Tech. Conf. Mod. Comput. Netw. Technol. (MoNeTeC)*, Oct. 2018, pp. 1–6.
[35] B. Oryema, B. Lee, and J. Park, "Secure mobility management using CoAP in the Internet of Things," in *Proc. IEEE 5th Int. Congr. Inf. Sci. Technol. (CiSt)*, Oct. 2018, pp. 514–524.
[36] Z. Balogh, Š. Koprda, and J. Francisti, "LAN security analysis and design," in *Proc. IEEE 12th Int. Conf. Appl. Inf. Commun. Technol. (AICT)*, Oct. 2018, pp. 1–6.
[37] G. Varshney, M. Misra, and P. Atrey, "Secure authentication scheme to thwart RT MITM, CR MITM and malicious browser extension based phishing attacks," *J. Inf. Secur. Appl.*, vol. 42, pp. 1–17, Oct. 2018.
[38] V. Elamaran, N. Arunkumar, G. V. Babu, V. S. Balaji, J. Gómez, C. Figueroa, and G. Ramirez-González, "Exploring DNS, HTTP, and ICMP response time computations on brain signal/image databases using a packet sniffer tool," *IEEE Access*, vol. 6, pp. 59672–59678, 2018.
[39] F. Araujo, T. Taylor, J. Zhang, and M. Stoecklin, "Cross-stack threat sensing for cyber security and resilience," in *Proc. 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Jun. 2018, pp. 18–21.
[40] M. Levi and I. Hazan, "User profiling using sequential mining over web elements," in *Proc. IEEE 10th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2019, pp. 1–6.
[41] J. Xia, Z. Cai, G. Hu, and M. Xu, "An active defense solution for ARP spoofing in OpenFlow network," *Chin. J. Electron.*, vol. 28, no. 1, pp. 172–178, Jan. 2019.
[42] P. Asrodia and H. Patel, "Network traffic analysis using packet sniffer," *Int. J. Eng. Res. Appl.*, vol. 2, no. 3, pp. 854–856, 2019.
[43] Q. Hu, B. Du, K. Markantonakis, and G. P. Hancke, "A session hijacking attack against a device-assisted physical-layer key agreement," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 691–702, Jan. 2020.
[44] M. Zhang, X. Zheng, K. Shen, Z. Kong, C. Lu, Y. Wang, H. Duan, S. Hao, B. Liu, and M. Yang, "Talking with familiar strangers: An empirical study on HTTPS context confusion attacks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2020, pp. 1939–1952.
[45] P. Shrestha and N. Saxena, "Hacksaw: Biometric-free non-stop web authentication in an emerging world of wearables," in *Proc. 13th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jul. 2020, pp. 13–24.
[46] I. O. Ogundele, A. O. Akinade, and H. O. Alakiri, "Detection and prevention of session hijacking in web application management," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 9, no. 7, pp. 1–10, Jul. 2020.
[47] B. N. Biswas, S. D. Bhitkar, and S. N. Pundkar, "Secure login: A blockchain based web application for identity access management system," in *Proc. 2nd Int. Conf. Emerg. Technol. (INCET)*, May 2021, pp. 1–5.
[48] S. M. Alfassa, S. Nagasundari, and P. B. Honnavalli, "Invasion analysis of smart meter in AMI system," in *Proc. IEEE Mysore Sub Sect. Int. Conf. (MysuruCon)*, Oct. 2021, pp. 831–836.
[49] M. Matsubayashi, T. Koyama, Y. Okano, M. Tanaka, A. Miyajima, Y. Oshima, S. Ukai, T. Wakatsuki, T. Sugashima, and T. Nakamura, "Attacks against UDS on DoIP by exploiting diagnostic communications and their countermeasures," in *Proc. IEEE 93rd Veh. Technol. Conf. (VTC-Spring)*, Apr. 2021, pp. 1–6.
[50] V. O. Nyangaresi, "Lightweight key agreement and authentication protocol for smart homes," in *Proc. IEEE AFRICON*, Sep. 2021, pp. 1–6.
[51] M. Bilal, S. C. Showngwe, A. Bashir, and Y. Y. Ghadi, "Assessing secure OpenID-based EAAA protocol to prevent MITM and phishing attacks in web apps," *Comput., Mater. Continua*, vol. 75, no. 3, pp. 4713–4733, 2023.
[52] M. Bilal, M. Asif, and A. Bashir, "Assessment of secure OpenID-based DAAA protocol for avoiding session hijacking in web applications," *Secur. Commun. Netw.*, vol. 2018, pp. 1–10, Nov. 2018.

MUTEEB BIN MUZAMMIL received the bachelor's degree in computer science from the National University of Computer and Emerging Sciences, in 2018, and the master's degree in computer science from Riphah International University, Faisalabad Campus, Pakistan, in 2023. He has five publications in multiple domains. He is currently working on ERP systems with the IT Department, University of Agriculture Faisalabad. His research interests include recommendation systems, web accessibility, multi-criteria decision-making, and risk analysis.

MUHAMMAD BILAL received the bachelor's degree from the University of Engineering and Technology, Lahore, Pakistan, the master's degree from National Textile University, Faisalabad, Pakistan, and the Ph.D. degree in computer science and technology from Zhejiang University, Hangzhou, China. He is currently an Assistant Professor with the Computer Science and Information Technology Department, Superior University, Faisalabad Campus, Pakistan. He secured the CSC Scholarship for the Ph.D. degree. He has eight years of teaching experience in different institutions. He attended the International Conference on Information Technology: the IoT and Smart in Shanghai, China, and chaired the session. His research interests include web security protocol, computer networks, web accessibility, information systems, and innovation. He was appointed as a Journal Referee for reviewing articles in multiple journals, such as *Computers, Materials and Continua*, IEEE Internet of Things Journal, IEEE Access, and *PeerJ Computer Science*.

SAHAR AJMAL received the bachelor's and master's degrees in computer science from the National University of Computer and Emerging Sciences, Chiniot Faisalabad Campus, Pakistan, in 2016. She worked on compiler construction during the bachelor's degree. She also worked with the Software Engineering and Operation Research (SEOR) Group. As an active association with this group, she has worked as the author of multiple conference papers and journal articles. She provided her teaching services at Riphah International University. She is currently giving teaching services with the Department of Software Engineering, National University of Computer and Emerging Sciences. Her research interests include machine learning, data mining, recommendation systems, and multi-criteria decision-making schemes. She received the Bronze Medal for the master's degree.



SANDILE C. SHONGWE received the B.Sc. (Hons.) and M.Sc. degrees in applied and mathematical statistics from the Faculty of Natural Agricultural Sciences, University of Pretoria. He is currently a Lecturer with the Department of Mathematical Statistics and Actuarial Science, University of the Free State. His current research interests include statistical process monitoring for autocorrelated data, extensive data analysis, optimization models, and support vector machines.

YAZEED Y. GHADI received the Ph.D. degree in electrical and computer engineering from Queensland University. He was a Postdoctoral Researcher with Queensland University. He is currently an Assistant Professor of software engineering with Al Ain University. He has published over 25 peer-reviewed journals and conference papers and holds three pending patents. His current research interests include developing novel electro-acoustic-optic neural interfaces for large-scale and high-resolution electrophysiology and distributed optogenetic stimulation. His dissertation on developing novel hybrid plasmonic photonic on-chip biochemical sensors received the Sigma Xi Best Ph.D. Thesis Award. He was a recipient of several awards.