**KAMPUS AKADEMIK PUBLISING**
**Jurnal Sains Student Research (JSSR)**
**Vol.4, No.6 Desember 2026**
e-ISSN: 3025-9851, p-ISSN : 3025-986X, Hal 1251-1265
DOI : https://doi.org/10.61722/jssr.v4i6.13321

# Security Risks and Protection Levels of Mobile Device Users on Public Wi-Fi Networks

**Muhammad Adha Darojat**[1*]
[1]Department of Information Systems, Universitas Islam Negeri Syarif Hidayatullah Jakarta, Indonesia
Email: muhammad.adha24@mhs.uinjkt.ac.id

***Abstract.*** *Public Wi-Fi offers convenient internet access; however, it also exposes mobile device users to data security risks. This systematic literature review, conducted in accordance with PRISMA guidelines, synthesizes 23 studies with accessible full text published between 2022 and 2026. Of 943 articles identified via Semantic Scholar, 25 passed screening and 23 were analyzed in depth. Three research questions addressed the attacks most frequently targeting mobile device users on public Wi-Fi (RQ1), the factors that make mobile devices more vulnerable than desktops (RQ2), and the most effective technical mitigations (RQ3). The most discussed attacks were eavesdropping (or traffic analysis) and man-in-the-middle (MitM), followed by rogue access points, deauthentication, and WPA2 handshake (KRACK) attacks. Reported vulnerability factors include moderate user awareness, delayed operating system updates, weak TLS implementation in applications, and device identity leakage via wireless signals. Reported mitigations include attack detection, device updates, VPNs (as a recommendation), TLS certificate validation, and user education. Only one study examined Android and Linux in the same attack scenario, no study evaluated MAC address randomization, and VPN effectiveness has not been empirically measured. Consequently, the answers to RQ2 and RQ3 remain partial, highlighting the need for comparative empirical evaluations of mitigations on public Wi-Fi..*

***Keywords****: man-in-the-middle; mobile devices; public Wi-Fi; systematic literature review; wireless security*

**Abstrak.** Wi-Fi publik memudahkan akses internet, tetapi membuka risiko bagi data pengguna perangkat seluler. Tinjauan sistematis (PRISMA) ini mensintesis 23 studi terbitan 2022–2026 yang teks lengkapnya dapat diakses. Pencarian di Semantic Scholar menghasilkan 943 artikel, 581 di antaranya memiliki teks lengkap yang dapat diakses; setelah penyaringan judul dan abstrak, 25 studi lolos dan 23 dapat dibaca penuh. Tiga pertanyaan penelitian diajukan: jenis serangan yang paling sering menargetkan pengguna seluler di Wi-Fi publik (RQ1), faktor yang membuat perangkat seluler lebih rentan dibanding desktop (RQ2), dan mitigasi teknis yang efektif (RQ3). Kategori serangan yang paling banyak dibahas adalah penyadapan/analisis trafik dan man-in-the-middle (MitM), disusul rogue access point atau jaringan palsu, deauthentication, dan serangan terhadap handshake WPA2 (KRACK). Faktor kerentanan yang dilaporkan mencakup kesadaran pengguna yang hanya berada pada tingkat sedang, pembaruan OS yang tertunda, praktik TLS yang lemah di aplikasi, dan kebocoran identitas perangkat lewat sinyal nirkabel. Mitigasi yang dilaporkan meliputi deteksi serangan, pembaruan perangkat, VPN (sebagai rekomendasi), validasi sertifikat TLS, dan edukasi pengguna. Hanya satu studi yang menguji Android dan Linux pada skenario serangan yang sama, tidak ada evaluasi MAC randomization, dan tidak ada pengukuran empiris efektivitas VPN, sehingga jawaban RQ2 dan RQ3 bersifat parsial. Temuan ini menuntut evaluasi empiris komparatif atas mitigasi di Wi-Fi publik.

**Kata kunci**: keamanan nirkabel; man-in-the-middle; perangkat seluler; tinjauan sistematis; Wi-Fi publik

## 1. BACKGROUND

Wi-Fi is widely used to access the internet in airports, hotels, cafés, schools, and other public spaces (Amin et al., 2024). However, Wi-Fi does not guarantee that users are authenticated or that their data is encrypted (Trianto et al., 2022). Most Wi-Fi services

*Naskah Masuk:01 November 2026; Revisi: 02 November 2026; Diterima: 03 November 2026; Terbit: 07 November 2026*

utilize WPA2. The 4-way handshake mechanism in WPA2 is vulnerable to attacks via the key reinstallation (KRACK) method, and many access points (APs) cannot be patched—or, in some cases, never receive updates at all (Trianto et al., 2022). WPA3 was introduced to address these weaknesses, yet certain vulnerabilities have been discovered within it as well (Saini et al., 2022). Deauthentication attacks exploit flaws in the management frames of the IEEE 802.11 standard. Such attacks often serve as a precursor to "Evil Twin" or "Man-in-the-Middle" (MitM) attacks, and the use of firewalls or network encryption alone is insufficient to prevent them (Riza et al., 2025). Furthermore, even encryption does not close every potential security gap; in encrypted Wi-Fi networks, the analysis of MAC-layer metadata can still reveal user behavior (Hu et al., 2025).

