Unified Public Wi-Fi Security Monitoring System for Smart Cities

1st Md. Hadique
Department of AIT CSE
Chandigarh University
Mohali, Punjab
mdhadique999@gmail.com

2nd Shail Gupta
Department of AIT CSE
Chandigarh University
Mohali, Punjab
shailgupta278@gmail.com

3rd Jahir
Department of AIT CSE
Chandigarh University
Mohali, Punjab
jk0786j@gmail.com

4th Komal Mehta
Department of AIT CSE
Chandigarh University
Mohali, Punjab
komal.e15888@cumail.in

***Abstract*—The proliferation of smart cities is fundamentally dependent on ubiquitous connectivity, with public Wi-Fi networks serving as a critical infrastructure. This connectivity, however, introduces a complex and expansive attack surface. Existing security paradigms are often fragmented, device-centric, and incapable of providing a holistic, city-wide security posture. This paper proposes an Integrated Cybersecurity Framework (ICF) designed to unify security monitoring across all public Wi-Fi access points within a smart urban environment. The ICF integrates a centralized management plane with distributed sensors, leveraging a hybrid threat detection model that combines signature-based analysis with machine learning-based anomaly detection[1]. Key components include real-time data aggregation, automated incident response, and a unified security dashboard for municipal operators. This framework aims to provide a scalable, proactive, and resilient security solution that not only protects users from common threats (e.g., Man-in-the-Middle, rogue APs) but also secures the underlying smart city services that rely on this network infrastructure.**

***Index Terms*—Smart City, Cybersecurity, Public Wi-Fi, Network Security, Intrusion Detection System (IDS), Anomaly Detection, Unified Security, IoT Security, Threat Monitoring**

I. Introduction

The 21st-century urban landscape is being transformed by the ”smart city” concept, which leverages data and technology to improve the efficiency of services and the quality of life for its citizens. A cornerstone of this digital transformation is the provision of free and accessible public Wi-Fi. This infrastructure supports everything from citizen internet access and e-governance portals to critical Internet of Things (IoT) deployments, such as smart traffic management, connected utilities, and public safety systems[2]. While this connectivity fosters innovation and inclusivity, it simultaneously creates significant cybersecurity vulnerabilities. The open and broadcast nature of public Wi-Fi makes it a prime target for malicious actors. Threats range from passive data interception and session hijacking to active attacks like rogue access points, ”Evil Twin” spoofing, and Denial of Service (DoS) attacks[4]. The core problem is not a lack of security tools, but a lack of integration. A typical city may deploy security solutions from various vendors, resulting in isolated security ”silos.” An alert on one network node provides no context to the rest of the city’s network, making it impossible to detect large-scale, coordinated attacks. This research addresses this gap by proposing a unified framework that centralizes monitoring, analysis, and response, thereby creating a cohesive and intelligent defense mechanism for the entire urban Wi-Fi ecosystem.

II. Related Work

Significant research has been conducted on the vulnerabilities of public wireless networks. Early studies focused heavily on protocol-level weaknesses in WEP and WPA, while more recent work examines the risks of open, unencrypted networks, particularly the prevalence of Manin-the-Middle (MitM) attacks in public hotspots[7]. In response, solutions such as Wireless Intrusion Prevention Systems (WIPS) have been developed to detect and block unauthorized access points. Furthermore, numerous studies have proposed the use of machine learning (ML) and artificial intelligence (AI) for anomaly detection in network traffic, moving beyond static, signature-based methods. These approaches are adept at identifying zero-day attacks and novel threat patterns[1][8]. However, a review of the current literature reveals a persistent gap: the lack of a holistic, scalable, and citywide management framework. Most proposed solutions 1 are localized, designed to protect a single enterprise or campus, not a sprawling, heterogeneous municipal network. They often fail to integrate with other critical smart city systems[9]. This paper builds upon existing research in anomaly detection and intrusion detection but distinguishes itself by focusing on the architectural challenges of centralization, scalability, and cross-domain integration for a complete smart city environment.

III. Methodology

The proposed Integrated Cybersecurity Framework (ICF) is founded on a centralized, multi-layered security methodology. The objective is to ingest, analyze, and act upon security telemetry from every public access point in real-time.
The core methodology follows a four-stage process :

A. Unified Data Ingestion:

All network access points (APs) and controllers are configured to stream relevant data (e.g., traffic flows, connection logs, device metadata) to a central data lake.

