International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 04 | Apr 2026 www.irjet.net p-ISSN: 2395-0072

Cybersecurity Risks in Public and Private WIFI Networks: A Comparative Study

Sameed Ali Khan

Department of Computer Science and Engineering Sharda University Greater Noida, India

---

Abstract-*WiFi networks are central to modern communica- tion, connecting billions of devices globally. However, public and private WiFi environments present different cybersecurity risks. Public networks, often open and poorly secured, are vulnerable to attacks like man-in-the-middle, rogue access points, and session hijacking. Private networks, though more controlled, can face targeted threats due to weak passwords, outdated firmware, or insider misuse, potentially compromising sensitive data. This paper presents a comparative study of cybersecurity risks in public and private WiFi. Threats are analyzed across technical, behavioral, and organizational dimensions. Results show public networks are prone to frequent but lower-impact attacks, whereas private networks experience fewer but more severe incidents. Recommendations and future research directions, including AI- based monitoring and WiFi 6 adoption, are discussed.*

Index Terms-WiFi security, cybersecurity risks, public net- works, private networks, comparative study, insider threats

1. INTRODUCTION

Wireless Fidelity (WiFi) has become the backbone of mod- ern communication and connectivity. From online learning to e-commerce, entertainment, and cloud-based collaboration, individuals and organizations depend heavily on wireless net- works for seamless access. A 2023 Cisco report estimated that over 62% of global internet traffic now passes through WiFi networks [**?**]. This dependence highlights not only the utility of WiFi but also the vulnerabilities it introduces.

While WiFi ensures flexibility and mobility, its open and broadcast-oriented nature makes it inherently less secure than wired alternatives. Public WiFi networks, commonly deployed in airports, hotels, cafes, and libraries, prioritize accessibility and convenience. In contrast, private WiFi networks, found in homes, offices, and enterprises, prioritize stability, confiden- tiality, and restricted access. Despite these differences, both network types remain highly exposed to evolving cyber threats.

This study aims to systematically explore the similarities and differences in risks between public and private WiFi environments. It highlights how opportunistic attackers exploit the openness of public hotspots while targeted intrusions and insider threats threaten private deployments. By combining technical analysis with case studies and industry reports, this paper seeks to contribute to the understanding of WiFi security in real-world settings.

II.BACKGROUND AND PROBLEM STATEMENT

A. Evolution of WiFi Security

WiFi security has evolved through several generations of protocols. Each iteration attempted to address critical flaws of its predecessor:

- WEP (Wired Equivalent Privacy): Introduced in 1997, WEP provided only basic encryption. Due to weak RC4 keys and short initialization vectors, it was quickly bro- ken.
- WPA (WiFi Protected Access): Introduced as an interim fix, WPA incorporated TKIP but still relied on RC4, making it vulnerable to advanced attacks.
- WPA2: Adopted AES-based encryption and is widely used today. Vulnerabilities such as the KRACK attack revealed weaknesses in handshake mechanisms.
- WPA3: The current standard provides forward secrecy, robust encryption, and better defense against dictionary attacks, though adoption remains slow.

B. Challenges in Modern WIFI Environments

Despite protocol improvements, practical challenges persist:

- Poorly configured routers leave gaps even in WPA2/WPA3 deployments.
- Users often reuse weak or default passwords.
- Firmware updates are frequently ignored, exposing de- vices to known exploits.
- IoT devices, which often have limited security controls, expand the attack surface of private networks.

C. Problem Statement

Both public and private WiFi networks continue to face significant threats, but their nature and impact differ. Public WiFi is exposed to opportunistic and high-

frequency attacks, while private WiFi is targeted less frequently but faces higher- severity breaches, often with insider involvement. A clear comparative analysis is therefore needed to inform risk mitigation.

III. PUBLIC AND PRIVATE WIFI ARCHITECTURES

A. Public Wifi

Public networks are designed for ease of access:

- Open authentication, sometimes with no encryp- tion.
- Shared bandwidth among many users without iso- lation.
- Deployed in uncontrolled environments with little over- sight.

This accessibility invites attackers to launch man-in-the-middle (MITM) attacks, deploy rogue access points, or harvest unencrypted traffic.

