Physical Education, Health and Social Sciences
https://journal-of-social-education.org
E-ISSN: 2958-5996
P-ISSN: 2958-5988

The Dangers of Public Wi-Fi and Mitigation Strategies: A Comprehensive Analysis

Waqas Ahmad[1] Syed M. Hassan Shah[2,] Uzair Iqbal[3], Zeeshan[4]

[1] CS&IT Department, Sarhad University, Peshawar
[2] CS&IT Department Iqra National University Peshawar
[3] Computer System Engineering, UET, Peshawar
[4] ICS & IT Department the University of Agriculture Peshawar

DOI: https://doi.org/10.63163/jpehss.v4i1.1098

Abstract
The ubiquity of public Wi-Fi in locations such as cafes, airports, and hotels offers significant convenience but simultaneously exposes users to substantial cybersecurity threats. This paper provides a systematic analysis of the security risks inherent in public wireless networks and evaluates the effectiveness of current countermeasures. Employing a methodological approach based on a comprehensive review of contemporary academic research and established cybersecurity frameworks, the study examines a range of vulnerabilities. These include classic threats like packet sniffing, evil twin access points, and man-in-the-middle attacks, as well as more sophisticated techniques such as packet-size side-channel attacks. The analysis of recent empirical studies reveals the severity of these risks, with successful TCP hijacking attacks demonstrated in 93.75% of tested real-world networks, underscoring the urgent need for robust protection. Based on this review, the paper critically assesses the efficacy of key mitigation strategies, including Virtual Private Networks (VPNs), HTTPS adoption, and secure device configurations. The findings culminate in a set of actionable recommendations aimed at enhancing the security posture of public Wi-Fi for both individual users and network providers.

Keywords: Public Wi-Fi security, man-in-the-middle attacks, evil twin, VPN, network encryption, TCP hijacking, cyber security

1. INTRODUCTION:

The deployment of public Wi-Fi has grown exponentially due to the proliferation of mobile devices and the need for continuous internet connectivity. In 2023, roughly 58% of people worldwide used public Wi-Fi services, according to Cisco's Annual Internet Report [1]. As digital transformation picks up speed in both developed and developing nations, usage is expected to increase dramatically. The convenience and perceived need for ubiquitous internet access in modern life are reflected in this widespread adoption.

However, open networks with few authentication barriers the basic architecture that makes public Wi-Fi accessible also introduce inherent security flaws. Malicious actors can intercept communications because public Wi-Fi hotspots often function as shared media where multiple users transmit data across the same radio frequencies, in contrast to private networks that are secured by strong encryption and access controls [2]. A recurring issue in network architecture and user behavior is the conflict between security and accessibility.

Recent warnings issued by significant technology companies and governmental organizations in the United States demonstrate the growing nature of this threat. According to an advisory that was

issued by Google in October 2025, public Wi-Fi networks have been identified as a major attack vector due to the fact that they are not encrypted and are simple to exploit. This puts 94% of Android users at risk from attacks that are based on messaging [3]. In a similar vein, the European Union Agency for Cybersecurity (ENISA) identified public Wi-Fi as a primary concern in its threat landscape assessment for the year 2025. The agency cited evil twin deployments and man-in-the-middle attacks as examples of emerging threats that exploit the inherent vulnerabilities of open wireless networks [4].

The purpose of this paper is to provide a comprehensive analysis of the security risks that are associated with public Wi-Fi and provide an evaluation of the techniques that are based on evidence to mitigate those risks. The purpose of this study is to answer three primary questions: (1) What are the current threat vectors that target users of public Wi-Fi networks? (2) How effective are the defences that are currently in place to protect against these threats against the current situation? as well as (3) What are some helpful recommendations that can be derived from recent research and authoritative guidance?

2. Literature Review

2.1 Historical Context of Wi-Fi Security Evolution

Wi-Fi security has evolved significantly since the introduction of the first wireless encryption standards. Wired Equivalent Privacy (WEP), established in 1999, was the initial attempt to provide confidentiality comparable to wired networks. However, by 2001, researchers had identified fundamental vulnerabilities in the RC4 encryption algorithm used by WEP, demonstrating that encryption keys could be recovered through packet eavesdropping [5]. This discovery initiated a continuous cycle of vulnerability identification and protocol enhancements.

The subsequent standards, namely Wi-Fi Protected Access (WPA), WPA2, and the most recent WPA3, have continued to improve the security of the network through the use of better encryption algorithms and more secure authentication techniques. However, the basic flaw in public Wi-Fi networks still persists, as even the strongest encryption algorithms are unable to counter the potential risks arising from the network structure rather than the algorithms themselves [6].

2.2 Public Wi-Fi Adoption and Risk Perception

The gap between the perceived threat and the actual threat in the context of public Wi-Fi security represents a major challenge. The results obtained from the Pew Research Center indicate that while 81% of adults view public Wi-Fi security as an important concern, 45% still use public Wi-Fi for financial transactions in the last year [7]. The apparent gap between the perceived and actual threat represents the so-called "convenience-security trade-off" in the context of public Wi-Fi security, as discussed by security experts.

The prevalence of the default setting for routers represents another challenge in the context of public Wi-Fi security. According to the results obtained from the survey conducted by the Cybersecurity and Infrastructure Security Agency (CISA) in 2023, only 23% of users change the default passwords for their routers' Wi-Fi, with more than 60% using the default setting indefinitely [8].

Public Wi-Fi networks, while offering convenience, present significant security risks that necessitate a comprehensive understanding and robust mitigation strategies. Research from 2020 to 2026 highlights a continuous evolution of threats, alongside advancements in protective measures. The inherent vulnerabilities of public Wi-Fi, often due to unencrypted or weakly secured connections, make them prime targets for various cyberattacks, including man-in-the-middle (MitM) attacks, the deployment of rogue access points, packet sniffing, malware distribution, and session hijacking [21][22]. Users frequently underestimate these risks, partly due to a lack of awareness and a focus on convenience over security [23][43][22][44].

One of the most prevalent and dangerous threats on public Wi-Fi is the Man-in-the-Middle (MitM) attack [26]. In a MitM attack, an attacker intercepts communication between two parties, often without their knowledge, allowing them to eavesdrop, alter, or inject malicious content into the data stream [26]27]. This can lead to the compromise of sensitive information, such as login credentials, financial details, and personal data [22]. Multi-Channel MitM (MC-MitM) attacks are particularly sophisticated, capable of manipulating encrypted wireless frames between legitimate endpoints [29][28]. These attacks have targeted Wi-Fi networks since 2014, exploiting vulnerabilities like cipher downgrades, denial of service, Key Reinstallation Attacks (KRACK) in 2017, and more recently, FragAttacks in 2021, which impacted millions of Wi-Fi devices, including IoT devices [26][28].

Another critical threat is the "Evil Twin" attack, a specific type of Wi-Fi spoofing where an attacker sets up a malicious access point (AP) that mimics a legitimate one, often by using the same Service Set Identifier (SSID) and MAC address [28][29][29][30]. Unsuspecting users connect to this fake AP, believing it to be a trusted network, thereby granting the attacker full access to their internet traffic [28][32]. This allows for credential stealing, data interception, and the injection of malware [30]. The ubiquity of Wi-Fi has, unfortunately, contributed to a high incidence of such network attacks [34]

The security landscape is further complicated by the rise of advanced persistent threats (APTs) and the increasing sophistication of cyber adversaries [35][36]. Emotet, for example, is a notorious multi-infrastructure botnet that has caused substantial damage through various attack waves [37]. These threats underscore the need for continuous monitoring and adaptive security measures [37]. The increase in internet users and the proliferation of IoT devices have broadened the attack surface, making network security even more critical to protect data integrity and user privacy [39].

Mitigation strategies against these dangers are multifaceted and continuously evolving. One of the primary recommendations for users connecting to public Wi-Fi is the use of Virtual Private Networks (VPNs) [21]. VPNs encrypt all traffic between a user's device and the VPN server, creating a secure tunnel that protects data from interception, even on unsecured networks . This effectively neutralizes the threat of packet sniffing and MitM attacks by making intercepted data unreadable to unauthorized parties. The mandatory use of modern VPNs with post-quantum-ready protocols is increasingly emphasized.

Enforcing HTTPS (Hypertext Transfer Protocol Secure) is another crucial mitigation measure.HTTPS encrypts communication between a user's browser and websites, ensuring that data exchanged remains confidential and untampered. Strict enforcement via HTTP Strict Transport Security (HSTS) and certificate pinning further enhances this protection by ensuring browsers only connect to websites using HTTPS and by preventing fraudulent certificates.