Mobile device users face particular risks. Smartphones are used for banking, e-commerce, and communication, so they store a lot of sensitive data (Oludayo et al., 2023). Mobile banking can be used anytime and anywhere, but some users behave in unsafe ways, such as assuming that transactions over public Wi-Fi are completely safe (Candiwan & Rianda, 2024). At the application level, three problems stand out. First, apps that switch off TLS certificate validation allow third parties to intercept traffic (Ferreira, 2026). Second, third-party apps and SDKs send local network information to remote servers (Girish et al., 2023). Third, service discovery protocols leak device identity, including on public Wi-Fi (Yang et al., 2024).

Many studies have examined threats to Wi-Fi networks, but the evidence is scattered across three areas: attack techniques, user behavior and awareness, and defense mechanisms. Earlier systematic reviews covered mobile device security in general for 2017–2021 and did not discuss Wi-Fi (Engel et al., 2022). Others focused on mobile identity authentication (Zukarnain et al., 2022) or on smartphone security challenges (Oludayo et al., 2023). No synthesis seems to bring together attacks, vulnerability factors, and mitigations for mobile users on public Wi-Fi. The novelty of this review is that it maps the evidence across these three areas and reports the remaining gaps. For example, the corpus contains no evaluation of MAC randomization and no empirical measurement of VPN effectiveness.

This study answers three research questions. RQ1 asks which cyberattacks (for example Man-in-the-Middle, Evil Twin, and Packet Sniffing) most often target mobile

device users on public Wi-Fi. RQ2 asks which factors make mobile devices more vulnerable than desktop devices on open networks. RQ3 asks which technical approaches (for example VPN, end-to-end encryption, and MAC randomization) are most effective in protecting user data. The objective is to map and synthesize the evidence from the 23 selected studies to answer RQ1–RQ3.

## 2. THEORETICAL REVIEW

Public Wi-Fi refers to wireless internet access provided in public spaces, such as airports, hotels, and cafés (Amin et al., 2024). Such networks do not inherently guarantee authentication or encryption (Trianto et al., 2022). Most Wi-Fi services utilize WPA2. Within the WPA2 protocol, an attacker can retransmit the third message of the 4-way handshake process, causing the device to reinstall the same key. This attack is called key reinstallation (KRACK). Many access points (APs) cannot be patched or never receive a patch (Trianto et al., 2022). WPA3 was designed to remove these weaknesses, but new problems were found. An attacker can force a connection down to WPA2 using a Rogue AP, and beacon flooding can cause denial of service for clients (Saini et al., 2022).

Attacks against Wi-Fi users can be categorized based on the techniques employed. Deauthentication involves the misuse of IEEE 802.11 management frames to sever a user's connection. This technique often serves as a precursor to "Evil Twin" or "Man-in-the-Middle" (MitM) attacks and cannot be prevented solely through firewalls or network encryption (Riza et al., 2025). In the WPA3 protocol, such attacks remain possible if the "Management Frame Protection" feature is not automatically enabled (Saini et al., 2022). "Evil Twin" and "Rogue AP" attacks exploit open hotspots that use names similar to those of legitimate networks (Oludayo et al., 2023; Saini et al., 2022). Eavesdropping utilizes packet-sniffing tools, such as Wireshark, to intercept and read unprotected data traffic (Oludayo et al., 2023). Even within encrypted networks, the analysis of metadata at the MAC layer can still reveal user behavior (Hu et al., 2025). At the application layer, incomplete or disabled TLS certificate validation can facilitate the interception of data traffic (Ferreira, 2026; Berbecaru, 2025).

Mobile devices have several characteristics that affect their security. Smartphones store sensitive data and are used for banking, e-commerce, and communication (Oludayo et al., 2023). Android is open source and has many customized versions, so timely updates

are important for its security (Oludayo et al., 2023). The release of security updates also differs greatly between manufacturers (OEMs), models, and regions (Acar et al., 2024). Human factors matter as well, because mobile banking users are often not fully aware of the risks of using public Wi-Fi (Candiwan & Rianda, 2024; Khamis, 2025). The literature discusses several mitigations: attack detection (Riza et al., 2025; Trianto et al., 2022; Saini et al., 2022), device updates (Trianto et al., 2022; Oludayo et al., 2023), VPN (Candiwan & Rianda, 2024; Oludayo et al., 2023), TLS certificate validation (Ferreira, 2026; Berbecaru, 2025), end-to-end encryption (Harshvardhan et al., 2023), and user education (Amin et al., 2024).

## 3. RESEARCH METHOD

### Design and Data Sources

This review follows the PRISMA guidelines. In the Identification stage, articles were searched through the Semantic Scholar API. The search returned metadata and abstracts in CSV format, totaling 943 articles. The search string was:

("Public Wi-Fi" OR "Public Wireless Network" OR "Open Wi-Fi") AND ("Security Vulnerability" OR "Cyber Attack" OR "Data Breach") AND ("Mobile Device" OR "Smartphone" OR "Mobile User")

The search was then limited to articles whose full text could be accessed. This left 581 articles, and the other 362 of the 943 articles could not be accessed in full text. The 581 articles became the basis for selection.

### Inclusion and Exclusion Criteria

Studies were included if they were published in 2022–2026, focused on end users, and discussed wireless (Wi-Fi) network security. Studies were excluded if they discussed ISP infrastructure security, were opinion papers without experiments or case studies, or focused on cellular networks (4G/5G).