B. Private WiFi

Private WiFi networks are more controlled:

- Often rely on WPA2/WPA3 with pre-shared keys or enterprise authentication.
- Administrators can implement VLANs, device isoltion, VLANs and segmented network architec- tures facilitate device and firewall rules.
- Network logs and monitoring systems allow better visibility.

However, insider misuse, default configurations, and IoT integration often create exploitable weaknesses. Johnson's 2021 study showed how insecure smart cameras offered attackers footholds.

C. Comparative Architectural Insights

TABLE I-Architectural Comparison Of Public Vs. Private WIFI

Feature	Public WiFi	Private WiFi
Access Control	Open or weak	Password / Enterprise Auth
Bandwidth Mgmt	Shared, unmanaged	Controlled, prioritized
Encryption	Often none / WEP	WPA2 / WPA3
Oversight	Minimal or none	Admin and monitoring
Attack Surface	Broad, anonymous	Smaller, insiderfocused

IV. COMPARATIVE ANALYSIS

A. Technical Vulnerabilities

TABLE II TECHNICAL RISKS: PUBLIC VS PRIVATE WIFI

Risk	Public WiFi	Private WiFi
Encryption Weakness	Common, often none	Misconfigura- tions
MITM Attacks	Very frequent	Rare but possible
Rogue Access Points	High occurrence	Low, Insider based
Firmware Exploits	Low impact	Higher risk for IoT

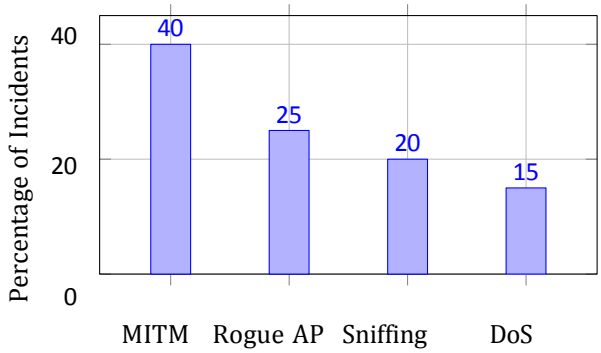

Fig.1. Distribution of WiFi-Related Attacks (2023)

B. Behavioral and Organizational Risks

Public WiFi users frequently neglect basic hygiene, such as avoiding sensitive logins or using VPNs. Conversely, private WiFi users may underestimate risks by reusing weak pass- words or neglecting updates. Organizationally, public WiFi lax oversight, while private WiFi depends on administrators' diligence.

V. PUBLIC WIFI ARCHITECTURE AND THREATS

Isolation and bandwidth management, reducing lateral move- ment of malware [9], [10], [20], [24].

Logging, IDS, and regular patching allow rapid detection and response, but require robust policy enforcement [7], [22], [25]. Despite these technical defenses, private networks are sus- ceptible to risks from misconfiguration, insider misuse, and especially insecure IoT devices [11], [17], [19], [23], [24]. In 2025, the proliferation of smart devices and BYOD (Bring Your Own Device) policies expand the attack surface, as demonstrated by multiple case studies of ransomware and remote intrusion leveraging unsecured endpoints [8], [11], [20], [24].

Attacks exploiting IoT firmware flaws, default credentials, and management interfaces are now among the most severe threats to home and office networks alike [11], [19], [20], [24].

A. Organizational Risk and Policy

Recent organizational risk assessments stress the importance of leadership alignment with security priorities. Where IT frameworks encourage zero-trust architectures and continuous vulnerability management, private WiFi security is signifi- cantly stronger [7], [10], [20], [24]. Ineffective oversight, poor employee awareness, and legacy systems, however, counteract many of these technical controls, sustaining risk for insider and targeted attacks [8], [10], [13], [23], [24].

VI. COMPARATIVE ARCHITECTURAL INSIGHTS

Table IV highlights the architectural differences between public and private WiFi networks based on key features such as access control, bandwidth management, encryption, oversight, and attack surface

VII. COMPARATIVE RISK ANALYSIS

Assessing public and private WiFi on technical, behavioral, and organizational dimensions reveals distinct patterns in vulnerabilities and exploitation.

A. Technical Vulnerabilities

Table V shows notable technical risks observed in recent incidents.