Users can also adopt several self-protective behaviors to enhance their security on public Wi-Fi. These include disabling auto-connect and Wi-Fi auto-join features on their devices, which prevent automatic connection to potentially malicious networks [4]. Maintaining updated operating systems and applications is also vital, as software updates often include security patches for newly discovered vulnerabilities. Using strong, unique passwords for all online accounts and enabling multi-factor authentication (MFA) adds layer of security, even if credentials are compromised. The figure below illustrates a typical phishing attack flow, which can be facilitated by public Wi-Fi vulnerabilities where attackers might redirect users to malicious login pages [33].

For organizations and service providers, implementing robust network security protocols is paramount. Upgrading to the latest Wi-Fi Protected Access (WPA) standards, such as WPA3, is critical [22][32]. WPA3 offers enhanced encryption and authentication mechanisms compared to its predecessors, making it significantly harder for attackers to compromise networks [42]. This includes features like Simultaneous Authentication of Equals (SAE) for stronger password-based

authentication and individualized data encryption [41]. However, even with WPA3, threats like the Evil Twin attack can still be effective if not properly detected [32].

Network segmentation via client isolation can prevent devices connected to the same public Wi-Fi network from directly communicating with each other, thereby limiting the lateral movement of malware or attackers within the network. Adoption of WPA3-Enterprise with 802.1X authentication provides a robust authentication framework suitable for larger networks, such as those found in universities, where each user is authenticated individually against a central server [33].

The concept of zero-trust networking is gaining prominence as a foundational security principle [23]. A zero-trust model assumes that no user, device, or application, whether inside or outside the network perimeter, should be trusted by default [42]. Instead, every access request must be authenticated and authorized, and access privileges are granted based on the principle of least privilege [42]. This architecture significantly reduces the attack surface and enhances resilience against various cyber threats, including APTs [42]. Risk propagation assessment models, particularly those based on ATT&CK frameworks, are being developed to quantify and manage risks within zero-trust networks [42]. The diagram below illustrates a risk assessment framework, which is crucial for managing cyber threats [36].

User education and behavioral cybersecurity frameworks are also vital components of any comprehensive mitigation strategy [23][24]. Raising awareness about the dangers of public Wi-Fi and promoting secure practices can significantly reduce risky user behaviors [23][40][43]. Studies show that fear arousal and coping appraisal can influence users' avoidance behaviors regarding risky Wi-Fi use [43]. Organizations need to provide clear guidelines and training on safe public Wi-Fi usage to their employees and constituents.

Advancements in detection technologies, such as machine learning-based approaches, are proving effective in identifying and mitigating attacks like KRACK and Kr00k in IEEE 802.11 networks [39][38]. Deep learning models are also being applied for computer network cybersecurity monitoring to classify network traffic and detect anomalies [47]. Research is also exploring data mining approaches for Evil Twin attack identification in Wi-Fi networks, aiming to detect these rogue access points based on signal variants and hop counts [31][32].

Despite technological advancements, a significant challenge remains in balancing convenience with security [42][44]. Users often prioritize ease of access over security precautions, leading to risky behaviors [6]. This "false sense of security" can even extend to protected Wi-Fi networks if users rely solely on WPA2/WPA3 without additional layers of protection [45].

In conclusion, the landscape of public Wi-Fi security is dynamic, characterized by increasingly sophisticated threats and continuous efforts in mitigation. A comprehensive approach involves a combination of robust technical measures such as VPN usage, HTTPS enforcement, WPA3 implementation, and zero-trust architectures, alongside continuous user education and advanced threat detection systems. Ongoing research continues to unveil new vulnerabilities and develop more effective countermeasures to safeguard digital communications in an increasingly connected world [34][46][47][48].

2.3 Research Gap

Despite extensive research on individual Wi-Fi security threats, critical gaps persist that leave real-world users vulnerable. First, a knowledge translation chasm exists between cutting-edge academic findings (e.g., the 93.75% success rate of TCP hijacking attacks demonstrated at NDSS 2025 [14]) and practical user guidance, which remains focused on outdated threats. Second, the literature disproportionately emphasizes active external attacks while neglecting systemic "by-design" vulnerabilities, such as deterministic default passwords in 30 out of 44 consumer routers [17] and unencrypted management frames, which place an unfair security burden on end-users. Third, the

"convenience-security paradox" has not been re-examined in light of modern "stealth attacks" that bypass traditional encryption, rendering user perceptions of safety (e.g., "HTTPS protects me") dangerously obsolete. Finally, the field suffers from critical fragmentation: technical, behavioral, and infrastructural analyses remain siloed, with no integrated framework explaining how these factors compound in real-world attacks.

This study is justified by the urgent need to bridge these gaps. It provides the first integrated synthesis of 2025-side-channel research, authoritative cybersecurity frameworks, and behavioral data into a unified threat taxonomy and defense framework. By translating complex technical findings into actionable intelligence for users, providers, and manufacturers, this paper addresses the dangerous disconnect between academic progress and real-world security practice.

3. Threat Taxonomy: Understanding Public Wi-Fi Vulnerabilities

3.1 Man-in-the-Middle Attacks

One of the biggest risks to users of public Wi-Fi is man-in-the-middle (MITM) attacks. An adversary places themselves in the middle of the user and the intended connection point in this attack scenario, intercepting and possibly altering communications without the knowledge of either party [9]. These attacks are made easier by wireless networks' shared medium, which allows any device within range to receive data packets sent over the air.

When a user connects to a legitimate public Wi-Fi network, their device transmits data to the access point, which then relays it to the intended destination on the internet. By intercepting this transmission, the attacker establishes distinct connections to both the user and the legitimate network, relaying messages between them in a man-in-the-middle attack. This configuration enables the attacker to access private communications, financial data, and login credentials [2].

3.2 Evil Twin Attacks

An advanced variant of the Man-in-the-Middle (MITM) attack is known as an "evil twin" attack. In this scenario, the attacker establishes a counterfeit access point that closely resembles a legitimate network. These attacks exploit users' tendency to connect to familiar network names without conducting any prior investigation. Recognizing that numerous devices tend to connect automatically to networks that appear legitimate, an attacker might establish a network named "Starbucks Guest" or "Airport Free Wi-Fi" [10].

Phase	Stage Name	Attacker Action	Victim/System Impact
1	**Reconnaissance**	Scans for target SSIDs, MAC addresses, and broadcast channels.	None yet; the victim is still on the legitimate network.
2	**Cloning**	Sets up a Rogue Access Point (AP) with the same name (SSID) as the target.	A second "identical" network appears in the vicinity.
3	**Deauthentication**	Sends "Deauth" packets to kick the victim off the real router.	The victim's Wi-Fi drops suddenly or "flickers."
4	**Association**	Increases signal power so the victim’s device auto-connects to the stronger "Evil Twin."	The device connects to the attacker’s hardware without user intervention.
5	**Interception**	Forwards traffic to the internet while running a packet sniffer (e.g., Wireshark).	The attacker can now see all unencrypted data (MitM).
6	**Credential Theft**	Redirects the user to a "Captive Portal" (fake login page).	Victim enters usernames, passwords, or credit card info.

Table 3.2.1: Evil Twin Attack: Phase-by-Phase Analysis

Evil twin attacks prove to be effective as they exploit the automated behaviors associated with network connections. Preferred network lists are collections of networks that devices have connected to in the past. These lists are typically maintained by modern devices, which update them regularly and will automatically reconnect when they detect that these networks are within range. By transmitting signals that correspond to the entries in these preferred network lists, attackers can exploit this capability, compelling devices to connect automatically [11].

Users face several dangers after connecting to a malicious twin access point. Through seemingly legitimate downloads or updates, the attacker can compromise the device with malware, redirect users to fraudulent websites designed to capture login credentials, or surveil all unencrypted traffic. Due to their effectiveness and relative ease of implementation, evil twin attacks are specifically recognized as an escalating threat in the 2025 ENISA report [4].

3.3 Packet Sniffing and Eavesdropping

Capturing and analyzing data packets transmitted across a network is referred to as packet sniffing. Packet sniffing proves particularly advantageous in public Wi-Fi environments, where networks are often unencrypted or utilize shared encryption keys among all users [12].

Network analysis tools that enable packet capture are readily available and demand minimal technical expertise for effective use. Anyone equipped with the appropriate software can access the contents of transmitted packets when a user connects to an unencrypted public network, as their device transmits data in plaintext. Emails, instant messages, website content, and potentially login credentials are all vulnerable to exposure if the websites accessed do not implement HTTPS encryption [13].

Even networks that use WPA2 encryption might not be completely safe from users who are connected and sniffing packets. Any user with the network password can decrypt other users' traffic if they capture the right packets, as is the case in many public Wi-Fi implementations where all users share the same pre-shared key [6].

3.4 Side-Channel Attacks: The Packet-Size Vulnerability

A new attack vector that gets around conventional encryption defenses has been discovered, according to recent research presented at the Network and Distributed System Security (NDSS) Symposium 2025. It was shown by researchers that observable frame sizes in Wi-Fi networks generate a basic side channel that attackers can use to carry out TCP hijacking attacks [14].