### Selection Process and Number of Screened Data

Screening of titles and abstracts (*Screening*) had four steps: removing duplicate titles, filtering Wi-Fi and security topics by keywords, assessing the end-user or mobile focus, and reading the abstracts of the top candidates manually. All articles were published in 2022–2026, so none was excluded because of publication year. Next, the full

texts of the 25 candidates were sought for the *Eligibility* stage. Two articles could not be obtained, so 23 articles were read and kept. The research flow and the selection results are shown in Figure 1:

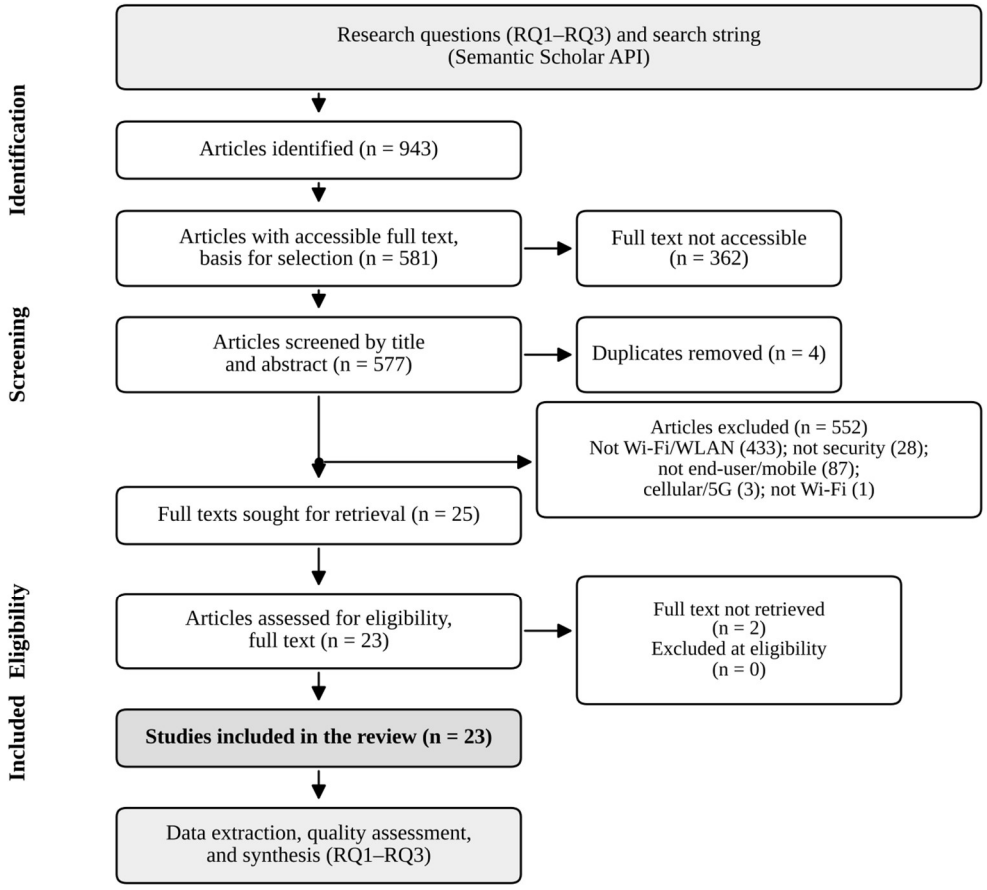



**Figure 1.** Research methodology flow and study selection based on PRISMA

*Source:* Author's analysis

The initial screening used keywords and abstract reading by one assessor (the author), not by two independent assessors. All 23 articles were kept at the eligibility stage based on the researcher's decision. Some of them are only partly relevant, as explained in the limitations subsection.

## Data Extraction and Quality Assessment

Data were extracted into a synthesis matrix with four groups of columns. The first group contains study metadata, study design, devices and operating systems, test environment, and sample. The second group is for RQ1 and contains attack types, attack vectors, evidence of frequency, and impact. The third group is for RQ2 and contains vulnerability factors and the comparison between mobile devices and desktops. The

fourth group is for RQ3 and contains mitigation techniques, level of application, metrics, results, and limitations. Study quality was scored on four items: a clear objective, a replicable method, empirical evidence, and a discussion of limitations. Each item received a score of 0, 0.5, or 1.

## 4. RESULTS AND DISCUSSION

### Characteristics of the Studies

The selected studies were published in 2022 (5 studies), 2023 (4 studies), 2024 (8 studies), 2025 (5 studies), and 2026 (1 study). Only three studies are set directly in public Wi-Fi or public places: Riza et al. (2025), Trianto et al. (2022), and Amin et al. (2024). Study Saini et al. (2022) examines Evil Twin on open APs in public places, but it is set in an enterprise network. Study Yang et al. (2024) examines identity leakage on public Wi-Fi. Studies Candiwan and Rianda (2024), Khamis (2025), and Oludayo et al. (2023) mention public Wi-Fi as a risk factor for mobile users. The other studies support the topic only indirectly. Because the corpus is limited to articles with accessible full text, some public Wi-Fi studies are not included (see the Limitations and Threats to Validity subsection).

### RQ1: Types of Attacks Targeting Mobile Users on Public Wi-Fi

None of the studies in this corpus measure the frequency with which each type of attack occurs on public Wi-Fi networks. Therefore, the question of which attack type occurs "most frequently" is addressed by counting the number of studies that discuss each category. This serves as an indirect indicator rather than a measure of actual prevalence in the real world. Table 1 summarizes the attack categories and the studies that address them.