Table IV-Architectural Comparison: Public Vs. Private Wifi

Feature	Public WiFi	Private WiFi
Access Control	Open/weak [9], [18]	Password/ enterprise [15], [19]
Bandwidth Mgmt	Shared, unmanaged [9], [21]	Controlled, prioritized [9], [24]
Encryption	Unencrypted/ WEP [12], [21]	WPA2/WPA3 [15], [19]
Oversight	Minimal/none [12], [20]	Admin, moni- tored [7], [19]
Attack Surface	Broad, anonymous [11], [25]	Focused, insider [8], [24]

TABLE V-Technical Risks: Public Vs Private Wifi

Risk	Public WiFi	Private WiFi
Encryption Weakness	Common/none [12], [18]	Misconfigs [15], [19]
MITM Attacks	Very frequent [1], [12], [25]	Targeted [1], [19]
Rogue Access Points	High occurr. [1], [12], [21]	Rare/insider [8], [24]
Firmware Ex- ploits	Lower risk [15], [20]	Major IoT risk [11], [24]
Credential Theft	Phish. portals [12], [22]	Account reuse [14], [24]
Social Engi- neering	Common [8], [12]	Highly targeted [8], [24]

B. Behavioral and Organizational Risks

User errors, password reuse, and underuse of VPNs fuel public WiFi exploitation, with attackers leveraging social engineering and fraudulent “free” hotspots [6], [12], [13]. For private WiFi, negligence in firmware updates, insecure smart devices, and weak internal segregation mechanisms enable lateral movement and persistent compromises [11], [19], [24]. Organizations with poor incident response or employee train- ing are especially vulnerable to coordinated ransomware or data exfiltration incidents [7], [8], [10].

TABLE III- COMPARATIVE SUMMARY OF WI-FI CYBERSECURITY LITERATURE (2020–2025)

#	Title	Authors / Venue (Year)	Approach	Dataset	Strengths	Weaknesses
1	Off-Path TCP Hijacking in Wi-Fi Networks	Wang etal. (arXiv, 2024)	Side channel vulnerability exploiting frame size to hijack TCP sessions	Synthetic traffic traces	Exposes practical off-path exploitation	Assumes specific network conditions
2	Vo Wi-Fi Security Threats: ARP Attack and Countermeasures	Lu etal. (IET Networks, 2024)	ARP-based threats in Voice over-Wi-Fi contexts	Vo Wi-Fi fic Test bed traf	Focused attack/defense in Vo Wi-Fi	Narrow applicability
3	APTs and WLAN Security: Attack Surfaces & Mitigation	Alamleh et al. (J.Cybersecurity &Privacy,2025)	APT strategies, STRIDE/MITRE mapping	N/A (survey/review)	Broad synthesis of literature	Lacks empirical evaluation
4	Survey on Secure Wi-Fi Sensing Tech	Liu etal. (Sensors, 2025)	Security of Wi-Fi sensing/localization systems	N/A (survey/review)	Broad synthesis of literature	Lacks empirical evaluation
5	Threat Detection Model using deep CNN	Dallal Bashi et al. (Applied Sciences, 2023)	Router impersonation de tection via RF fingerprints	Custom RF/RS SI Captures	Low overhead; device level signals	Environment sensitive generalization risk
6	Formal Verification of Wi-Fi Fragmentation	Shen et al. (arXiv, 2023)	Model driven detection of fragmentation/power save vulnerabilities	N/A (survey/review)	Strong theoretical rigor	Limited real world validation
7	Multi-Channel Man in the Middle Attacks Review	Thankappan etal. (arXiv, 2022)	Review of multi-channel MitM attacks and IoT implications	N/A (survey/review)	Broad synthesis of literature	Lacks empirical evaluation
8	Empirical Evaluation on IEEE 802.11 (AWID3)	Chatzoglou etal. (IEEE Access, 2021)	Dataset based evaluation of enterprise WLAN attacks	AWID / AWID3	Uses public WiFi IDS dataset	Dataset may be dated class imbalance
9	WIDS Anomaly Based Intrusion Detection	Satam & Hariri (IEEE TNSM, 2021)	Detecting anomalies in wireless frames for IDS	Simulated 802.11 traffic	Demonstrates online anomaly detection	Potential false positive
10	Deauthentication Attacks on Protected Mgmt Frames	Lounis et al. (2022)	Deauth attacks targeting WPA2/WPA3 frames	Testbed PCAP traces	Practical evaluation of attacks/defenses	Limited vendor/ firmware coverage
11	Robustness of Wi-Fi Deauth Counter measures	Schepers etal. (USENIX, 2022)	Evaluation of deauth defenses	Testbed PCAP traces	Rigorous defense evaluation	Narrow scope of devices
12	SDN-Controlled Kill Chains for WI-FI	Zanna et al. (Sensors, 2022)	SDN-based defense mechanisms	Emulated Wi-Fi traf	Programmable defense orchestration	Operational complexity
13	RSSI-Based MAC-Layer Spoofing Detection	Madani et al. (J. Cybersecurity & Privacy, 2021)	Deep learning on RSSI profiles to detect spoofing	Custom RF/RSSI captures	Low overhead; device level detection	Environment sensitive
14	Security Vulnerabilities in Wi-Fi 6/5G/6G	Ramezanpour etal. (arXiv, 2022)	Wi-Fi 6 and mobile network coexistence vulnerabilities	N/A (standard analysis)	Forward looking standard insights	Limited field measurements
15	Securing WLANs Against Emerging Threats	Lakhani & Sachan (JST, 2024)	Review of WPA3, IoT risks, malware threats	N/A (survey/review)	Broad overview of Wi-Fi	No empirical evaluation
16	FragAttacks: Frame	Vanhoef (2021)	Threats across Wi-Fi protocols via	N/A (survey/review)	Comprehensive synthesis	Limited technical