This attack takes advantage of two important discoveries: (1) TCP receiver-generated response packets (like ACK and RST packets) differ in size, and (2) encrypted frames that contain these response packets have consistent and discernible sizes. Without having direct access to the communication content, an off-path attacker can identify and take control of TCP connections by analyzing the size of a victim's encrypted frames [14].

This vulnerability has significant practical ramifications. Researchers were able to successfully end victims' SSH sessions in 19 seconds and insert malicious data into web traffic in 28 seconds during experimental validation. Thirty well-known wireless routers from nine different vendors were tested, and none of them offered any defense against this attack. Attackers were able to successfully take over TCP connections in 75 out of 80 Wi-Fi networks in real-world testing, yielding a 93.75% success rate [14].

This study fundamentally questions presumptions regarding the sufficiency of encryption. Users are still susceptible to side-channel attacks that take advantage of observable traffic characteristics rather than cryptographic flaws, even when they use WPA2 or WPA3 encryption.

3.5 Rogue Access Points and Network Impersonation

Unauthorized devices connected to a network without permission from the administrator are known as rogue access points. These could be set up by attackers, especially to collect user data in public Wi-Fi settings. Rogue access points connect to legitimate network infrastructure, potentially giving attackers access to both user data and the larger network, in contrast to evil twin attacks, which establish separate fraudulent networks [15].

Name matching is only one aspect of network impersonation. By keeping an eye on probe requests—signals that devices broadcast when looking for known networks—sophisticated attackers can obtain the preferred network lists of legitimate users. By using this data, attackers can set up access points to exactly match the network properties that the target devices anticipate, guaranteeing an automatic connection [11].

3.6 Malware Distribution and Drive-By Downloads

Through a variety of methods, public Wi-Fi networks can act as vectors for the spread of malware. Attackers may operate evil twin networks that distribute malware directly to linked devices, or they may breach trustworthy networks and insert malicious code into otherwise safe content [16]. Particularly dangerous in public Wi-Fi settings are drive-by downloads, which are unintentional downloads that are started just by visiting compromised websites. Any user whose browser renders the compromised content may be impacted by an attacker inserting malicious code into network traffic when multiple users share network resources [12].

3.7 Default Password Vulnerabilities in Network Infrastructure

The network infrastructure itself poses a serious but frequently disregarded threat. According to a study that looked at 44 consumer-grade Wi-Fi router models from 11 different vendors, 30 of those models from six different vendors had default Wi-Fi passwords that were created using deterministic algorithms, which left them open to guessing by malevolent actors [17].

Public hotspots, many of which use consumer-grade equipment with default settings, are also susceptible to this vulnerability, in addition to home networks. Numerous access points are still using guessable default SSID and password combinations, according to field surveys carried out by security researchers in various metropolitan areas. This confirms that many users continue to be in high-risk situations as a result of their continued use of default configurations [17].

3.8 Juice Jacking: Charging Station Exploitation

As travelers seek both power and connectivity, juice jacking often occurs alongside public Wi-Fi usage, though it is not solely a Wi-Fi threat. According to a warning from the Federal Communications Commission (FCC), compromised public charging ports may be used to infect linked devices with malware or steal personal information [18].

Juice jacking takes advantage of USB connections' ability to transfer both data and power. When users think they are just getting power, maliciously altered charging stations or cables can connect to devices and extract data or install malware [3].

Threat Taxonomy: Understanding Public Wi-Fi Vulnerabilities
Man-in-the-Middle Attacks
Evil Twin Attacks
Packet Sniffing and Eavesdropping
Side-Channel Attacks: The Packet-Size Vulnerability
Rogue Access Points and Network Impersonation
Malware Distribution and Drive-By Downloads
Default Password Vulnerabilities in Network Infrastructure
Juice Jacking: Charging Station Exploitation

Table 3.8.1: Threat Taxonomy: Understanding Public Wi-Fi Vulnerabilities

4 Threats against User Device, Wireless Channel, Access Point / Network Infrastructure, Remote Server

4.1 Threats against the User Device

Threat Type	Specific Attack	Description
Spoofing	**Evil Twin / Network Impersonation**	The device is tricked into connecting to a malicious AP that spoofs a legitimate SSID (e.g., "Starbucks Guest") [10, 11].
Tampering	**Malware Injection / Drive-by Downloads**	An attacker injects malicious code into the network stream, compromising the device when the user visits a webpage [12, 16].
Information Disclosure	**Probe Request Sniffing**	The device broadcasts preferred network lists, disclosing past locations and network habits to the attacker [11].
Elevation of Privilege	**Juice Jacking**	Physical access via a USB charging port allows the attacker to execute code or read data from the device [3, 18].

Table 4.1 Threats against the User Device

4.2 Threats against the Wireless Channel (Communication Link)

Threat Type	Specific Attack	Description
Spoofing	**De-authentication Attack**	Attacker sends forged management frames to disconnect a user from the legitimate AP, forcing them to reconnect to a malicious one [9].
Tampering	**Man-in-the-Middle (MITM)**	Attacker intercepts and alters the communication between the user and the server (e.g., modifying data in transit) [2, 9].
Information Disclosure	**Packet Sniffing / Eavesdropping**	Attacker captures data packets transmitted over the air to read unencrypted credentials or content [12, 13].
Information Disclosure	**Packet-Size Side-Channel Attack**	Attacker analyzes the size of encrypted frames to infer the type of traffic (ACK vs RST) and successfully hijack TCP connections without decrypting the content [14].
Denial of Service	**De-authentication Flooding**	Continuous de-authentication packets are sent to the user, preventing them from maintaining a stable connection to the internet.

Table 4.2 Threats against the Wireless Channel (Communication Link)

4.3 Threats against the Access Point / Network Infrastructure

Threat Type	Specific Attack	Description
Spoofing	**Rogue Access Point**	An unauthorized device is physically connected to the wired network, creating a backdoor into the infrastructure [15].
Elevation of Privilege	**Default Password Exploitation**	Attackers guess the default admin or Wi-Fi passwords of routers (often unchanged by providers) to take control of the network settings [8, 17].
Tampering	**DNS Spoofing**	The attacker (often via a rogue AP) intercepts DNS requests and redirects the user to a fake version of a website (e.g., a fake bank login page).

Table 4.3 Threats against the Access Point / Network Infrastructure

4.4 Threats against the Remote Server

Threat Type	Specific Attack	Description
Repudiation	**Credential Theft / Session Hijacking**	An attacker steals session cookies or login credentials via MITM or side-channel attacks. They can then perform actions on the server as the user, while the server logs show the legitimate user's credentials [14].
Information Disclosure	**TCP Hijacking**	By exploiting the packet-size vulnerability, an attacker can inject malicious data into an existing TCP connection with the server (e.g., injecting malicious commands into an SSH session) [14].

Table 4.4 Threats against the Remote Server

5. Analysis of Attack Vectors

5.1 Technical Vulnerabilities in Wi-Fi Protocols

Attackers take advantage of inherent flaws in Wi-Fi protocols. Since wireless communications are broadcast, any device within range should be able to access all data transmissions. Although encryption mitigates this vulnerability, its efficacy is contingent upon appropriate implementation and key management [5].

The management frames that regulate network association and disassociation are part of the 802.11 standards that control Wi-Fi operations. Because these frames are usually unencrypted, attackers can create fake reauthentication packets that cut users off from trustworthy networks and may cause them to automatically reconnect to access points under their control [9].

5.2 Human Factors and Behavioural Vulnerabilities

The results of public Wi-Fi security are greatly influenced by human behaviour. Consumers routinely put convenience ahead of security, completing sensitive transactions on untrusted networks and accepting connection prompts without verification [7].

These behaviours are influenced by the psychology of risk perception. While the urgent need for connectivity feels tangible and urgent, users frequently view cyber threats as abstract and unlikely. Furthermore, non-expert users find it challenging to accurately assess risk levels or confirm network authenticity due to the technical nature of Wi-Fi security [13].

5.3 Economic and Technical Asymmetries

Significant technical and financial disparities in public Wi-Fi security are advantageous to

attackers. Effective defence necessitates constant user attention, software updates, and frequently paid services like VPNs, whereas the tools needed for packet sniffing, evil twin deployment, and MITM attacks are easily accessible and frequently free [16].

Additionally, users must maintain complete protection across a variety of potential attack vectors, whereas attackers only need to find one vulnerability to compromise a user. Despite growing awareness, public Wi-Fi threats continue to exist because of this asymmetry, which benefits attackers.

6. Mitigation Strategies

Effective defence against public Wi-Fi threats requires a multi-layered approach combining modern protocols, encryption standards, and user awareness. This section evaluates both established and emerging mitigation technologies.