B. Hybrid Analysis Engine

The ingested data is processed by a hybrid engine. A signature-based IDS scans for known threats, while an ML-based anomaly detection module flags statistically significant deviations.

C. Automated Orchestration

Upon detection, alerts are fed into a Security Orchestration, Automation, and Response (SOAR) system [3] to initiate an automated response.

D. Centralized Visualization

All data, alerts, and actions are presented in a unified dashboard for operators.

ADVANTAGES

- **Unified Visibility:** Provides a ”single-pane-of-glass” view of the entire city’s Wi-Fi security posture.
- **Proactive Threat Detection:** The ML component can identify zero-day attacks that signature-based systems miss
- **Proactive Threat Detection:** The ML component can identify zero-day attacks that signature-based systems miss
- **Scalable Architecture:** The framework is modular, allowing the city to add new zones, APs, or IoT sensors.
- **Data-Driven Insights:** Aggregated data provides valuable insights into network usage and threat patterns.

CONS

- **High Initial Investment:** Requires significant investment in a central processing platform, storage, and software.
- **Implementation Complexity:** Integrating with diverse, multi-vendor legacy network equipment can be challenging
- **Potential for False Positives:** ML-based anomaly detection can generate false alarms, requiring careful tuning.
- **Data Privacy Concerns:** Centralized collection of metadata raises privacy implications, necessitating robust anonymization and governance[2].
- **Single Point of Failure:** A centralized system requires careful design for high availability and redundancy

IV. IMPLEMENTATION

The practical implementation of the ICF is divided into three distinct functional layers:

A. Network Data Collection

This layer acts as the sensory grid of the framework.

- **Packet Sniffing& Flow Analysis:** Lightweight agents capture packet metadata and traffic flow information.
- **Centralized Logging:** All APs, firewalls, and authentication servers forward their logs to a central aggregator.
- **Device Fingerprinting:** The system actively and passively fingerprints connected devices to identify device types and detect spoofing.

B. Threat Detection and Analysis

This is the ”brain” of the operation, where raw data is turned into actionable intelligence.

- **Signature-Based Detection:** A ruleset engine scans traffic for known attack patterns and malware signatures.
- **Anomaly Detection:** ML models are trained on a baseline of normal network activity to detect deviations[6] .
- **Threat Correlation:** The system correlates alerts from multiple sources to identify distributed attacks.

C. Automated Response and Mitigation

When a high-confidence threat is identified, this layer takes action.

- **Session Termination:** The system can automatically send a de-authentication packet to disconnect a malicious user[11].
- **Device Quarantine:** The system can place a compromised device into a firewalled ”quarantine” VLAN.
- **Alerting and Reporting:** Generates an alert on the central dashboard for a human analyst to investigate.

V. SYSTEM ARCHITECTURE

The proposed system architecture is multi-tiered, ensuring separation of concerns and scalability.

1) **Edge Layer:** Consists of all public-facing Wi-Fi Access Points, which serve as the primary sensors[13].
2) **Aggregation Layer:** A series of data collectors, or ”aggregators,” are deployed regionally to normalize and forward data.
3) **Core Processing Layer:** A central data center (or cloud environment) that hosts the main components: Data Lake, Real-time Analysis Engine, Security Incident Management (SIM) System, and Automation Engine (SOAR).
4) **Interface & Integration Layer:** Contains the Unified Security Dashboard for human operators and APIs to connect to other smart city platforms.

VI. SMART CITY INFRASTRUCTURE INTEGRATION

The true value of this framework is its ability to protect not just Wi-Fi users, but the critical city infrastructure that shares the network[9].

- **Traffic Management:** If an attacker compromises a smart traffic light via an adjacent AP, the ICF can detect the intrusion and lateral movement, quarantining the AP.
- **Public Safety:** The system ensures the integrity of data for first responders who may use public Wi-Fi on their mobile data terminals.
- **Utilities:** The ICF provides a security overlay to monitor smart utility meters for anomalous behavior that could indicate a service disruption attack.
- **Incident Correlation:** By integrating with CCTV, the system can correlate a ”Wi-Fi jamming” alert with a physical event, automatically notifying security cameras [12].

