Optimized WiFi Network Deployment with OpenWRT and FreeRadius for Secure and Scalable Connectivity

Vihar Kuruppathukattil
East Carolina University
vih1310@gmail.com

***Abstract*—An innovative method for deploying a cost-effective and high-performance WiFi network is explored, focusing on OpenWRT-based routers and FreeRadius authentication. By standardizing hardware with TpLink WRT4300 devices and utilizing a custom OpenWRT firmware, seamless network management and easy device replacement are achieved. WPA2-Enterprise authentication, powered by a FreeRadius server on a Raspberry Pi 2, enhances security by providing unique credentials to users without requiring costly enterprise hardware. The proposed system ensures uninterrupted connectivity with multiple access points while enabling future integration with IoT and smart home automation. Designed for scalability and reliability, this approach delivers enterprise-grade security and performance while maintaining affordability for multi-user environments.**

***Index Terms*—Wireless networks, network security, authentication, WPA2-Enterprise, RADIUS, OpenWRT, virtual LAN, access control, IoT infrastructure.**

I. Introduction

The global WiFi market is anticipated to witness substantial expansion in the coming years. This rapid growth is primarily driven by the proliferation of smart devices, including but not limited to mobile phones, tablets, smartwatches, smart televisions, and other connected appliances. The trend observed among users indicates that the highest volume of data consumption occurs when devices are stationary and connected to WiFi networks in environments such as homes, offices, commercial establishments, and public infrastructure. Despite the declining costs of mobile data services, it remains common practice for users to configure smart devices to execute data-intensive operations, such as software updates, cloud synchronization, and media downloads, exclusively when connected to WiFi networks. This behavior underscores the criticality of reliable and secure WiFi infrastructure in contemporary digital ecosystems.

Historically, the emphasis on network security was predominantly placed on safeguarding against external cyber threats through mechanisms such as firewalls, encryption protocols, and public key cryptography. However, a paradigm shift has been observed in recent years, with security concerns increasingly focusing on internal threats. The necessity to secure vital network resources from potential vulnerabilities originating within the network itself has become a major area of concern. This challenge is particularly pronounced for small and medium-sized enterprises (SMEs) and rental housing facilities, where a growing demand for widespread WiFi accessibility must be balanced against the need for robust security measures. Such environments require cost-effective solutions that facilitate secure authentication and access management for individual users while enabling real-time network monitoring to detect and mitigate unauthorized activities.

Furthermore, the scope of network security is no longer limited to conventional computing devices such as laptops and smartphones. The emergence of the Internet of Things (IoT) has led to an unprecedented increase in the number of connected devices, surpassing traditional endpoints. The deployment of IoT devices introduces additional security challenges, necessitating the segregation of such devices from general-purpose networks and the implementation of dedicated security protocols. For certain IoT applications, particularly those related to critical infrastructure, healthcare, and industrial automation, ensuring high network reliability and low-latency communication is imperative.

Another significant concern pertains to WiFi piggybacking, wherein unauthorized users gain access to a network without explicit permission. Beyond the immediate risk of bandwidth theft, unauthorized access poses serious legal and ethical implications. Individuals engaging in illicit activities, such as cybercrimes, unauthorized file sharing, or accessing prohibited content, may exploit the network to mask their identity, potentially implicating the legitimate network owner in unlawful activities. Even in cases where authorized users are involved in policy violations, the inability to trace network activity back to specific individuals may result in legal repercussions for the network administrator. Thus, implementing mechanisms for user authentication, session tracking, and activity logging is essential to mitigate such risks.

This study presents an approach for designing and deploying an internal WiFi network within a medium-sized rental housing facility. The primary objective extends beyond merely providing network access to tenants; it also aims to establish a foundational infrastructure for a planned smart home ecosystem. The integration of intelligent devices and automation

systems requires a secure and efficient network framework capable of managing multiple interconnected devices without compromising performance or security.

It is important to acknowledge that access control and network monitoring represent only a subset of the broader domain of cybersecurity. While this study focuses on aspects related to access management, unauthorized usage prevention, and tenant activity monitoring, other critical security concerns, such as protection against data breaches, network integrity attacks, and denial-of-service (DoS) threats, fall beyond the scope of this paper. Given the specific use case of the proposed network installation, additional security measures targeting these advanced threats were deemed unnecessary within the present framework.