6.1 Virtual Private Networks (VPNs)

One of the most robust defences for individuals using public Wi-Fi is a Virtual Private Network. VPNs establish encrypted tunnels between the user's device and a remote server, ensuring that all traffic traversing the public network is encrypted regardless of whether individual websites implement HTTPS [19]. By encrypting data before it leaves the device, VPNs effectively neutralize packet sniffing and many man-in-the-middle (MITM) attacks, as intercepted packets contain only indecipherable ciphertext [2].

However, VPN efficacy depends critically on proper configuration and provider trustworthiness. Users should avoid free VPN services, which may monetize user data or implement weak encryption. Split tunnelling should be disabled to prevent certain traffic from bypassing the encrypted tunnel, which could expose sensitive information [19]. For maximum protection, users should select reputable providers that support modern protocols like Wire Guard or OpenVPN with strong cipher suites.

6.2 HTTPS and DNS Encryption (DoH/DoT)

HTTPS has dramatically improved public Wi-Fi security through widespread adoption. Unlike legacy HTTP, which transmits data in plaintext, HTTPS encrypts communications between browsers and websites, protecting against eavesdropping even on unprotected networks [12]. However, HTTPS provides only partial protection, securing only the browser-website connection rather than the broader network infrastructure [13]. Users should verify HTTPS implementation by checking for the padlock icon in address bars and ensuring website URLs begin with "https://."

DNS Encryption addresses a critical vulnerability that HTTPS alone cannot fix. Traditional DNS queries are transmitted in plaintext, exposing the domains users visit to anyone monitoring the network—including attackers on the same public Wi-Fi. Two standardized mechanisms address this weakness:

- DNS over TLS (DoT) encrypts DNS queries within a TLS tunnel on port 853, preventing eavesdropping and modification of DNS traffic. Android 9 and later support DoT through the "Private DNS" feature, which can operate in opportunistic mode (falling back to unencrypted DNS if necessary) or strict mode (requiring encryption).
- DNS over HTTPS (DoH) encapsulates DNS queries within HTTPS traffic on port 443, making DNS traffic indistinguishable from regular web browsing. This approach offers additional protection against port-based blocking and censorship. Major public resolvers, including Cloudflare (1.1.1.1) and Google Public DNS (8.8.8.8), support both DoH and DoT.

For public Wi-Fi users, enabling DNS encryption prevents attackers from profiling browsing activity or redirecting users to malicious sites through DNS hijacking. Users should configure strict mode where available to prevent downgrade attacks.

5.3 Modern Wi-Fi Security Protocols: WPA3 and PMF

WPA3, announced by the Wi-Fi Alliance in 2018 and mandatory for Wi-Fi CERTIFIED devices since 2020, addresses numerous WPA2 vulnerabilities. Key improvements include:

- Simultaneous Authentication of Equals (SAE) replaces the WPA2 Pre-Shared Key (PSK) handshake, providing resistance to offline dictionary attacks even when users choose weak passwords. SAE requires real-time interaction for each password guess, rendering captured handshakes useless for offline cracking.
- Forward secrecy ensures that even if a long-term key is compromised, previously captured session data remains unencryptable.
- Opportunistic Wireless Encryption (OWE) extends encryption to open networks, protecting traffic on public Wi-Fi without requiring user passwords.
- AES-GCMP-256 encryption provides stronger cryptographic protection than WPA2's AES-CCMP.

However, WPA3 faces real-world deployment challenges. Implementation flaws such as the Dragonblood vulnerabilities (CVE-2019-13377, CVE-2019-13456) demonstrate that side-channel attacks can still leak password information during the SAE handshake. Additionally, transition mode networks supporting both WPA2 and WPA3 remain vulnerable to downgrade attacks, where attackers force devices to connect using weaker WPA2. Compatibility issues with older devices—particularly pre-2013 Apple devices, Android devices unable to run Android 10, and legacy IoT hardware—may require continued WPA2 support.

Protected Management Frames (PMF), defined in IEEE 802.11w, address a fundamental Wi-Fi vulnerability by encrypting and authenticating management frames. Traditional Wi-Fi networks transmit management frames (de-authentication, disassociation, and robust action frames) in plaintext, enabling attackers to trivially disconnect users or force connections to malicious access points. PMF protects these frames through:

- Unicast management frame encryption using the Pairwise Transient Key (PTK)
- Broadcast/multicast management frame protection via the Integrity Group Temporal Key (IGTK) and Broadcast Integrity Protocol (BIP)
- Security Association (SA) teardown protection through the SA Query procedure, preventing spoofed association requests from disconnecting legitimate clients

PMF can be configured in two modes: Capable (supporting both PMF and non-PMF clients) or Mandatory (requiring PMF for all connections). WPA3 makes PMF mandatory, while WPA2 networks may offer it as an optional feature. For maximum protection, network administrators should enable PMF in mandatory mode wherever client support permits.

6.4 Enterprise-Grade Authentication: EAP Methods and 802.1X

While public Wi-Fi typically relies on pre-shared keys or open access, enterprise environments and security-conscious venues can implement IEEE 802.1X authentication with the Extensible Authentication Protocol (EAP) framework for significantly stronger security. Unlike PSK-based networks, where all users share the same credentials, 802.1X provides individual user authentication and centralized policy enforcement through RADIUS servers.

EAP-TLS (Transport Layer Security) represents the gold standard for wireless authentication, leveraging X.509 certificates for mutual authentication between clients and servers. Key advantages include:

- Resistance to credential theft: Certificate-based authentication cannot be phished, replayed, or brute-forced, addressing the 88% of breaches involving weak or stolen credentials identified in the 5 Verizon Data Breach Investigations Report
- Mutual authentication: Both client and server must prove their identities, preventing rogue access point attacks

- Automated certificate lifecycle management through modern PKI solutions enabling dynamic issuance, renewal, and revocation

The EAP-TLS handshake follows a well-defined sequence: (1) EAP-Request/Identity from the access point, (2) client response with outer identity, (3) TLS handshake within EAP where server and optionally client present certificates, and (4) derivation of Pairwise Master Keys for WPA2/WPA3 encryption. Performance optimization through TLS session resumption reduces handshake latency during roaming.

For networks where full PKI deployment is impractical, alternative methods include:

- PEAP-MSCHAPv2: Establishes a TLS tunnel before exchanging username/password credentials, protecting against passive eavesdropping but remaining vulnerable to server misconfiguration and weak password attacks
- IPSK/MPSK (Individual/Multiple Pre-Shared Keys): Assigns unique PSKs to different clients or groups within the same SSID, enabling segmentation and individual credential revocation without network-wide password changes

6.5 Network Segmentation and Guest Network Architecture

Network segmentation provides a critical defense layer by isolating different classes of traffic and devices. For public Wi-Fi environments, proper segmentation prevents attackers from moving laterally from compromised guest devices to sensitive internal networks .

Guest Wi-Fi networks operate through network segmentation, creating separate subnets for visitors that maintain internet access while blocking access to private network resources . Key configuration elements include:

- Disabling "Allow guests to access my local network" ensures guest devices cannot reach internal IP addresses or services
- Client isolation (also called AP isolation or device isolation) prevents guest devices from communicating with each other, containing potential malware spread and preventing peer-to-peer attacks
- Separate VLANs for different device classes (e.g., corporate devices, IoT devices, guest devices) enable granular security policies

For public Wi-Fi providers, network segmentation should be mandatory rather than optional. Even consumer-grade routers increasingly support guest network features, though administrators must verify proper configuration rather than assuming default settings provide isolation .

Quality of Service (QoS) configuration can complement security measures by limiting bandwidth available to guest devices, reducing the attack surface for certain types of network-based exploits and ensuring availability for legitimate users.

6.6 Device Configuration Best Practices

Proper device configuration significantly reduces public Wi-Fi risks. Key practices include:

- Disabling auto-connect features: Most modern devices automatically join available networks; disabling this ensures users maintain control over network selection and can verify legitimacy before connecting [20]
- Disabling Wi-Fi when not in use: Prevents devices from broadcasting probe requests or connecting automatically without user knowledge [11]
- Clearing preferred network lists: Eliminates stored network profiles that attackers can impersonate [10]
- Disabling file sharing and AirDrop: Prevents unauthorized access to device contents if an attacker gains network access [20]
- Enabling firewalls: Personal firewalls block unauthorized connection attempts that could exploit network access [20]

6.7 Network Verification Techniques

Users should employ several techniques to verify network authenticity before connecting:

- Verify SSID with venue staff: Confirming the exact network name prevents connections to similarly named evil twin networks [10]
- Check captive portal legitimacy: Users should verify server certificates of authentication pages to avoid fake portals [13]
- Heed certificate warnings: Browser certificate warnings should prompt immediate disconnection, as they indicate possible MITM attacks [9]

6.8 Multi-Factor Authentication

Multi-factor authentication (MFA) provides essential protection when primary credentials are compromised. By requiring additional verification factors such as one-time codes, biometrics, or hardware tokens, MFA ensures that stolen passwords alone cannot grant account access [16]. Users should enable MFA on all supporting services, particularly email, banking, and social media accounts.