VII. Results and Outcome

The deployment of this framework is projected to yield four principal outcomes:

1) **Enhanced Threat Detection:** The hybrid AI/signature model provides superior detection rates, moving the city from a reactive to a proactive security posture.
2) **Centralized Data Aggregation:** All network and security data is consolidated, providing unified visibility and streamlining compliance and forensics.
3) **Real-Time Alerting and Response:** Automated mitigation actions reduce the ”dwell time” of an attacker from days to seconds, minimizing damage.
4) **User Behavior Insights and Policy Optimization:** The system provides a macro-level view of network usage, which can be used to optimize network performance and craft data-driven security policies.

VIII. Future Scope

This framework serves as a foundational platform for future security advancements.

1) **Expansion to City-Wide IoT:** The framework can be expanded to monitor all connected IoT devices in the city (LoRaWAN, 5G, etc.)[8].
2) **Predictive AI Models:** Future work will focus on moving from anomaly detection to threat prediction, patching vulnerabilities before they are exploited.
3) **Blockchain-Based Authentication:** Explore blockchain-based decentralized identities (DIDs) for user authentication to enhance privacy.
4) **Federated Learning:** To address privacy concerns, ML models could be trained at the ”edge” using federated learning, keeping raw data localized.

IX. CONCLUSION

The Unified Public Wi-Fi Security Monitoring System represents a critical evolution in municipal cybersecurity. By treating the entire city’s Wi-Fi network as a single, cohesive entity, this framework overcomes the critical limitations of isolated, siloed security solutions. It provides a scalable, intelligent, and automated defense mechanism that is essential for protecting both citizens and the critical services they rely on. This research demonstrates that as cities become ”smarter” and more connected, their security architectures must evolve in parallel. A unified framework is no longer an optional upgrade; it is a fundamental requirement for building resilient, trustworthy, and efficient urban environments. This work provides a comprehensive blueprint for municipalities to secure their digital future.

References

[1] Chen, L., & Li, J. (2024). ”Machine Learning for ZeroDay Threat Detection in IoT Networks.” IEEE Transactions on Information Forensics and Security, 19, 45-59..

[2] Gupta, R., & Tanwar, S. (2023). ”Security and Privacy Challenges in Smart City Public Wi-Fi: A Comprehensive Review.” Journal of Network and Computer Applications, 210, 103521.

[3] Al-Hamadi, H., & Al-Amri, J. (2024). ”A SOARbased Framework for Automated Incident Response in Smart City Infrastructures.” Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP).

[4] Patel, D., & Shah, M. (2023). ”Vulnerabilities of Public Wireless Networks: An ’Evil Twin’ and MitM Attack Analysis.” International Journal of Computer Security & E-Learning, 12(1)

[5] European Union Agency for Cybersecurity (ENISA). (2023). Guidelines on Securing Smart City Services. ENISA Report.

[6] Chen, L., & Li, J. (2024). ”Machine Learning for Zero-Day Threat Detection in IoT Networks.” *IEEE Transactions on Information Forensics and Security*, 19, 45-59.

[7] Gupta, R., & Tanwar, S. (2023). ”Security and Privacy Challenges in Smart City Public Wi-Fi: A Comprehensive Review.” *Journal of Network and Computer Applications*, 210, 103521.

[8] Al-Hamadi, H., & Al-Amri, J. (2024). ”A SOAR-based Framework for Automated Incident Response in Smart City Infrastructures.” *Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP)*.

[9] Patel, D., & Shah, M. (2023). ”Vulnerabilities of Public Wireless Networks: An ’Evil Twin’ and MitM Attack Analysis.” *International Journal of Computer Security & E-Learning*, 12(1).

[10] European Union Agency for Cybersecurity (ENISA). (2023). *Guidelines on Securing Smart City Services*. ENISA Report.

[11] Ali, M., et al. (2021). ”Anomaly detection in large-scale public Wi-Fi networks.” *Journal of Network and Computer Applications*, 178, 102971.

[12] Conti, M., et al. (2021). ”A Survey on Man-in-the-Middle attacks in smart public Wi-Fi.” *Computer Communications*, 173, 25-47.

[13] Baig, Z., et al. (2021). ”Machine learning approaches to IoT security: A systematic review.” *IEEE Access*, 9, 155779-155809.

[14] Lo´pez, J., et al. (2021). ”Cyber resilience in smart city infrastructures.” *IEEE Transactions on Industrial Informatics*, 17(6), 4319-4328.

[15] Cisco Systems. (2022). ”Public Wi-Fi Security: Threats and Best Practices.” *Cisco White Paper*.