**Table 1.** Attack categories and the studies that discuss them

| Attack category | Studies | Evidence reported |
|---|---|---|
| Eavesdropping, sniffing, traffic analysis | Guo et al., 2024; Ramezanpour et al., 2022; Oludayo et al., 2023; Girish et al., 2023; Hu et al., 2025; Yang et al., 2024 | Oludayo et al. (2023): Wi-Fi and Bluetooth interfaces are vulnerable to eavesdropping with Wifite and Aircrack-ng, and data traffic can be read by packet sniffers such as Wireshark. Guo et al. (2024): sniffing BLE and WiFi signals of phones links wearables with phones (accuracy above 80%). Hu et al. (2025): on encrypted Wi-Fi traffic, MAC-layer metadata features distinguish video uploads from other activities with 98.1% accuracy. Girish et al. (2023): broadcast and multicast traffic in local networks enables household fingerprinting. Yang et al. (2024): service discovery leaks device identity |
| Man-in-the-Middle | Riza et al., 2025; Trianto et al., 2022; Ramezanpour et al., 2022; Mwakajwanga & | Trianto et al. (2022) classifies KRACK as MitM. Riza et al. (2025) describes deauthentication as an initial step of MitM. Saini et al. (2022): Evil Twin on open APs leads to MitM. Ramezanpour et al. (2022): |

| Attack category | Studies | Evidence reported |
|---|---|---|
| | Mwambe, 2024; Saini et al., 2022 | 5G/WiFi coexistence facilitates MitM. Mwakajwanga and Mwambe (2024) is not specific to public Wi-Fi |
| Rogue AP, Evil Twin, fake networks | Trianto et al., 2022; Oludayo et al., 2023; Saini et al., 2022 | Trianto et al. (2022): connection to a Rogue AP created with Vanhoef's script. Saini et al. (2022): a Rogue AP with a lower beacon interval downgrades WPA3 connections to WPA2; Evil Twin "works on open APs in public places"; on password-protected APs, the attacker guesses the password through an offline dictionary attack and then creates a twin AP. Oludayo et al. (2023): open hotspots with names resembling legitimate networks, and the "No iOS Zone" vulnerability that connects iPhones to fake networks |
| Deauthentication | Riza et al., 2025; Saini et al., 2022 | Riza et al. (2025): 97.8% detected among 600 high-intensity deauth packets (589 detected, 11 missed). Saini et al. (2022): deauth still succeeds on WPA3 simply by flooding deauth frames because Management Frame Protection is not automatically enabled |
| KRACK (WPA2 key reinstallation) | Trianto et al., 2022; Saini et al., 2022 | Trianto et al. (2022): 3 of the 4 tested Android smartphones are vulnerable to key reinstallation (PTK and/or GTK). Saini et al. (2022): the latest Windows, Android, and iOS do not accept retransmission of the 3rd message and are therefore safe from KRACK |
| Beacon flooding, WPA3 vulnerabilities | Saini et al., 2022; Ramezanpour et al., 2022 | Saini et al. (2022): beacon flooding exposes clients to denial of service; a WPA3 attack dataset was created (250 attributes) |
| Weak TLS and application traffic interception | Ferreira, 2026; Berbecaru, 2025 | Ferreira (2026): 24.7% of 954 Flutter applications have at least one anti-pattern; 21.0% use cleartext URLs; 5.0% disable certificate validation. Berbecaru (2025): certificate validation is still often performed incompletely in applications and browsers (the author cites earlier measurements) |
| Data exfiltration by applications/SDKs | Girish et al., 2023 | Mobile applications and third-party SDKs send local network data to remote servers; 93% of 93 IoT devices use broadcast protocols and 73% use multicast |
| Hijacking of Wi-Fi remote protocols | Majors et al., 2023 | All four analyzed Smart TV platforms violate at least one security property; Spook uses an Android phone to guess the PIN and install an ADB proxy |
| Phishing, malware, spyware | Candiwan & Rianda, 2024; Khamis, 2025; Oludayo et al., 2023; Bartłomiejczyk & El Fray, 2024 | Khamis (2025): the score for responding to emails claiming to be from a bank is 2.46 (scale 1–5). Oludayo et al. (2023): ENISA threats such as phishing and spyware. Bartłomiejczyk and El Fray (2024): passive/active malware attacks on SMS OTP on Android |

*Source:* Author's analysis of the 23 selected studies

### *RQ1 Findings*

The most discussed categories are eavesdropping or traffic analysis (6 studies) and MitM (5 studies, one of which is not specific to Wi-Fi). They are followed by rogue AP, Evil Twin, or fake networks (3 studies). Evil Twin is discussed explicitly only in Saini et al. (2022), and in Riza et al. (2025) as a follow-up to deauthentication. Only two studies measured attacks directly on smartphones or similar devices. Study Trianto et al. (2022) tested four Android devices. Study Saini et al. (2022) used a Samsung tablet, a MacBook, and a Windows laptop, but it did not report results per device. In Riza et al. (2025), the detector is a separate ESP32 device, and the test victim is not described as a smartphone.