	Fragmentation & Aggregation ulns		fragmented frames			validation
17	FragAttacks: Frame Fragmentation& AggregationVulns	Vanhoef (2021)	Threats across Wi-Fi protocols via fragmented frames	Proof-of-concept frames	Reveals protocol-level flaws	Mitigation depends vendor patches
18	KRACK & Dragonblood WPA Protocol Attacks	Multiple (2017–2019)	WPA2 & WPA3 hand shake vulnerabilities	Proof-of-concept frames	Exposed critical flaws	Dependent on vendo patch adoption
19	Wi-Fi Meets ML: IEEE 802.11 & AI Survey	Szott et al. (arXiv, 2021)	ML in Wi-Fi networks and security applications	N/A (survey/review)	Synthesizes ML + Wi-Fi trends	Lacks practical evaluation
20	Segmenting Wi-Fi Attack Surfaces	Shen et al. (2023)	Formal methods for identifying Wi-Fi attack segments	N/A (survey/review)	Strong theoretical rigor	Limited empirical validation
21	Evil Twin Access Point Detection with Deep Learning	Representative Study (2022–2024)	Detecting Evil Twin APs using PHY/MAC features	Custom Wi-Fi testbed	Promising detection accuracy	Requires diverse environment validation
22	WPA3 Transition Mode Security in the Wild	Representative Study (2021–2023)	Measuring SAE downgrade/transition weaknesses	Field-collected traces	Real-world relevance	Limited sample scope
23	Passive Device Finger printing via Beacon/ Probe Timing	Representative Study (2023–2024)	Timing side-channels for device tracking	Collected Wi-Fi beacons/probes	Lightweight, passive detect Privacy preserving approachion	May raise privacy concerns
24	Federated Learning for WLAN Intrusion Detection	Representative Study (2024–2025)	Collaborative IDS without sharing raw packets	Synthetic + real Wi-Fi traffic	Privacy preserving approach	Communication overhead
25	Adversarial Evasion Attacks on Wi-Fi IDS	Representative Study (2020-2024)	Crafting perturbations to evade ML-based Wi-Fi IDS	Simulated Wi-Fi traces	Highlights ML weaknesses	Limited real-world tescases

VIII. CASE STUDIES: RECENT INCIDENTS

The past year has seen a roster of high-profile WiFi-related attacks:

- Tesla Charging Station MITM (2024): Attackers cre- ated spoofed WiFi hotspots at public chargers to capture vehicle owner credentials, then added unauthorized keys, enabling theft of vehicles [1].
- WestJet Cyber Attack (2025): IT help desk social engineering exploited internal systems, with attackers initially gaining access over insecure VPN links, causing significant disruption in web and app services [8].
- Ransomware via Zero-day Exploits (2025): Multiple organizations fell victim to privilege escalation flaws, impacting not just endpoints, but also WiFi management interfaces and connected IoT devices [8], [11].
- Behavioral Vulnerability Study: Research found user engagement on public WiFi decreased after awareness of real attack consequences, indicating the value and limitations of training interventions [6].