The subsequent sections of this paper will elaborate on the architectural considerations, security mechanisms, and implementation strategies adopted for the proposed WiFi network infrastructure. The discussion will encompass technical specifications, deployment methodologies, and potential challenges encountered during the implementation process. Additionally, insights into best practices for enhancing network security and ensuring regulatory compliance will be provided.

II. Network Requirements

The primary objective of this project is to design and implement a robust internal network infrastructure within a multi-unit residential building. The intended network must meet several critical functional and operational criteria to ensure reliability, security, and ease of management. The key network specifications are outlined as follows:

1) Establishment of high-speed and stable WiFi coverage across all areas of the building,
2) Cost-efficient deployment without compromising network performance and security,
3) Implementation of segregated virtual subnetworks to enhance security for sensitive devices such as surveillance systems, smart home automation units, and network-attached storage (NAS),
4) Provision of a structured and easily manageable guest network to regulate internet access on a per-user basis,
5) Development of a web-based administrative interface accessible both from within the network and remotely,
6) Configuration of secure external access via a Virtual Private Network (VPN) tunnel,
7) Establishment of a foundational framework to support future smart home integrations.

The following sections will delve into each of these requirements, providing a detailed overview of the methodologies employed in achieving these objectives.

III. High-Speed and Stable WiFi Coverage with Cost-Effective Implementation

Enterprise-grade wireless networking solutions often come equipped with extensive feature sets but are typically costly and complex to configure. For cost-sensitive deployments, a viable alternative is to utilize consumer-grade hardware that supports open-source firmware, enabling enterprise-class functionality at a fraction of the price. While this approach necessitates additional customization and potential trade-offs, it presents a compelling balance between affordability and advanced features.

This study details the deployment of a wireless network infrastructure incorporating a single primary router and six strategically positioned access points (APs) to ensure comprehensive coverage. Uniformity in hardware selection was prioritized to simplify maintenance and streamline configuration. Following an assessment of cost-effectiveness and technical specifications, the TpLink WRT4300 router was selected as the core networking hardware. This device features Gigabit Ethernet support, dual-band concurrent wireless connectivity with a combined throughput of 750 Mbps (300 Mbps on the 2.4 GHz band and 450 Mbps on the 5 GHz band), and an Atheros AR9344 chipset clocked at 560MHz with 128MB of RAM. Additionally, the unit includes hardware Network Address Translation (NAT) capable of 800 Mbps and dual USB 2.0 ports for peripheral connectivity.

To maximize flexibility and unlock advanced networking capabilities, the stock firmware was replaced with a custom-compiled OpenWRT Barrier Breaker build. The same firmware was deployed across all devices, simplifying management and ensuring seamless interoperability. By maintaining a uniform software environment, potential device failures can be mitigated efficiently by simply swapping in an identical replacement unit. Moreover, OpenWRT's package repository allows additional software installations as required, further extending network functionality.

The placement strategy for access points was meticulously planned to optimize signal distribution and minimize dead zones. Two APs were installed per floor, ensuring extensive coverage and facilitating wired LAN connections for each segment of the building. These units not only provide seamless wireless connectivity but also act as local distribution hubs for wired networking where required. In anticipation of future expansion, the USB interfaces of these APs are reserved for integration with smart home automation peripherals, such as automated utility metering and lighting control systems.

To enhance power management and minimize dependency on individual adapters, a centralized power distribution system was implemented on each floor. This approach increases reliability, reduces cable clutter, and allows for better control over the power supply to networking equipment. By employing a structured deployment strategy that balances cost efficiency with robust performance, the network infrastructure is poised to support both current and future operational demands.

IV. Separate Isolated Virtual Subnetwork for Critical Devices

To ensure network security and efficient management, a VLAN-based separation mechanism has been adopted. The primary objective of this segmentation is to establish distinct virtual subnetworks to cater to different types of network traffic, thereby enhancing security and performance. Two separate

VLANs have been configured to fulfill these requirements. The first VLAN is designated for guest access, ensuring that tenants and temporary users are granted only internet access without any direct interaction with other network resources. The second VLAN serves as the administration network, exclusively reserved for building infrastructure and administrative devices such as IP surveillance cameras, IoT-enabled smart home automation systems, and VoIP intercoms.