### RQ2: Vulnerability Factors of Mobile Devices

a. **Human factors**

In a survey of mobile banking service users in Indonesia (n=197), 52.3% of respondents agreed with the statement, "I do not like using public Wi-Fi to conduct financial transactions" (33.5% indicated agreement, and 18.8% indicated strong agreement). Meanwhile, 28.4% of respondents remained neutral, and 19.3% expressed disagreement. The authors concluded that users are not yet fully aware of these risks (Candiwan & Rianda, 2024). Perceptions regarding security have the strongest influence on positive security-related behaviors (path coefficient 0.305; p=0.001), followed by the management of device infrastructure (0.189) (Candiwan & Rianda, 2024).In a survey in Zanzibar (n=94), awareness of the risk of public Wi-Fi transactions averaged 3.16 and concern about this risk averaged 3.20 (scale 1–5). The habit of checking website security before entering data scored only 2.74 (Khamis, 2025). The qualitative study Amin et al. (2024) concludes that low public awareness comes from a lack of education and information, the wrong belief that public Wi-Fi is safe, and dependence on technology. However, it does not report its interview and observation data.

b. **Devices, operating systems, and updates**

Study Oludayo et al. (2023) names outdated operating systems or third-party apps, public Wi-Fi use, and low-security network protocols as causes of smartphone security problems. Android is open source and has many customized versions, so timely updates determine its security. Based on a literature review, the authors conclude that iPhones have security problems less often than Android phones. An analysis of 367K Android security update records (599 devices, 4 major OEMs, 2014–2023) found large differences in roll-out across OEMs, models, and regions. The average release delay was 25 days for monthly updates, 42 days for quarterly updates, and 62 days for biannual updates. The average support period was 274 days in China and 136 days in other regions. Devices that are no longer supported still receive critical CVEs that remain unpatched (Acar et al., 2024). In the survey Candiwan and Rianda (2024), 79.2% of respondents said their OS or mobile banking app is always updated, but many ignored firewalls and anti-spyware.

c. **Application layer**

A static analysis of 954 Flutter apps found that 5.0% disable TLS certificate validation. It also found that 92.3% of the apps that depend on the network show no sign of certificate pinning. The author stresses that the detection is syntactic. It shows how

common risky practices are, but it is not a count of exploitable vulnerabilities (Ferreira, 2026). In open-source Android apps, permission issues are the most frequent security problem (370 cases, 53.7%), and the WiFi permission is among those developers discuss. The Network category has only 10 cases (1.45%), including server certificate issues and TLS implementation (Das et al., 2024). Third-party apps and SDKs also send local network information out (Girish et al., 2023). In addition, apps create a new attack path through SMS reader APIs. In the analyzed sample, 190 apps use the SMS Retriever API and 200 use the SMS User Consent API (Bartłomiejczyk & El Fray, 2024).

d. **Device identity and wireless signals**

Wireless devices periodically emit signals that can be intercepted and analyzed by third parties (Guo et al., 2024). Existing service discovery protocols broadcast device information. On public Wi-Fi networks, an internet service provider can identify an individual based on the broadcasted device name (as noted in the research background by Yang et al. (2024)). Connection behavior is also a significant factor. The KRACK scenario, as described in a study by Trianto et al. (2022), requires the victim to be within range, the signal from a rogue access point (Rogue AP) to be stronger, and the device to have previously connected to the SSID in question.

***Comparison with Desktop***

Only Trianto et al. (2022) tested both platforms under the same scenario (Table 2). Three of the four Android smartphones are vulnerable to key reinstallation for at least one type of key, while both Ubuntu laptops are not. This comparison has limits. The laptops use wpa_supplicant 2.4 and 2.6, which the authors say have been updated. The Android versions are old (Jelly Bean 4.2.2 to Lollipop 5.1), and the sample has only six devices. Study Saini et al. (2022) stresses that the latest versions of Windows, Android, and iOS all reject a retransmitted third message. Therefore, the evidence points to the role of OS version and updates, not to an inherent weakness of mobile devices.

**Table 2.** KRACK test results in Trianto et al. (2022)

| Device | OS / wpa_supplicant | PTK reinstallation | GTK reinstallation |
|---|---|---|---|
| Acer Aspire E14 notebook | Ubuntu 16.04 / v2.4 | Not vulnerable | Not vulnerable |
| Asus X441UV notebook | Ubuntu 18.04 / v2.6 | Not vulnerable | Not vulnerable |
| Huawei GR3 | Android Lollipop 5.1 | Vulnerable | Vulnerable |
| OPPO A37 | Android Lollipop 5.1 | Not vulnerable | Not vulnerable |

| Device | OS / wpa_supplicant | PTK reinstallation | GTK reinstallation |
|---|---|---|---|
| Samsung SM-G355H | Android KitKat 4.4.2 | Vulnerable | Not vulnerable |
| Samsung GT-I9060 | Android Jelly Bean 4.2.2 | Vulnerable | Not vulnerable |

*Source:* Trianto et al. (2022)

### *Answer to RQ2*

For mobile devices, the reported factors are moderate user awareness, delayed and uneven OS updates across OEMs, weak TLS practices and excessive permissions in apps, the habit of remembering and reconnecting to networks, and device identity leaked through signals and service discovery. The comparison with desktops rests on limited evidence from Trianto et al. (2022).

## RQ3: Technical Mitigations

The corpus reports mitigations in several areas: detection, updates, networks, applications, cryptography, authentication, and user education. Table 3 summarizes the evidence and the limitations of each approach.