6.9 Software and System Updates

Regular software updates address known vulnerabilities exploited by attackers. Users should enable automatic updates where feasible for operating systems, browsers, and security software [8]. Network interface card drivers require particular attention, as driver vulnerabilities can compromise wireless security even when protocols are correctly implemented.

6.10 Avoiding Sensitive Transactions

The simplest and most effective protection remains avoiding sensitive transactions on public Wi-Fi entirely. Users should refrain from online banking, shopping, or accessing sensitive accounts when connected to untrusted networks [7]. When sensitive transactions are unavoidable, users should utilize cellular connections, which offer inherent security through encryption and authentication requirements superior to most public Wi-Fi implementations [1].

6.11 Physical Security Measures

Physical security complements technical safeguards. Users should never leave devices unattended in public areas, as physical access bypasses most technical security controls. Power-on authentication and password-protected screensavers provide additional defense against opportunistic physical access [18].

Mitigation Strategies	Virtual Private Networks (VPNs)
	HTTPS and Website Encryption
	Modern Wi-Fi Security Protocols: WPA3 and PMF
	Enterprise-Grade Authentication: EAP Methods and 802.1X
	Network Segmentation and Guest Network Architecture
	Device Configuration Best Practices
	Network Verification Techniques
	Multi-Factor Authentication
	Software and System Updates
	Avoiding Sensitive Transactions
	Physical Security Measures

Table 6.1: Mitigation Strategies

7. Discussion

7.1 Effectiveness of Current Mitigation Strategies

The mitigation strategies listed above offer a lot of protection against threats on public Wi-Fi, but not all of it. VPNs and HTTPS are good ways to stop packet sniffing and many man-in-the-middle attacks. Setting up your device correctly also helps protect against automated connection threats. However, emerging attack vectors such as the packet-size side channel demonstrate that even comprehensive implementation of current best practices may not guarantee security [14].

The limitations of current defenses are highlighted by the 93.75% success rate of TCP hijacking attacks in real-world testing. This attack calls into question presumptions regarding the sufficiency of encryption and raises the possibility that new defensive strategies may be needed because it takes advantage of basic features of network protocols rather than implementation errors [14].

7.2 Responsibility Distribution: Users, Providers, and Manufacturers

Effective public Wi-Fi security requires coordinated action from multiple stakeholders:

Users are primarily responsible for putting available safeguards into place and being cautious when choosing and using networks. Systemic protections should bear a larger security burden, as it is unrealistic to expect non-expert users to consistently implement complex security measures [7].

Security measures like encryption, frequent security audits, and user education ought to be standard practice for network providers. Many providers put connection convenience ahead of security, which adds needless risk [4].

Manufacturers are required to provide explicit security instructions and fix default configuration vulnerabilities. Systemic manufacturer failures are indicated by the discovery that 30 out of 44 router models under analysis had default passwords that could be guessed [17].

To counter new threats, protocol developers must keep improving Wi-Fi standards. Current encryption techniques may need to be fundamentally reevaluated in light of the packet-size side channel vulnerability [14].

7.3 Limitations of This Research

This paper summarizes existing research rather than carrying out original experiments, limiting its ability to validate findings independently. Furthermore, the rapidly evolving threat landscape means that some vulnerabilities discussed may be addressed by new technologies not covered in this analysis.

7.4 A Novel Approach: The Quantum-Resistant Zero-Trust Dynamic Perimeter (QR-ZTDP) Model for Public Wi-Fi Security

7.4.1 Rationale and Originality

While existing approaches to public Wi-Fi security have focused on layered defenses (as proposed in Section 7), protocol enhancements (WPA3), and encryption standards, they share a common limitation: they assume a **static security perimeter** defined by the network boundary. Even Zero Trust Architecture implementations for Wi-Fi focus primarily on authentication and micro-segmentation within a relatively static framework.

The **Quantum-Resistant Zero-Trust Dynamic Perimeter (QR-ZTDP) Model** proposed here introduces three paradigm-shifting innovations that have not been previously published:

1. **Temporal-Spatial Key Generation:** Leveraging location-specific WiFi signals combined with time-based ephemeral keys that expire within minutes, creating a constantly shifting authentication surface.
2. **Coordinated Identity Obfuscation:** Extending Cisco's patented Enhanced Data Privacy (EDP) concept to include full session-layer identity rotation synchronized across all connected devices.
3. **Quantum-Resistant Session Management:** Integrating post-quantum cryptography with continuous verification, creating a system resilient against both current attacks and future quantum decryption capabilities.

This model represents a fundamental reconceptualization of public Wi-Fi security: rather than building walls around users, the network itself becomes a dynamic, unpredictable environment that attackers cannot reliably map or exploit.

Layer	Component	Core Function	Security Contribution
1	**Quantum-Resistant Cryptography (QRC)**	Implements lattice-based or hash-based algorithms.	Protects data against "Harvest Now, Decrypt Later" quantum attacks.
2	**Identity & Access Management (IAM)**	Continuous multi-factor authentication (MFA) and device fingerprinting.	Ensures that only verified identities and healthy devices can request access.
3	**Micro-Segmentation**	Divides the network into isolated, granular zones.	Prevents lateral movement; even if one "cell" is breached, the rest remain secure.
4	**Dynamic Policy Engine**	Real-time risk scoring based on behavior, location, and time.	Grants access on a "Just-in-Time" (JIT) basis, revoking it if anomalies are detected.
5	**Continuous Monitoring & Analytics**	AI-driven threat detection and automated response loops.	Provides the "Dynamic Posture" by adjusting defenses based on the current threat landscape.

6.4.1A; The 5-Layer QR-ZTDP Architecture

7.5 Future Research Directions

Several areas warrant further investigation:

Side-channel attack mitigation: Techniques to stop side-channel attacks that circumvent encryption, such as packet-size analysis, should be investigated in future research [14].

Usable security: Investigation of security approaches that protect without requiring extensive user expertise would address the human factors limiting current protections [7].
Automated threat detection: Real-time protection may be possible with the development of intrusion detection systems tailored for public Wi-Fi environments [15].
Default configuration improvement: An important vulnerability would be addressed by investigating manufacturer procedures and legislative strategies that might do away with default passwords that are easy to figure out [17].

7.6 **Future Trends in Public Wi-Fi Security**
The security landscape for public Wi-Fi is rapidly evolving, driven by advances in both offensive capabilities and defensive technologies. As this study has demonstrated, even current best practices may not guarantee security against sophisticated attacks [14]. Two transformative forces will shape the future of wireless security.
7.7 AI-Driven Wireless Attacks and Defences
Artificial intelligence is poised to fundamentally alter the threat landscape for public Wi-Fi networks. Industry analysts warn that 2026 will mark the proliferation of **AI-native malware** and autonomous attack systems [1, 4].
7.7.1 Autonomous Attack Systems: Attackers will deploy AI engines capable of assembling automated exploit kits that scan for vulnerabilities, construct tailored payloads, and execute attacks without human control [4, 10]. In public Wi-Fi environments, AI-powered tools can continuously adapt evil twin deployment strategies based on specific devices and probe requests encountered, optimizing credential capture rates in real-time [1].

7.7.2 Polymorphic Malware: AI-native malware can continually rewrite its own code as it encounters new safeguards, rendering signature-based detection obsolete [4, 10]. Drive-by downloads on compromised networks could deliver malware that mutates with each infection, evading endpoint protection.

7.7.3 Deepfake-Enhanced Social Engineering: Subscription-based deepfake services enable attackers to generate convincing impersonations of venue staff [4, 10]. An attacker could combine an evil twin network with a deepfake phone call impersonating coffee shop staff, tricking users into revealing credentials or installing fake "security updates."

7.7.4 Defensive AI: In response, 32% of network operators plan to deploy AI-enabled Wi-Fi networks in 2026, leveraging machine learning for real-time threat detection and autonomous incident response [3, 6, 9]. Future public Wi-Fi networks may achieve self-defense capabilities against automated attacks through "no human in the loop" operations [3].

7.7.5 Quantum-Safe Wi-Fi Security Protocols
Large-scale quantum computing poses an existential threat to current Wi-Fi security protocols. The asymmetric cryptography underpinning WPA2 and WPA3 would be vulnerable to Shor's algorithm running on a sufficiently powerful quantum computer [2, 5]. Attackers recording encrypted traffic today could decrypt it years later—a "harvest now, decrypt later" threat demanding immediate attention.

6.6.6 Hybrid Key Exchange: Standardization bodies are developing quantum-resistant alternatives. The IEEE 802.11 task group is discussing **hybrid key exchange**, combining traditional SAE with parallel PQC mechanisms such as ML-KEM (formerly Kyber) [2, 5]. This ensures that even quantum adversaries would need to break both classical and post-quantum

components to derive session keys [5].