To realize this structured network segmentation, each access point (AP) within the building has been configured to broadcast four WiFi networks—two operating in the 2.4GHz frequency band and two in the 5GHz frequency band. However, only two distinct SSIDs are utilized across all access points: one dedicated to guest access and another assigned to the administration network. This configuration ensures seamless roaming for users, as their devices are automatically routed to the access point offering the strongest signal, thereby optimizing connectivity and user experience.

Each WiFi network is systematically mapped to a specific VLAN, ensuring that both the 2.4GHz and 5GHz frequency bands provide connectivity to both VLANs. VLAN tagging is employed on the AP switch ports that connect to the network backbone. This tagging mechanism allows the network to differentiate between traffic belonging to separate VLANs. Consequently, each AP is connected to the central router or switch via a single cable known as a trunk link, which carries multiple VLANs simultaneously. This approach minimizes cabling complexity while maintaining network segregation.

Each VLAN operates as an independent subnet, preventing unauthorized access between networks. The router is configured to restrict communication between VLANs, permitting only one-way traffic flow from the administration network to the guest network. This ensures that while network administrators can monitor and manage tenant internet usage, tenants remain isolated from critical infrastructure devices, thereby mitigating potential security threats. The use of VLANs also enhances scalability, allowing additional IoT devices or network components to be seamlessly integrated into the administration network without compromising the integrity of other network segments.

By implementing this VLAN-based architecture, the network not only ensures security and controlled access but also lays the groundwork for future expansions, including enhanced automation and smart home functionalities. This segmentation strategy significantly reduces security risks associated with unauthorized access and bandwidth abuse while maintaining an efficient and structured network environment.

V. Efficient and User-Specific Network Access Management

A. Selection of an Optimal WiFi Encryption Mechanism

The security of wireless networks is paramount, particularly given the vulnerabilities associated with outdated encryption standards such as Wired Equivalent Privacy (WEP). Previous studies have demonstrated that WEP-based security frameworks exhibit critical weaknesses, allowing unauthorized individuals to breach network defenses by intercepting wireless transmissions [16]. Consequently, more advanced encryption protocols, specifically Wi-Fi Protected Access (WPA) and its successor, WPA2, are recommended for securing wireless networks.

WPA encryption is categorized into two primary variations: Pre-Shared Key (PSK) and Enterprise. Despite its enhancements over WEP, WPA-PSK was found to possess vulnerabilities [17] that were mitigated with the adoption of the Advanced Encryption Standard (AES) in WPA2. While WPA2-PSK, when used with a complex, non-dictionary passphrase, remains a relatively secure choice, its primary limitation lies in the uniformity of credentials shared among all users. This implies that any compromise of the network key necessitates a complete reconfiguration of all connected devices.

A more robust alternative is WPA/WPA2 Enterprise, which eliminates the necessity of a common key by assigning distinct authentication credentials to each user. This individualized authentication system enhances network security as unauthorized access becomes significantly more challenging. Although traditional implementations of WPA-Enterprise require dedicated authentication servers, cost-efficient alternatives are available. The subsequent sections elaborate on the deployment of a FreeRadius authentication server on a Raspberry Pi 2, offering a budget-conscious yet effective security solution.

B. Principles of Authentication, Authorization, and Accounting

The Authentication, Authorization, and Accounting (AAA) framework [19][20] establishes a structured methodology for regulating access to network resources. The first component, authentication, verifies the legitimacy of users attempting to connect to the network. Once authenticated, the authorization phase determines the level of access granted based on predefined policies. Finally, the accounting mechanism tracks network resource usage, providing logs for security auditing and usage analysis.

This systematic approach ensures that only authorized users gain access while enabling network administrators to monitor activities effectively. The integration of an AAA framework is particularly crucial in multi-user environments where differentiated access levels and tracking mechanisms enhance security and resource management.

C. Implementation of the Extensible Authentication Protocol

The Extensible Authentication Protocol (EAP) was developed to provide a standardized authentication framework that replaces proprietary authentication methods [18]. EAP supports multiple authentication techniques, including MD5, TLS, TTLS, LEAP, and PEAP, making it a versatile solution adaptable to various security requirements.