**Table 3.** Mitigation approaches in the corpus

| Approach | Studies | Evidence reported | Notes |
|---|---|---|---|
| User-side deauthentication detection | Riza et al., 2025 | Accuracy 98–98.5% (normal to medium scenarios) and 97.8% (high); consumption of 68–79 mA vs 110–120 mA under continuous monitoring; notification latency of 220–270 ms; tested in a laboratory and on a public network | 11 of 600 packets missed at high intensity; requires an ESP32 device; not tested on phones |
| KRACK Detector | Trianto et al., 2022 | Gives a warning when the 3rd handshake message is retransmitted; validated with Wireshark | No accuracy metric; 6 devices |
| Two-stage IDS (AP + controller) | Saini et al., 2022 | Flood Detection System at the AP (a packet surge of more than 10 times per user or 15 times in total triggers a 500 ms capture) followed by an ML classifier; Decision Tree 99.98% and Random Forest 99.97%; FPR 0.00054 (DT); classifier of 1.7 MB; code and dataset are public | Enterprise setting, not public Wi-Fi |
| OS updates and patches | Trianto et al., 2022; Acar et al., 2024; Oludayo et al., 2023; Saini et al., 2022 | Trianto et al. (2022): Ubuntu 16.04 and 18.04 are not vulnerable to KRACK after updates. Saini et al. (2022): the latest OSs do not accept retransmission of the 3rd message. Oludayo et al. (2023) recommends timely updates. Acar et al. (2024) shows release delays across OEMs | Effectiveness not measured directly |
| VPN and avoiding public Wi-Fi | Candiwan & Rianda, 2024; Amin et al., 2024; Oludayo et al., 2023 | Candiwan and Rianda (2024) and Oludayo et al. (2023) recommend a trusted VPN on public Wi-Fi. Oludayo et al. (2023) also recommends using only WPA2 or better. Amin et al. (2024) mentions the absence of VPN habits as a vulnerability factor | Recommendations only; no VPN evaluation in the 23 studies |
| Wi-Fi provider security standards | Amin et al., 2024 | Cafés use WPA2 + user authentication; hotels use WPA2 + firewall; airports use WPA3 + traffic monitoring. Constraints: cost, technical knowledge, user volume | The number of informants in the interview data is not stated |
| TLS certificate validation | Ferreira, 2026; Berbecaru, 2025 | Ferreira (2026): 5.0% disable validation, 92.3% without pinning (pinning is not suitable for every application). Berbecaru (2025): trusted proxy architecture for certificate validation with privacy options (SCVP/DVCS) | Berbecaru (2025) has not been evaluated (future work). Ferreira (2026) reports prevalence, not a mitigation test |

| Approach | Studies | Evidence reported | Notes |
|---|---|---|---|
| Hardware-based human attestation | Majors et al., 2023 | Pairing signed with a TrustZone key with a physical button; average overhead of 113 ms | Tested on a Smart TV remote protocol, not public Wi-Fi |
| Secure virtual networks (overlay) | Autefage & Magoni, 2025 | Noise handshake 26.4 ms vs TLS 59.6 ms (tunnel) and 87.2 ms vs 202.4 ms (end-to-end); TCP throughput 94 MB/s (Noise AES) vs 81 MB/s (TLS 1.3 AES) | 8-node testbed; not specific to public Wi-Fi |
| Service discovery privacy | Yang et al., 2024 | Service discovery and secure connection in under 0.973 seconds on desktops, laptops, and phones; under 2.712 seconds on Raspberry Pi 4B | Not a direct public Wi-Fi attack |
| Cryptography and E2EE | Mwakajwanga & Mwambe, 2024; Harshvardhan et al., 2023 | Mwakajwanga and Mwambe (2024): steganography + AES + EdDSA tested with MSE (8.51e-6), PSNR, and SSIM. Harshvardhan et al. (2023): Signal implementation (X3DH + Double Ratchet) in a web chat application | Mwakajwanga and Mwambe (2024) robustness not yet tested. Harshvardhan et al. (2023) has no quantitative evaluation and no attack tests |
| Authentication | Zukarnain et al., 2022; Bartłomiejczyk & El Fray, 2024 | Zukarnain et al. (2022): review of mobile authentication methods and a proposed MFA combination. Bartłomiejczyk and El Fray (2024): risk assessment protocol for SMS OTP | Not specific to Wi-Fi |
| User education | Candiwan & Rianda, 2024; Khamis, 2025; Amin et al., 2024; Oludayo et al., 2023 | Recommend awareness and education programs | Effectiveness not measured |

*Source:* Author's analysis of the 23 selected studies

### *Answer to RQ3*

The corpus **does not support naming one approach as the "most effective"**. The studies use different metrics (accuracy, latency, power consumption, vulnerability status, and image metrics), and no study compares the approaches directly. Four points can be concluded. First, high-accuracy attack detection is reported for deauthentication (Riza et al., 2025) and for WPA2/WPA3 attacks (Saini et al., 2022). Second, device updates are consistent with the results of Trianto et al. (2022) and Saini et al. (2022), where updated devices are not vulnerable to KRACK. Third, VPN appears only as a recommendation (Candiwan & Rianda, 2024; Oludayo et al., 2023), and its effectiveness was not measured. Fourth, no study evaluated *MAC randomization* as a mitigation, and *end-to-end encryption* is discussed only for messaging apps (Harshvardhan et al., 2023), not for public Wi-Fi.