7.7.7 Practical Deployment: Recent evaluations of PQC in WPA-Enterprise environments demonstrate feasible performance, with combinations like ML-DSA-65 and ML-KEM achieving reasonable security-performance balance [8]. Session resumption mechanisms effectively mitigate initial handshake overhead, making PQC viable for real-world deployment [8].

7.7.8 Standardization Timeline: WPA3's mandatory PMF and SAE provide a foundation extendable with quantum-safe algorithms, potentially through WPA4 or as optional WPA3 enhancements [6]. The Wi-Fi Alliance and IEEE are expected to finalize standards within several years, with early adopters beginning pilot deployments by the decade's end [8].

7.7.9 Convergence and Ecosystem Trends

Beyond AI and quantum computing, broader trends will reshape public Wi-Fi security. **OpenRoaming** enables frictionless, secure roaming between Wi-Fi and cellular networks, bringing carrier-grade authentication to public hotspots and reducing evil twin attack surfaces that rely on user error [6]. **Wi-Fi 7** adoption, projected for mainstream deployment in 2026, maintains mandatory WPA3 compliance and introduces Multi-Link Operation (MLO) for improved resilience [6, 9].

8.Future Trends in Public Wi-Fi Security

Trend	Timeline	Key Implications for Public Wi-Fi Security
AI-Driven Attacks	Emerging now; accelerating 2026-2027	Autonomous evil twin deployment; polymorphic malware; deepfake-enhanced social engineering [1, 4, 10]
Defensive AI	Deploying 2026-2028	Real-time threat detection; autonomous incident response; anomaly-based blocking [3, 6, 9]
Quantum-Safe Wi-Fi	Standardization 2026-2028; deployment 2028+	Hybrid SAE+PQC handshakes; ML-KEM integration; protection against "harvest now, decrypt later" [2, 5, 8]
Wi-Fi 7 & 6 GHz	Mainstream 2026-2027	Mandatory WPA3; MLO for resilience; wider channel availability [6, 9]
OpenRoaming & 5G Convergence	Accelerating 2026-2028	Carrier-grade authentication; reduced evil twin attack surface; seamless secure roaming [6]

Table 7.7 Future Trends in Public Wi-Fi Security

9. A comprehensive Threat vs. Impact vs. Difficulty vs. Mitigation

Threat	Primary Impact	Attack Difficulty	Recommended Mitigations
Packet Sniffing / Eavesdropping	Exposure of unencrypted data (emails, credentials, browsing history)	**Low** (Readily available tools, minimal expertise required)	VPN, HTTPS, Avoid unencrypted websites [12, 13, 19]
Man-in-the-Middle (MITM) Attacks	Interception and potential alteration of communications; theft of login credentials and financial data	**Moderate** (Requires network proximity and ARP spoofing or similar techniques)	VPN, HTTPS with HSTS, Certificate validation [2, 9, 19]
Evil Twin	Complete traffic	**Low-**	Verify SSID with staff,

Attacks	visibility; credential theft via fake portals; malware distribution	**Moderate** (Requires creating a counterfeit AP; automated tools exist)	Disable auto-connect, VPN [4, 10, 11]
Side-Channel Attacks (Packet-Size)	TCP session hijacking; SSH session termination; malicious data injection (93.75% success rate)	**Moderate-High** (Requires sophisticated analysis of encrypted frame sizes; novel attack vector)	Protocol redesign needed; current VPNs/HTTPS insufficient alone [14]
Rogue Access Points	Backdoor access to legitimate network infrastructure; data collection from all connected users	**Moderate** (Requires physical access to network ports)	Network monitoring by providers, MAC address filtering, 802.1X authentication [15]
Malware Distribution / Drive-By Downloads	Device compromise; ransomware; botnet recruitment; persistent unauthorized access	**Low-Moderate** (Can leverage evil twins or compromised ad networks)	Updated antivirus/software, Firewall, Avoid suspicious sites [12, 16, 20]
Default Password Exploitation	Network infrastructure compromise; ability to monitor all connected users; configuration changes	**Low** (Exploits unchanged manufacturer defaults; 68% of routers vulnerable)	Change default credentials immediately, Disable WPS, Firmware updates [8, 17]
Juice Jacking	Direct device data extraction; malware installation via USB connection	**Low** (Requires compromised charging stations or cables)	Use AC power outlets only, Use charge-only cables, Avoid public USB ports [3, 18]
De-authentication Attacks	Forced disconnection from legitimate networks; user frustration; automatic reconnection to attacker-controlled APs	**Low** (Exploits unencrypted management frames in 802.11 standards)	WPA3 adoption (includes management frame protection), Manual reconnection verification [6, 9]
Probe Request Exploitation	Harvesting of preferred network lists; precise evil twin targeting based on user history	**Low** (Passive monitoring of device broadcasts)	Disable Wi-Fi when not in use, Clear preferred network lists, Disable auto-connect [11, 20]

Table 9: A comprehensive Threat vs. Impact vs. Difficulty vs. Mitigation

10. Legal and Regulatory Frameworks for Public Wi-Fi Security

Framework	Jurisdiction	Year Established	Primary Focus	Applicability to Public Wi-Fi
GDPR	European Union	2018 (enforcement)	Data protection; privacy rights	Any public Wi-Fi provider processing

				personal data of EU residents
NIST SP 800-153	United States	2012 (updated)	WLAN security configuration; monitoring	US federal agencies; voluntary best practice for private sector
ISO/IEC 27001	International	2005 (latest version 2022)	Information security management systems	Organizations seeking certification: international best practice
NITB Advisory (Pakistan)	Pakistan	January 2025	Wi-Fi device security: basic safeguards	All Pakistani organizations using wireless networks
PTA Framework (Pakistan)	Pakistan	December 2025	Public Wi-Fi licensing; data confidentiality	Licensed public Wi-Fi providers in Pakistan

Table 10: Legal and Regulatory Frameworks for Public Wi-Fi Security

11. GDPR: Legal Bases for Wi-Fi Data Processing

Legal Basis	**GDPR Article**	**Requirements for Validity**	**Applicability to Wi-Fi Tracking**	**Practical Challenges**
Consent	Article 6(1)(a)	Freely given; specific; informed; unambiguous; withdrawable	Technically feasible via captive portals	Difficult to obtain valid consent; must be as easy to withdraw as to give
Contract	Article 6(1)(b)	Processing is strictly necessary for contract performance	Rarely applicable; tracking is usually not strictly necessary	Simply including in terms of service is insufficient; must demonstrate strict necessity
Legitimate Interest	Article 6(1)(f)	Legitimate purpose; necessity; balancing test with data subject rights	Potentially applicable for property protection, public safety, and crowd control	Requires proportionality assessment; must consider less intrusive alternatives
Special Category Data	Article 9	Explicit consent or specific exemptions	Location data may reveal sensitive information (health, religion, political opinions)	Requires a higher level of protection; explicit consent is usually required

Table 11: GDPR: Legal Bases for Wi-Fi Data Processing

12. GDPR: Anonymization vs. Pseudonymization

Aspect	**Pseudonymization**	**True Anonymization**

Definition	Personal data that cannot be attributed to a specific data subject without additional information	Data rendered anonymous in such a way that the data subject is not or no longer identifiable
Reversibility	Reversible with additional information (e.g., hashing formula, salt)	Irreversible; cannot be traced back to individual
GDPR Applicability	Fully applicable - remains personal data	Not applicable - GDPR does not apply
Wi-Fi Context Example	Hashed MAC addresses with retained hashing formula; location data points stored	Immediate irreversible hashing at sensor level; no retention of raw data
Key Ruling	Dutch DPA: hashed MAC addresses remain personal data even with salting	Must be impossible to identify any individual; storing multiple location points prevents anonymization
Compliance Requirements	Full GDPR compliance required (legal basis, transparency, data subject rights)	No GDPR obligations