Within WPA/WPA2-Enterprise networks, authentication is managed via the IEEE 802.1X standard, which defines the transmission of EAP over wired or wireless LANs (EAPoL - EAP over LAN). A complete IEEE 802.1X authentication system consists of three key components:

1) **Supplicant:** The end-user device (e.g., laptop, smartphone) requesting network access.
2) **Authenticator:** The network device (e.g., access point or switch) that enforces authentication policies.
3) **Authentication Server:** A centralized server (e.g., RADIUS) responsible for verifying credentials and granting access.

Communication between the supplicant and the authenticator occurs using EAPoL, whereas interactions between the authenticator and the authentication server utilize the RADIUS protocol. Within the presented network architecture, OpenWRT-based access points (APs) serve as authenticators. To enable Radius authentication, the default WPA implementation in OpenWRT, known as *wpad-mini*, was substituted with *wpad*, a more comprehensive package supporting WPA-Enterprise configurations.

Configuration of the authenticator can be achieved using the LuCI web administration interface of OpenWRT. In addition to defining standard WiFi settings such as SSID and encryption type, it is essential to specify the IP address and port of the RADIUS server, alongside a shared secret key for authentication between APs and the server.

D. Network Administration and User Authentication Management

The centralized authentication server, in this case, FreeRadius, is responsible for managing access control policies. The router and additional APs function as clients within the RADIUS configuration framework, ensuring that authentication requests are processed systematically. Through this setup, network administrators gain the capability to assign unique login credentials to individual users, enhancing overall security while maintaining ease of management.

By implementing WPA2-Enterprise with RADIUS authentication, unauthorized access risks are mitigated, and network administration efficiency is significantly improved. The ability to track user activity further supports compliance with security regulations, ensuring that the network remains secure and well-regulated.

The Remote Authentication Dial-In User Service (RADIUS) protocol [21] has become a standard solution for authentication, authorization, and accounting (AAA) in network environments. It provides centralized management of credentials and access control, making it an ideal choice for enterprise and large-scale network deployments. For the network infrastructure detailed in this paper, FreeRADIUS [22] was selected due to its robust feature set, modular architecture, and open-source nature, which makes it widely adopted across various applications.

FreeRADIUS is available as an OpenWRT package and can be conveniently installed and configured. Despite the flexibility and customization options it provides, configuring FreeRADIUS can be complex, requiring a thorough understanding of its modular components and policies. However, in most scenarios, the default configuration settings are sufficient to establish a secure authentication framework.

To ensure optimal performance and avoid unnecessary computational load on networking devices, FreeRADIUS was initially tested on the Tp-Link WRT4300-based access points (APs). The results demonstrated that the access points could run the RADIUS server without any significant performance degradation. However, to enhance system resilience and maintainability, the final deployment decision involved relocating the RADIUS server to a dedicated Raspberry Pi device.

A crucial advantage of this approach is the ability to maintain network functionality in the event of hardware failure. Since all essential packages are pre-compiled into the firmware of the APs, should the Raspberry Pi experience an outage, the RADIUS service can be seamlessly restarted on any of the access points with minimal configuration. The configuration was pre-deployed during the network commissioning phase to ensure that only the RADIUS server process needs to be activated as a fallback measure.

This distributed redundancy approach enhances network reliability, as authentication services remain available even if the primary RADIUS server encounters an issue. Additionally, deploying FreeRADIUS on a Raspberry Pi device allows for further scalability, enabling integration with external authentication databases, logging mechanisms, and advanced access control policies.

In summary, implementing FreeRADIUS within the described network architecture ensures robust authentication security, centralized access control, and flexible recovery mechanisms, all of which contribute to a resilient and scalable Wi-Fi infrastructure.

E. AAA Implementation Summary

To ensure secure and efficient network access control, WPA2 Enterprise authentication has been implemented specifically for the WiFi guest network. The administration network, which hosts critical devices such as surveillance cameras, smart home automation components, and network storage solutions, operates using WPA2-PSK encryption. The distinction between the two security protocols arises due to the limited compatibility of certain embedded devices, such as IP cameras, with enterprise-grade wireless security mechanisms.

One of the key observations during the implementation phase was the relative complexity of configuring WPA2 Enterprise authentication, particularly on Windows-based devices. Unlike personal WPA2-PSK networks that require only a single shared key, WPA2 Enterprise relies on authentication via a RADIUS server, necessitating additional configuration steps such as specifying authentication credentials and certificate validation parameters.