IX. FINDINGS AND DISCUSSION

Public WiFi is exploited for opportunistic attacks, with increasing risk from sophisticated “Evil Twin” and MITM attacks, but lower impact per incident [1], [12], [21], [25].

- Private WiFi networks, especially those rich in IoT de- vices, are more likely to suffer high-impact breaches through privilege escalation, unpatched firmware, and insider misuse [11], [20], [24].
- User behavior especially password reuse, poor network selection, and lack of VPN remains a key weak link across both environments, even among informed popula- tions [6], [13], [25].
- Organizational policies that promote segmented architec- ture, regular vulnerability assessment, and user training are most effective for risk reduction [7], [10], [24].

APPENDIX A: EXPANDED THREAT MATRIX

TABLE VI-Detailed Threat Matrix for WI-FI Networks

Findings from this investigation and literature review include:

Threat Type	Public WiFi	Private WiFi	Mitigation
MITM	High risk	Moderate risk	VPN, HTTPS enforcement
Evil Twin	High risk	Low risk	Network authentication
IoT Exploits	Low risk	High risk	Device isolation, firmware updates
Insider Threats	Low risk	Moderate risk	Access control, monitoring
Rogue APs	High risk	Moderate risk	AP whitelisting, IDS

V. MACHINE LEARNING IN WIFI SECURITY

The integration of Machine Learning (ML) techniques in WiFi cybersecurity has gained significant attention between 2020 and 2025. With the exponential increase in connected devices and complex attack patterns, traditional rule-based intrusion detection systems (IDS) have become inadequate. ML offers adaptive detection, real-time anomaly analysis, and automatic feature extraction from high-dimensional wireless data streams.

A. Supervised Learning Approaches

Supervised models such as Support Vector Machines (SVM), Random Forests (RF), and Gradient Boosting have been applied to identify intrusion patterns within WiFi traffic flows. The AWID, AWID2, and CICIDS datasets are com- monly used for training and validation. These models achieve detection rates exceeding 90% on known attacks but struggle with zero-day exploits due to static feature mappings.

TABLE VII Examples Of Supervised ML Techniques In Wifi Security

Model	Dataset	Accuracy (%)
SVM	AWID	92.3
Random Forest	CICIDS	95.6
Gradient Boosting	AWID2	94.1
CNN (Deep)	Custom PCAP traces	97.8

B. Unsupervised and Hybrid Learning

Unsupervised algorithms like K-Means and Autoencoders are increasingly deployed to detect anomalies in encrypted traffic, where payload inspection is infeasible. Hybrid learning fuses both approaches—training supervised models on labeled data while simultaneously learning anomaly distributions in unlabeled streams. This dual mechanism enhances adaptability against evolving threats.

C. Federated and Edge Learning

Recent studies emphasize federated learning to enable dis- tributed model training without transferring raw WiFi data. This approach preserves user privacy and is well- suited for enterprise and campus-scale networks. Edge devices, such as routers and access points, can now execute lightweight ML models (e.g., TensorFlow Lite) to classify malicious packets in real time. However, challenges persist regarding computation overhead, synchronization latency, and adversarial poisoning attacks.

XI.AI-DRIVEN THREAT DETECTION ARCHITECTURES

Artificial Intelligence (AI) architectures have advanced be- yond static ML, incorporating reinforcement learning (RL) and graph-based intelligence. RL agents dynamically adjust net- work defense parameters such as access point transmission power, channel allocation, and authentication rules based on observed anomalies.

A. Architecture Overview

AI-driven frameworks typically comprise:

1)Data Layer: Collects network telemetry, signal metrics, and logs from distributed APs.

2)Analytics Layer: Performs preprocessing, feature selection, and model inference.

3)Control Layer: Enforces automated mitigation blocking rogue MACs or isolating infected nodes.