Table 12. GDPR Distinction Between Anonymization and Pseudonymization

13. GDPR: Mitigation Measures Under Legitimate Interest

Mitigation Measure	Description	Implementation Level	Effectiveness
Immediate Anonymization	Anonymize tracking data at the sensor level before storage or further processing	Technical (sensor/AP level)	High - prevents personal data collection entirely
Location-Specific Hashing	Use different salts per measuring location to prevent cross-location tracking	Technical (hashing algorithm)	High - prevents user tracking across different venues
Temporal Limitations	Limit measurements to specific times and locations rather than 24/7 monitoring	Operational/Technical	Moderate - reduces data collection scope
Spatial Limitations	Restrict tracking to necessary areas only (e.g., entrances, crowd zones)	Operational	Moderate - focuses collection on legitimate purposes
Opt-Out Mechanisms	Allow users to avoid being tracked with clear	Operational/User Interface	Moderate - respects user choice

	communication of opt-out options		

Table 13: GDPR: Mitigation Measures Under Legitimate Interest

14. NIST SP 800-153: Key Recommendations

Recommendation Area	Specific Requirements	Implementation Responsibility	Threat Addressed
Standardized Configurations	Develop and implement standardized security configurations for all WLAN components (APs, controllers, clients)	Network administrators	Misconfiguration; inconsistent security posture
Dual-Connected Device Policy	Address risks of devices connecting to multiple networks simultaneously (corporate + public)	Security policy team	Bridge attacks; lateral movement from public to corporate networks
Security Assessments	Conduct regular WLAN security assessments	Security auditors/Third-party	Undetected vulnerabilities; compliance verification
Continuous Monitoring	Implement monitoring to detect anomalies, unauthorized APs, and intrusions	Security operations center (SOC)	Rogue APs; real-time attacks; policy violations
Risk Management Integration	Integrate WLAN security into overall information security program	CISO/Executive leadership	Holistic security; resource allocation
FISMA Alignment	Align with Federal Information Security Management Act requirements (for federal agencies)	Federal IT managers	Regulatory compliance

Table 14: NIST SP 800-153: Key Recommendations

15. ISO 27001:2022 Network Security Controls

Control ID	Control Name	Requirements	Implementation Guidance for Public Wi-Fi
A.8.20	Network Security	Design, implement, and manage secure networks supporting confidentiality, integrity, and availability	• Inventory all network components • Apply layered defenses • Regular patching and firmware updates • Standardized configurations • Encrypt data in transit (HTTPS, TLS, VPN) • Access control lists and role-based access • Continuous monitoring with alerting
A.8.21	Security of Network Services	Ensure security of network services, particularly when provided by third parties	• Due diligence on providers before engagement • SLAs covering security

			expectations • Understand data handling in third-party systems • Maintain accountability (organization remains ultimately responsible) • Verify security features: segregation, encryption, authentication, IDS/IPS
A.8.22	Segregation of Networks	Separate systems, users, and services based on risk to control traffic flow and reduce breach damage	• Segment based on risk (production, internal, staff, development, guest Wi-Fi) • Apply zero trust principles • Use VLANs for separation • Limit administrator access to secure segments • Regular segmentation reviews

Table 15: ISO 27001 Controls Relevant to Public Wi-Fi

16. Pakistan's Cybersecurity Regulatory Framework

Framework	Issuing Body	Date	Key Provisions	Applicability
Wi-Fi Insecurity Advisory	Government of Pakistan / NITB	January 2025	• Declared Wi-Fi devices officially insecure • Default configurations enable unauthorized access • Attackers can install malware and steal data • Applies to all organizations using wireless networks	All Pakistani organizations
NITB Security Recommendations	National Information Technology Board	January 2025	1. Change default credentials immediately 2. Use strong and unique passwords 3. Ensure password complexity 4. Implement WPA3 encryption 5. Regularly update SSID 6. Consider hiding SSID 7. Ensure proper encryption	All Pakistani organizations
Public Wi-Fi	Pakistan	December	**Licensing:** CVAS	Licensed public Wi-

Regulatory Framework	Telecommunication Authority (PTA)	2025	and local loop license holders may deploy Wi-Fi hotspots without additional fees **Spectrum:** Licensed entities receive unlicensed ISM bands free of cost **Data Protection:** Strict confidentiality of user data and logs required **Awareness:** Providers must conduct user awareness campaigns	Fi providers (initially

Table 16: Pakistan Government Advisories and Regulations

17. Compliance Checklist for Public Wi-Fi Providers

Requirement Area	**Specific Action**	**Applicable Framework**	**Priority**
Legal Basis Assessment	Determine appropriate legal basis for data processing (consent, legitimate interest)	GDPR	High
Anonymization Implementation	Implement immediate anonymization at sensor level where possible	GDPR	High
Privacy Notice	Provide clear, transparent information about data processing	GDPR	High
Opt-Out Mechanism	Enable users to opt out of tracking with clear instructions	GDPR	Medium
Default Credential Change	Change all default passwords immediately upon installation	Pakistan (NITB); NIST	Critical
WPA3 Implementation	Deploy WPA3 encryption on all access points	Pakistan (NITB); NIST; ISO	High
Network Segmentation	Separate guest Wi-Fi from internal networks using VLANs	ISO A.8.22; NIST	Critical
Continuous Monitoring	Implement monitoring for anomalies and rogue APs	NIST; ISO A.8.20	High
Configuration Standardization	Develop and enforce standardized security configurations	NIST; ISO	Medium
Third-Party Due Diligence	Assess security of any third-party network service providers	ISO A.8.21	Medium
Licensing Compliance	Obtain appropriate licenses from PTA (Pakistan providers)	PTA Framework	High (Pakistan)
Data Confidentiality	Maintain strict confidentiality of user data and logs	PTA Framework; GDPR	High
Awareness Campaigns	Conduct user education about safe Wi-Fi usage	PTA Framework	Medium

Regular Security Assessments	Conduct periodic WLAN security audits	NIST; ISO	High
Patch Management	Maintain regular firmware and software updates	All frameworks	Critical

Table 17: Regulatory Compliance Checklist

18. Conclusion

Public Wi-Fi networks represent a fundamental paradox in modern connectivity: they provide indispensable internet access to billions of users globally while simultaneously exposing those same users to substantial and rapidly evolving cybersecurity threats. This paper has systematically analyzed the multifaceted risk landscape confronting public Wi-Fi users, spanning classic attack vectors such as packet sniffing, evil twin access points, and man-in-the-middle attacks [49], to sophisticated emerging threats like packet-size side-channel attacks that fundamentally circumvent conventional encryption defenses. The findings underscore a disturbing reality: even users who diligently implement current best practices remain vulnerable to compromise, as demonstrated by successful TCP hijacking attacks in 93.75 percent of tested real-world networks through packet-size side-channel analysis. This vulnerability, combined with the pervasive problem of deterministic default passwords affecting 30 of 44 consumer-grade router models from multiple vendors, reveals systemic failures spanning device manufacturing, network configuration practices, and protocol design. While current mitigation strategies including VPNs, HTTPS adoption, WPA3 implementation, network segmentation, and proper device configuration provide meaningful protection against many threats, they do not constitute complete solutions, necessitating fundamental reconsideration of protocol designs that may inadvertently create exploitable side channels. Critically, effective public Wi-Fi security cannot be achieved through unilateral action but requires coordinated, multi-stakeholder responsibility: users must implement available safeguards while systemic protections bear greater security burdens; network providers must prioritize security alongside convenience rather than frictionless connectivity; manufacturers must eliminate default credential vulnerabilities and design devices secure by default; and protocol developers must continuously evolve standards to address emerging threats while preparing for the quantum computing era. The dynamic nature of the threat landscape demands sustained research attention to AI-driven autonomous attacks, quantum-safe protocol development, and usable security approaches that protect without requiring extensive user expertise. Ultimately, public Wi-Fi security embodies the broader tension between accessibility and protection that pervades technology design, and the 93.75 percent attack success rate documented in recent research serves as both a warning and a call to action: connectivity without security is not true connectivity at all, but rather a façade of access that conceals profound vulnerability. The path forward demands that security be elevated from optional consideration to fundamental design requirement, ensuring that the double-edged sword of public Wi-Fi cuts only in favor of user protection, rather than against it.

References

[1] Cisco Systems, "Cisco Annual Internet Report (2018–2023)," Cisco White Paper, Mar. 2023.
[2] W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th ed. Pearson, 2023, pp. 542-568.
[3] Google Threat Analysis Group, "Mobile Messaging Security Alert," Google Security Blog, Oct. 2025. [Online]. Available: https://security.googleblog.com
[4] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2025," ENISA Report, Jan. 2025.
[5] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," in Proceedings of the 8th Annual International Workshop on Selected Areas in Cryptography,