### Cross-RQ Discussion

Four patterns emerge from this synthesis. **First**, threats come from several layers. These are protocols (KRACK on WPA2 [Trianto et al., 2022; Saini et al., 2022] and WPA3 vulnerabilities [Saini et al., 2022]), networks (deauthentication [Riza et al., 2025], Evil Twin and fake networks [Oludayo et al., 2023; Saini et al., 2022]), applications (weak TLS validation and data leakage [Ferreira, 2026; Girish et al., 2023]), and metadata and

device identity that leak even when traffic is encrypted (Hu et al., 2025; Yang et al., 2024). **Second**, user awareness is consistently moderate in the surveys (Candiwan & Rianda, 2024; Khamis, 2025) and the study (Amin et al., 2024). The technical mitigations that were tested need extra devices or configuration (Riza et al. (2025) uses an ESP32, Trianto et al. (2022) uses a detector script, and Saini et al. (2022) uses a controller), or they are only recommendations (Candiwan & Rianda, 2024; Oludayo et al., 2023). *Author's interpretation:* this gap makes education and built-in device protection useful additions. However, the corpus has no quantitative evidence on how effective education is. **Third**, updates are a common thread. Updated devices are not vulnerable to KRACK (Trianto et al., 2022; Saini et al., 2022), while Android updates are rolled out very unevenly across OEMs and regions (Acar et al., 2024). **Fourth**, direct tests on smartphones are rare. Study Trianto et al. (2022) tested four Android devices, and its results reflect OS version and updates more than any built-in property of mobile devices. At the application level, Ferreira (2026) found that insecure TLS practices appear more often in more popular repositories (11.6% in the group with more than 1,000 stars, against 2.0% in the lowest group).

**Limitations and Threats to Validity**

The corpus is limited to papers whose full text can be accessed. Core public Wi-Fi studies that could not be accessed are not included. As a result, evidence for RQ1 and RQ3 in public Wi-Fi settings is thin, because only Riza et al. (2025), Trianto et al. (2022), and Amin et al. (2024) are set directly in that context.

Eight papers (Guo et al., 2024; Ramezanpour et al., 2022; Acar et al., 2024; Girish et al., 2023; Mwakajwanga & Mwambe, 2024; Zukarnain et al., 2022; Yang et al., 2024; Bartłomiejczyk & El Fray, 2024) were read only in their main parts, not in full.

Many papers are only partly relevant. Study Ramezanpour et al. (2022) covers 5G/WiFi coexistence, which is close to the 4G/5G exclusion. Study Engel et al. (2022) covers 2017–2021 and does not discuss Wi-Fi. Studies Majors et al. (2023) and Girish et al. (2023) cover Smart TVs and smart homes (home networks), and Saini et al. (2022) is set in an enterprise network. Studies Mwakajwanga and Mwambe (2024), Berbecaru (2025), Zukarnain et al. (2022), Autefage and Magoni (2025), Bartłomiejczyk and El Fray

(2024), and Harshvardhan et al. (2023) cover cryptography, authentication, and protocols that are not specific to Wi-Fi.

Some studies may fall under the exclusion criterion "opinion without experiment". Study Amin et al. (2024) claims to use interviews and observations but does not report the number of informants or the data. Study Oludayo et al. (2023) is a review. Study Harshvardhan et al. (2023) is a system design without quantitative evaluation or attack testing. Study Berbecaru (2025) is only a design without evaluation.

Selection was carried out by one assessor using keywords and abstracts, and the quality scores are not reported in this manuscript.

Two papers from the initial list of 25 (Patil & Patil on CPS/IoT and Tanaka on ECC) could not be obtained and were removed from the synthesis.

## 5. CONCLUSION AND SUGGESTIONS

Based on 23 studies (2022–2026) whose full text can be accessed, the answers to the research questions are as follows. **RQ1:** The most discussed attacks are eavesdropping or traffic analysis and MitM. They are followed by rogue AP, Evil Twin, or fake networks, then deauthentication and KRACK. Evil Twin is discussed explicitly in only one study. **RQ2:** The reported factors are moderate user awareness, delayed and uneven OS updates, weak TLS practices in mobile apps, and device identity leaked through signals and service discovery. The comparison between mobile and desktop rests on one small study with OS versions that are not equivalent. **RQ3:** The studies report attack detection, device updates, VPN (as a recommendation), certificate validation, and user education. However, there is no basis to call any one approach the most effective, and neither MAC randomization nor VPN effectiveness has been evaluated in the corpus. Future research should (a) compare mobile and desktop platforms under the same attack scenario with equivalent OS versions, (b) evaluate VPN, MAC randomization, and end-to-end encryption empirically on public Wi-Fi, and (c) use the same metrics across mitigations.

This review has limitations. The corpus is limited to papers whose full text can be accessed, one assessor carried out the selection, and several studies are only partly relevant to public Wi-Fi. Therefore, the conclusions should be read as a map of the

available evidence, not as a measure of attack prevalence or mitigation effectiveness in the field.