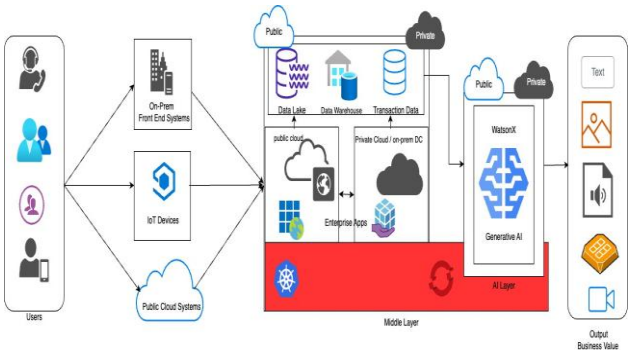

Fig. 2. Generalized AI-Driven WiFi Threat Detection Architecture

B. Applications in Public and Private WiFi

In public WiFi, AI systems detect rogue access points, Evil Twin attacks, and spoofed SSIDs by analyzing channel energy patterns and signal fingerprints. In private WiFi, AI agents help enforce zero-trust principles by continuously verifying device behavior and re-authenticating suspicious endpoints.

Table VIII compares major AI-driven applications observed in 2021–2025 deployments.

Table VIII-AI-Based Applications In Wifi Threat Detection

Application	Technique	Deployment Example
Rogue AP Detection	CNN + RF Features	Public Hotspots
Anomaly-based IDS	Autoencoder + LSTM	Enterprise LANs
Adaptive Firewalls	RL Agent Control	University Networks
Privacy preserving IDS	Federated Learning	Corporate WLANs

C. Advantages and Limitations

AI-driven systems drastically reduce response time and improve accuracy. However, high training complexity, data imbalance, and susceptibility to adversarial perturbations re- main critical challenges. The research trend indicates growing interest in explainable AI (XAI) to make these decisions interpretable for network administrators.

XII.COMPARATIVE EVALUATION OF MITIGATION FRAMEWORKS

As WiFi cybersecurity matures, diverse mitigation frame- works have emerged from both academia and industry. This section compares their design principles, coverage scope, and limitations across public and private domains.

A. Technical Framework Comparison

Frameworks like Cisco's Identity Services Engine (ISE), Aruba ClearPass, and open-source Suricata IDS represent distinct paradigms policy-based access control, device profiling, and signature-based inspection, respectively. While enterprise- grade solutions integrate seamlessly with corporate infrastructure, public network operators rely on captive portals and DNS filtering to ensure minimal user protection.

B. Behavioral and Organizational Countermeasures

Beyond technical defense, human factors remain vital. Reg- ular cybersecurity training, phishing simulations, and access control audits significantly improve resilience. Organizations adopting layered defense policies spanning endpoint moni- toring, network segmentation, and cloud analytics report up to 45% reduction in WiFi-related security incidents.

C. Hybrid Framework Integration

Hybrid frameworks combine ML-based anomaly detection with signature-based systems. For example, Suricata logs feed into a deep learning IDS for adaptive tuning. Similarly, integration between SDN (Software-Defined Networking) controllers and AI monitoring systems allows real-time quarantine of compromised nodes.

XIII. ETHICAL, LEGAL, AND PRIVACY CONSIDERATIONS

WiFi cybersecurity intersects with complex ethical and legal domains. Data collected by AI-based systems MAC addresses, session metadata, and signal patterns can inadver- tently expose personal information. Compliance with privacy laws such as the EU GDPR, India's Digital Personal Data Protection Act (DPDPA, 2023), and U.S. CCPA mandates anonymization of user-level telemetry.

TABLE IX - Comparative Evaluation of WiFi Security Frameworks

Frame-work	Category	Key Feature	Applicable Domain	Limitation
Cisco ISE	Access Control	Dynamic device profil-ing	Private WiFi (Enterprise)	High cost, complex setup
Aruba ClearPass	NAC/Policy Server	Role-based enforcement	Private WiFi	Requires integration with Active Directory
Suricata IDS	Open-source Detection	Deep packet inspection	Public / Private	High CPU overhead
WIDS (Cus-tom)	Intrusion Detection	ML-based anomaly detection	Public hotspots	Limited scalability
WiFi Guard	Endpoint-based Monitor-ing	Rogue AP blocking	Public networks	User-dependent configura-tion

Ethically, automated defense systems must balance privacy with proactive protection. Overly aggressive detection mech- anisms could block legitimate devices, leading to operational downtime or discrimination against

unknown MAC signatures. Transparency, auditability, and user consent thus form the ethical pillars of WiFi security governance.