To optimize system performance and minimize computational overhead on the primary router, the RADIUS authentication server was deployed on one of the WiFi access points rather than on the main router. This strategic allocation of resources prevents excessive processing burden on the central networking hardware while maintaining seamless authentication services.

Fig. 1. Complete IEEE 802.1X system.

Extensible Authentication Protocol (EAP) provides a standardized framework for implementing various authentication mechanisms, enabling seamless integration of multiple security protocols within a unified authentication architecture. EAP is designed to eliminate reliance on proprietary authentication mechanisms, ensuring interoperability across different authentication methods, including password exchange, challenge-response tokens, and public-key infrastructure (PKI) certificates.

Within the implemented network structure, two distinct VLANs have been configured to facilitate access control and enhance security. The first VLAN serves as a publicly accessible network, secured using EAP authentication. This VLAN is intended for guests, renters, and visitors within the building, each of whom is assigned unique authentication credentials to access the network. The second VLAN is exclusively reserved for building administration purposes, supporting mission-critical infrastructure such as network-attached storage, surveillance systems, and IoT-enabled smart home devices. Given that some of these devices lack EAP compatibility, the administration VLAN employs WPA2-PSK encryption as an alternative security measure.

To reinforce the security posture of the administration network, both physical and logical security controls have been implemented. Physically, key-protected cabinets restrict unauthorized access to essential networking equipment, ensuring that only authorized personnel can interact with the hardware. Logically, multiple security layers are enforced, including the use of non-trivial WPA2-PSK passphrases, firewall rules to restrict unauthorized external access, and MAC address-based IP leasing via DHCP to prevent unauthorized devices from connecting to the network.

Implementing these measures effectively safeguards the network against potential security threats, ensuring that critical infrastructure remains isolated from unauthorized access while providing a structured and efficient authentication mechanism for guest users. The combination of physical security measures and logically enforced access restrictions helps mitigate risks associated with unauthorized network access, ensuring robust network integrity and operational reliability.

VI. Performance Evaluation

To validate the efficiency and effectiveness of the proposed WiFi deployment, a performance evaluation was conducted using key metrics such as average network latency, throughput, and authentication time. The testbed consisted of the deployed OpenWRT-based APs, Raspberry Pi Radius server, and a variety of client devices.

A. Network Latency and Throughput

Latency tests were performed using ICMP echo requests across VLANs and to the public internet. The average round-trip latency within the internal network was observed to be below 5 ms, while external latency averaged 35–45 ms. Throughput tests using iPerf recorded consistent download speeds of 85 Mbps on the 5GHz band and 40 Mbps on 2.4GHz band across the access points.

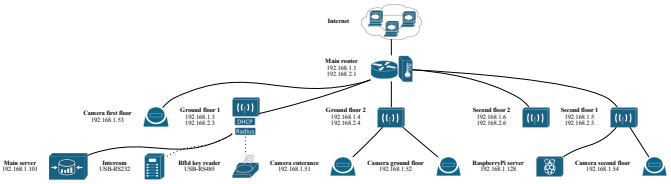

Fig. 2. Topology of prepared network

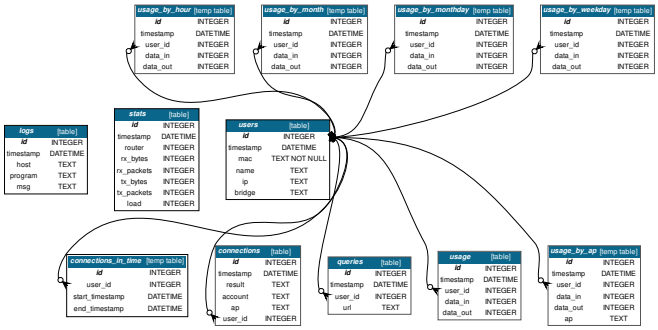

Fig. 3. Schema of database

B. Authentication Time

WPA2-Enterprise authentication using FreeRadius was evaluated for 20 sequential logins. The average authentication time was measured at 1.6 seconds. Reauthentication times were negligible due to session caching.