## REFERENCES

Acar, A., Tuncay, G. S., Luques, E., Oz, H., Aris, A., & Uluagac, S. (2024). 50 Shades of Support: A Device-Centric Analysis of Android Security Updates. *NDSS 2024*. https://doi.org/10.14722/ndss.2024.24175

Amin, M. Y., Isnaeni, D., & Utami, N. S. (2024). Legal Protection of Public WiFi Users from Cyber Crime. *Jurnal Mercatoria*, *17*(2), 217–226. https://doi.org/10.31289/mercatoria.v17i2.12599

Autefage, V., & Magoni, D. (2025). Secure Virtual Networks Built with Noise Tunnels and Iroha Key Management. *IEEE Virtual Conference on Communications 2025*. https://doi.org/10.1109/VCC67261.2025.11351221

Bartłomiejczyk, M., & El Fray, I. (2024). Device Risk Analysis Protocol for SMS-Based OTP Authentication. *IEEE Access*, *12*. https://doi.org/10.1109/ACCESS.2024.3445931

Berbecaru, D. G. (2025). TPValCert: Privacy-Preserving Trusted Proxy for Public Key Certificate Validation. *IEEE ISCC 2025*. https://doi.org/10.1109/ISCC65549.2025.11326465

Candiwan, C., & Rianda, L. M. (2024). Transactions at Your Fingertips: Influential Factors in Information Security Behavior for Mobile Banking Users. *International Journal of Safety and Security Engineering*, *14*(3), 795–806. https://doi.org/10.18280/ijsse.140312

Das, T., Ali, A., & Mikkonen, T. (2024). Taxonomy of Security-related Issues in Android Apps: An Empirical Study. *ASEW '24*. https://doi.org/10.1145/3695750.3695824

Engel, M., Ramadhan, A., Abdurachman, E., & Trisetyarso, A. (2022). Mobile Device Security: A Systematic Literature Review on Research Trends, Methods and Datasets. *Journal of System and Management Sciences*, *12*(2), 66–78. https://doi.org/10.33168/jsms.2022.0204

Ferreira, P. C. S. (2026). Prevalência de Anti-Padrões de Segurança de Rede em Aplicativos Flutter de Código Aberto. *Revista Científica Sistemática*, *16*(8). https://sevenpubl.com.br/RCS/article/download/10871/16823

Girish, A., Hu, T.-R., Prakash, V., Dubois, D. J., Matic, S., Huang, D. Y., Egelman, S., Reardon, J., Tapiador, J., Choffnes, D., & Vallina-Rodríguez, N. (2023). In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes. *ACM IMC '23*. https://doi.org/10.1145/3618257.3624830

Guo, N., Chen, Z.-F., Xu, H., Liu, Y., Zhao, Z., & Xu, S. (2024). WMLinks: Wearable Smart Devices and Mobile Phones Linking through Bluetooth Low Energy (BLE) and WiFi Signals. *Electronics*, *13*(16), 3268. https://doi.org/10.3390/electronics13163268

Harshvardhan, B., Saideep, C., Atharv, D., Ankit, J., & Bhise, A. (2023). A Secure Messaging Application with Unbreakable End to End Encryption. *IJRASET*, *11*(V), 234–239. https://doi.org/10.22214/ijraset.2023.50805

Hu, X., Huang, Y., & Wang, Q. (2025). Video Transmission Behavior Detection Based

on Differential Traffic Features. *BDCTA 2025*. https://doi.org/10.1145/3727505.3727531

Khamis, Z. A. (2025). Examining Information Security Knowledge, Attitude, and Behaviour among Mobile Banking Users in Zanzibar. *East African Journal of Information Technology*, *8*(1), 92–101. https://doi.org/10.37284/eajit.8.1.3010

Majors, J., Barsallo Yi, E., Maji, A., Wu, D., Bagchi, S., & Machiry, A. (2023). Security Properties of Virtual Remotes and SPOOKing their violations. *ACM ASIA CCS '23*. https://doi.org/10.1145/3579856.3582834

Mwakajwanga, G. H., & Mwambe, O. (2024). Digital-Signature Oriented Steganography Approach against Man-in-the-Middle Attack. *International Journal of Interactive Mobile Technologies*, *18*(16). https://doi.org/10.3991/ijim.v18i16.48709

Oludayo, O. I., Kikelomo, A. A., Adedeji, A. A., & Ayodeji, A. A. (2023). A Review of Smartphone Security Challenges and Prevention. *IRJIET*, *7*(5), 234–245. https://doi.org/10.47001/irjiet/2023.705030

Ramezanpour, K., Jagannath, J., & Jagannath, A. (2022). Security and Privacy vulnerabilities of 5G/6G and WiFi 6: Survey and Research Directions from a Coexistence Perspective. *arXiv:2206.14997*. http://arxiv.org/pdf/2206.14997

Riza, F., Hendrakusuma, D. F., & Wibowo, B. (2025). An Energy-Efficient ESP32 IoT System for Real-Time Detection of WiFi Deauthentication Attacks. *International Journal of Engineering Continuity*, *4*(2). https://ejournal.sultanpublisher.com/index.php/ijec/article/download/433/310

Saini, R., Halder, D., & Baswade, A. M. (2022). RIDS: Real-time Intrusion Detection System for WPA3 enabled Enterprise Networks. *arXiv:2207.02489*. https://arxiv.org/pdf/2207.02489

Trianto, N., Priambodo, D. F., & Insani, D. A. (2022). Implementasi KRACK dan KRACK Detector terhadap Wpa_Supplicant pada Perangkat Android dan Linux Ubuntu. *Jurnal TIKomSiN*, *10*(2). https://doi.org/10.30646/tikomsin.v10i2.639

Yang, Y., Deng, R. H., Yang, G.-M., Li, Y.-J., Pang, H., Huang, M., Shi, R., & Weng, J. (2024). PriSrv: Privacy-Enhanced and Highly Usable Service Discovery in Wireless Communications. *NDSS 2024*. https://doi.org/10.14722/ndss.2024.24174

Zukarnain, Z., Muneer, A., & Ab Aziz, M. K. (2022). Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges. *Symmetry*, *14*(4), 821. https://doi.org/10.3390/sym14040821