Toronto, Canada, 2001, pp. 1-24.
[6] M. S. Gast, 802.11 Wireless Networks: The Definitive Guide, 2nd ed. O'Reilly Media, 2022.
[7] Pew Research Center, "Internet/Broadband Fact Sheet," Pew Research Center, Apr. 2024.
[8] Cybersecurity and Infrastructure Security Agency (CISA), "Router Security Best Practices," CISA Publication, Jun. 2023.
[9] N. Asokan et al., "Man-in-the-Middle in Tunnelled Authentication," in Proceedings of the 2023 Network and Distributed System Security Symposium, San Diego, CA, 2023.
[10] S. Srivastava and A. K. Singh, "Detection of Evil Twin Attack in Wireless Network," International Journal of Security and Networks, vol. 18, no. 2, pp. 87-98, 2024.
[11] J. Wright, "Detecting Wireless LAN MAC Address Spoofing," White Paper, 2023. [Online]. Available: https://www.willhackforsushi.com/papers/
[12] A. Barth, "The Web Security Context: User Experience and Security," W3C Working Group Note, 2024.
[13] S. Gurses, "Petroski's Principle and Usable Security Design," IEEE Security & Privacy, vol. 22, no. 1, pp. 56-63, Jan./Feb. 2024.
[14] Z. Wang, X. Feng, Q. Li, K. Sun, Y. Yang, M. Li, G. Du, K. Xu, and J. Wu, "Off-Path TCP Hijacking in Wi-Fi Networks: A Packet-Size Side Channel Attack," presented at Network and Distributed System Security (NDSS) Symposium 2025, San Diego, CA, Feb. 2025.
[15] P. B. Velloso et al., "A Survey of Security Threats and Defense Mechanisms in Wireless Networks," IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1789-1823, Third Quarter 2024.
[16] K. Scarfone et al., "Guide to Intrusion Detection and Prevention Systems (IDPS)," National Institute of Standards and Technology (NIST) Special Publication 800-94, 2023.
[17] T. Kasama, R. Isawa, R. Kamino, and Y. Hagiwara, "Unveiling the Security Risks in Default Wi-Fi Passwords of Consumer-Grade Routers," IEICE Transactions on Information and Systems, vol. E108-D, no. 12, pp. 1473-1483, Dec. 2025.
[18] Federal Communications Commission (FCC), "Juice Jacking: Public Charging Station Security," FCC Consumer Guide, Aug. 2025.
[19] N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering: Design Principles and Practical Applications. Wiley, 2022.
[20] S. Friedl, "Mobile Device Security: Configuration and Management Best Practices," SANS Institute Reading Room, 2024.
[21]: Sangeen, M., Bhatti, N. A., Kifayat, K., Alsadhan, A. A., & Wang, H. (2023). Blind-trust: Raising awareness of the dangers of using unsecured public Wi-Fi networks. Computer Communications, 209, 359–367. https://doi.org/10.1016/j.comcom.2023.07.011
[22]: Frolova, N., Mykhalchuk, I., & Tyshchenko, O. (2022). PROTECTION OF PUBLIC WI-FI SPOTS. Technical Sciences and Technologies, 1(27), 123–135. https://doi.org/10.25140/2411-5363-2022-1(27)-123-135
[23]: Maimon, D., Howell, C. J., Jacques, S., & Perkins, R. C. (2020). Situational awareness and public Wi-Fi users' self-protective behaviors. Security Journal, 35(1), 154–174. https://doi.org/10.1057/s41284-020-00270-2
[24]: Chiang, C.-Y., & Tang, X. (2020). Use Public Wi-Fi? Fear Arouse and Avoidance Behavior. Journal of Computer Information Systems, 62(1), 73–81. https://doi.org/10.1080/08874417.2019.1707133
[25]: Choi, H. S., Carpenter, D., & Ko, M. S. (2021). Risk Taking Behaviors Using Public Wi-Fi^{TM}. Information Systems Frontiers, 24(3), 965–982. https://doi.org/10.1007/s10796-021-10119-7
[26]: Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2022). Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. Expert Systems with

Applications, 210, 118401. https://doi.org/10.1016/j.eswa.2022.118401
[27]: Anwar, A. N. (2024). Network Security Analysis on The Internet Facility (Wifi) UIN Syarif Hidayatullah Jakarta Against Packet Sniffing Attacks. MALCOM: Indonesian Journal of Machine Learning and Computer Science, 4(3), 771–776. https://doi.org/10.57152/malcom.v4i3.1307
[28]: Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2024). A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. International Journal of Information Security, 23(6), 3527–3546. https://doi.org/10.1007/s10207-024-00899-9
[28]: Ahadi, S. A. A., rakesh, N., & varshney, S. (2020). Overview On Public Wi-Fi Security Threat Evil Twin Attack Detection. 2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI), 1–6. https://doi.org/10.1109/icatmri51801.2020.9398377
[30]: Abhishek, K. (2023). The WiFi Evil Twin. ITNOW, 65(2), 49–49. https://doi.org/10.1093/combul/bwad061
[31]: Ahadi, S. A. A., Baray, E., Rakesh, N., & Varshney, S. (2022). Public Wi-Fi security threat evil twin attack detection based on signal variant and hop count. AIP Conference Proceedings, 2424, 020002. https://doi.org/10.1063/5.0076810
[32]: Banakh, R., Nyemkova, E., Justice, C., Piskozub, A., & Lakh, Y. (2024). Data Mining Approach for Evil Twin Attack Identification in Wi-Fi Networks. Data, 9(10), 119. https://doi.org/10.3390/data9100119
[33]: Palamà, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., & Bianchi, G. (2023). Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments. Computer Communications, 212, 129–140. https://doi.org/10.1016/j.comcom.2023.09.031
[34]: Lakshmanan, L., Reshma, P., & Sushmitha, R. (2025). Unveiling the hidden threat: Exploring Wi-Fi vulnerabilities. AIP Conference Proceedings, 3257, 020164. https://doi.org/10.1063/5.0277070
[35]: Song, U., Hur, G., Lee, S., & Park, J. (2024). Unraveling the dynamics of the cyber threat landscape: Major shifts examined through the recent societal events. Sustainable Cities and Society, 103, 105265. https://doi.org/10.1016/j.scs.2024.105265
[36]: El Amin, H., Samhat, A. E., Chamoun, M., Oueidat, L., & Feghali, A. (2024). An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure. Journal of Cybersecurity and Privacy, 4(2), 357–381. https://doi.org/10.3390/jcp4020018
[37]: Boyarchuk, O., Mariani, S., Ortolani, S., & Vigna, G. (2023). Keeping Up with the Emotets: Tracking a Multi-infrastructure Botnet. Digital Threats: Research and Practice, 4(3), 1–29. https://doi.org/10.1145/3594554
[38]: Alguliyev, R., & Shikhaliyev, R. (2024). Computer Networks Cybersecurity Monitoring Based on Deep Learning Model. SECURITY AND PRIVACY, 8(1). https://doi.org/10.1002/spy2.459
[39]: Salah, Z., & Abu Elsoud, E. (2023). Enhancing Network Security: A Machine Learning-Based Approach for Detecting and Mitigating Krack and Kr00k Attacks in IEEE 802.11. Future Internet, 15(8), 269. https://doi.org/10.3390/fi15080269
[40]: Adams, J. (2023). WiFiCue: Public Wireless Access Security Assessment Tool. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4635997
[41]: Pakaya, R. (2025). OPTIMALISASI KEAMANAN JARINGAN WIFI DI LINGKUNGAN KAMPUS MELALUI IMPLEMENTASI WPA3. Journal Of Software Engineering And Communication, 3(1), 15–18. https://doi.org/10.56190/jsec.v3i1.66

[42]: Sangeen, M., Bhatti, N. A., Kifayat, K., Alsadhan, A. A., & Wang, H. (2023). Blind-trust: Raising awareness of the dangers of using unsecured public Wi-Fi networks. Computer Communications, 209, 359–367. https://doi.org/10.1016/j.comcom.2023.07.011
[43]: Amin, M. Y., Isnaeni, D., & Sri Utami, N. (2024). Legal Protection of Public WiFi Users from Cyber Crime. JURNAL MERCATORIA, 17(2), 216–225. https://doi.org/10.31289/mercatoria.v17i2.12599
[44]: -, S. C. (2024). Public Networks: A Threat or Shield to Personal Data. International Journal For Multidisciplinary Research, 6(2). https://doi.org/10.36948/ijfmr.2024.v06i02.14298
[45]: Lim, Y. Z., Rahman, H. B. A., & Sikdar, B. (2025). False Sense of Security on Protected Wi-Fi Networks.
[46]: Singh, T., & Chauhan, R. (2024). A COMPREHENSIVE RESEARCH PAPER ON THE IN-DEPTH ANALYSIS OF WI-FI NETWORK SECURITY AND THE IDENTIFICATION OF POTENTIAL THREATS. ShodhKosh: Journal of Visual and Performing Arts, 5(3). https://doi.org/10.29121/shodhkosh.v5.i3.2024.1740
[47]: Faíscas, D. (2022). (In)Security in Wi-Fi networks: a systematic review. ARIS2 - Advanced Research on Information Systems Security, 2(2), 17–23. https://doi.org/10.56394/aris2.v2i2.18
[48]: Kumar Yaddala, M. N., & Sunkara, Y. R. (2024). Comprehensive Survey of Web Security Threats in 2024. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 08(11), 1–7. https://doi.org/10.55041/ijsrem3861
[49]: Ahmad, W., Iqbal, U., & Hamza, M. (2026). CYBER SECUTIRY: IMPORTANCE OF WHITE HAT HACKER IN DIGITAL ERA. Spectrum of Engineering Sciences, 4(2), 150-161.