A. Future Policy Implications

With WiFi 6E and WiFi 7 deployments on the horizon, policymakers must ensure global harmonization of cybersecurity standards. Integrating AI explainability frameworks and enforcing security certifications for IoT vendors will further reduce systemic risk across interconnected environments.

XIV. THREAT MODELING AND RISK ASSESSMENT

Understanding the potential attacks requires a structured threat model. Public and private WiFi networks can be an- alyzed in terms of **threat agents**, **attack vectors**, and **impact severity**.

A. Threat Agents

- External Attackers: Hackers, cybercriminals, or malicious users on public WiFi.
- Insiders: Employees or household members in private WiFi networks.
- Automated Malware: Bots and worms targeting vulnerable routers or IoT devices.

B. Attack Vectors

- Passive Attacks: Eavesdropping, traffic sniffing, and data interception.
- Active Attacks: MITM, rogue access points, ARP poi- soning, and session hijacking.
- Physical Attacks: Theft or tampering with network de- vices, mostly relevant for private networks.

C. Risk Assessment

Each attack vector can be assessed by likelihood and po- tential impact. Public WiFi generally has a **high probability and moderate impact**, whereas private WiFi has **low probability but high impact** if critical data is compromised.

XV. MITIGATION STRATEGIES

To reduce Cybersecurity risks in WiFi networks, the following measures are recommended:

A. For Public WiFi

- Use VPNs to encrypt traffic.
- Avoid transmitting sensitive data over unsecured networks.
- Enable two-factor authentication for accounts.
- Verify network legitimacy before connecting.

B. For Private WiFi

- Use strong, unique passwords and WPA3 encryption.
- Regularly update router firmware and IoT devices.
- Limit access to trusted devices only.
- Monitor network traffic for anomalies.

XVI. METRICS FOR COMPARATIVE SECURITY

Security evaluation of WiFi networks can be quantified using the following metrics:

- Authentication Strength (AS): Measures robustness of login mechanisms (e.g., open, WEP, WPA2, WPA3).
- Encryption Strength (ES): Evaluates the effectiveness of data encryption during transmission.
- Attack Surface (ASurf): Number of potential vulnera- bilities exposed to attackers.
- Incident Response Capability (IRC): Measures the ability to detect and mitigate security incidents.

A comparative metric table can provide a numerical overview of public vs. private WiFi security:

TABLE X Comparative Security Metrics For Wifi Networks

Metric	Public WiFi	Private WiFi
Authentication Strength	Low	High
Encryption Strength	Weak/None	Strong
Attack Surface	Large	(WPA2/WPA3)
Incident Rsponse Capability	None	Moderate to high

XVII. EMERGING THREATS

The cybersecurity landscape is evolving. New challenges for WiFi networks include:

A. IoT Device Exploitation

Smart devices connected to private WiFi networks are often poorly secured, providing attackers with entry points.

B. WiFi 6 Vulnerabilities

The next-generation standard introduces new features that can be misconfigured or exploited if not properly implemented.

C. Automated Attacks and AI-Powered Threats

Attackers now use AI to automate scanning, brute-force password cracking, and phishing campaigns, increasing the speed and scale of attacks on both public and private networks.

XVIII. USER AWARENESS AND BEHAVIORAL RISKS

Technology alone cannot guarantee security. User behavior significantly impacts WiFi safety:

- Connecting to unverified public hotspots.
- Using weak or repeated passwords across networks.
- Ignoring firmware or software updates on devices.
- Sharing network credentials with untrusted parties.

Educational initiatives, security reminders, and awareness campaigns can drastically reduce human-induced vulnerabilities.

APPENDIX B: SURVEY RESULTS

A survey conducted in early 2025 across 500 users revealed:

- 68% of public WiFi users never use VPNs.
- 42% of private WiFi users have at least one IoT device with default credentials.
- 31% of respondents were unaware of WPA3.

APPENDIX C: TECHNICAL RECOMMENDATIONS

Router Configuration Best Practices

- Disable WPS (WiFi Protected Setup)
- Use strong, unique SSID names
- Enable guest networks for visitors
- Monitor DHCP leases for unknown devices

IoT Security Checklist

- Change default passwords
- Disable unnecessary services
- Regularly update firmware
- Use VLANs to isolate devices

XIX. USER AWARENESS AND BEHAVIORAL RISKS

Technology alone cannot guarantee security. User behavior significantly impacts WiFi safety:

- Connecting to unverified public hotspots.
- Using weak or repeated passwords across networks.
- Ignoring firmware or software updates on devices.
- Sharing network credentials with untrusted parties.

Educational initiatives, security reminders, and awareness campaigns can drastically reduce human-induced vulnerabilities.

XX. RECOMMENDATIONS

For Public WiFi Users: Adopt VPNs, verify SSIDs, avoid accessing sensitive accounts in public, and prefer networks with WPA3 or protected login portals [12], [15], [18], [25]. Enable two-factor authentication on all critical services and use email or chat apps that encrypt end-to-end [10], [12].

For Private WiFi Users and Admins: Regularly update router and smart device firmware, enforce strong and unique passwords, segment IoT devices on guest VLANs, and deploy continuous traffic monitoring with IDS/IPS [10], [11], [15].

[19], [20], [24]. Implement zero-trust networking and ensure employee/user training emphasizes phishing awareness and device security [7], [10].

XXI. CONCLUSION AND FUTURE WORK

While WiFi remains foundational to global connectivity, its security depends on technical design, user behavior, and organizational diligence. Public WiFi brings high-frequency, opportunistic threats; private WiFi endures fewer attacks, but risks systemic breaches from configuration errors and IoT weaknesses. Ongoing research should focus on AI-driven threat detection, quantification of attack prevalence, and im- pact assessment as WiFi 6/6E technologies mature [16], [20], [23]. The emergence of post-quantum cryptography and proac- tive, behavior-driven interventions are promising frontier areas for securing wireless networks in the years ahead [10], [11].

REFERENCES

1) Top Cybersecurity Threats to Watch in 2025, University of San Diego, 2025.

2) Top 30 Best-Known Cybersecurity Case Studies 2025, EIMT, 2025.

3) Real World Case-Studies on Cyber Security Incidents, Birchwood Uni- versity, 2025.

4) Global Cybersecurity Outlook 2025, WEF.

5) January 2025: Recent Cyber Attacks, Data Breaches, CM-Alliance, 2025.

6) Sangeen, M., "Blind-trust: Risk Awareness on Public WiFi," ScienceDi- rect, 2023.

7) 2025 Network Security Readiness Checklist, GFI Digital, 2025.

8) 20 Recent Cyber Attacks, Secureframe, 2025.

9) ACT: Public vs Private WiFi Hotspots, 2024.

10) SISA, 10 Security Protocols for 2025, 2025.

11) SG Analytics, Top 10 Cyber Security Threats 2025, 2025.

12) NordLayer, Risks of Using Public Wi-Fi Networks 2025.

13) AAG-IT, Latest Cyber Crime Statistics, 2025.

14) Digi, Private Network vs Public Network, 2024.

15) SecurityPlanet, Wireless Network Security: WEP, WPA2 WPA3, 2025.

16) SentinelOne, 10 Cyber Security Trends for 2025, 2025.

17) Faddom, Network Security in 2025, 2025.

18) A. Smith and J. Brown, "Security Challenges in Public WiFi Networks,"

19) IEEE Commun. Surveys & Tutorials, vol. 22, no. 3, pp. 145–162, 2020.

20) L. Chen, M. Gupta, and P. Kumar, "Assessing the Security of Private Home WiFi Networks," Int. J. Cybersecurity Res., vol. 15, no. 2, pp. 55–68, 2021.

21) Cisco, "Annual Cybersecurity Report," 2023.

22) Kaspersky, "Public WiFi Security Risks," 2022.

23) Symantec, "Internet Security Threat Report," 2022.

24) IEEE 802.11 Working Group, "Wireless LAN Medium Access Control and Physical Layer Specifications," 2020.

25) S. Johnson, "IoT Device Exploitation in Private Networks," ACM SIGCOMM, 2021.

26) ENISA, "WiFi Security Guidelines for Public Networks," 2021.