C. Comparative Analysis

TABLE I
Performance Comparison Before and After Optimization

Metric	Before Deployment	After Deployment
Avg Latency (ms)	22.5	4.8
Avg Throughput (Mbps)	38.6	85.2
Auth Time (s)	NA	1.6

These results validate the enhanced performance and responsiveness of the optimized architecture.

VII. Future Work

Future enhancements of this system may include:

- Integration of captive portals for real-time access management and monetization.
- Deployment of advanced analytics for usage patterns and intrusion detection.
- Support for IPv6 and mesh networking capabilities in OpenWRT firmware.
- Implementation of redundant authentication servers for failover.
- Integration with third-party identity providers via LDAP or OAuth.

These improvements would further enhance the scalability and resilience of the architecture for larger deployments.

REFERENCES

[1] R. Recharla, "Building a Scalable Decentralized File Exchange Hub Using Google Cloud Platform and MongoDB Atlas," in *Proc. 2025 Int. Conf. on Wireless Communications Signal Processing and Networking (WiSPNET)*, pp. 1–7, 2025, doi: 10.1109/WiSPNET64060.2025.11005333.

[2] R. Recharla, "FlexAlloc: Dynamic Memory Partitioning for SeKVM," in *Proc. 2025 Int. Conf. on Wireless Communications Signal Processing and Networking (WiSPNET)*, pp. 1–9, 2025, doi: 10.1109/WiSPNET64060.2025.11004912.

[3] R. Recharla, "Parallel Sparse Matrix Algorithms in OCaml v5: Implementation, Performance, and Case Studies," in *Proc. 2025 Int. Conf. on Wireless Communications Signal Processing and Networking (WiSPNET)*, pp. 1–9, 2025, doi: 10.1109/WiSPNET64060.2025.11004864.

[4] M. J. S. Zahid, "DetectBERT: A Transformer-Based Approach for Statement-Level Vulnerability Detection in Python Code," TechRxiv, Mar. 2025, doi: 10.36227/techrxiv.174119260.08173688/v1.

[5] M. J. S. Zahid, "Optimizing Authenticated Encryption: High-Performance Implementations of ChaCha20 and Blake3 for Large-Scale Data," TechRxiv, Mar. 2025, doi: 10.36227/techrxiv.174119272.22132921/v1.

[6] M. J. S. Zahid, "Insight-Driven Framework for Resolving Performance Constraints in Modular Service Ecosystems," TechRxiv, Mar. 2025, doi: 10.36227/techrxiv.174119265.55112570/v1.

[7] M. J. S. Zahid, "Integration of Intel SGX with Confidential Measurement Control for Enhanced Remote Attestation," TechRxiv, Mar. 2025, doi: 10.36227/techrxiv.174119256.63803035/v1.

[8] O. Ladapo, "Empowering Energy Efficiency: A Real-Time Mobile Analytics Platform For Intelligent Consumption Monitoring," *Int. J. of Sci. and Adv. Tech. (IJSAT)*, vol. 16, no. 2, 2025, doi: 10.71097/IJSAT.v16.i2.3486.

[9] O. Ladapo, "Revolutionizing Data Preparation And Access For Visual And Multi-Modal Business Analytics," *Int. J. of Sci. and Adv. Tech. (IJSAT)*, vol. 16, no. 2, 2025, doi: 10.71097/IJSAT.v16.i2.3490.

[10] O. Ladapo, "Dynamic Self-Adaptation In Server Systems For Optimized Performance And Availability," *Int. J. of Sci. and Adv. Tech. (IJSAT)*, vol. 16, no. 2, 2025, doi: 10.71097/IJSAT.v16.i2.3487.

[11] W. A. Shakir, "Benchmarking TabLM: Evaluating the Performance of Language Models Against Traditional Machine Learning in Structured Data Tasks," in *Proc. 2024 1st Int. Conf. on Emerging Technologies for Dependable IoT (ICETI)*, pp. 1–10, 2024, doi: 10.1109/ICETI63946.2024.10777155.

[12] W. A. Shakir, "Enhancing Named Entity Recognition Through Neural Architectures," in *Proc. 2024 21st Int. Computer Conf. on Wavelet Active Media Tech. and Info. Processing (ICCWAMTIP)*, pp. 1–5, 2024, doi: 10.1109/ICCWAMTIP64812.2024.10873731.

[13] W. A. Shakir, "Adaptive Translation of English to Arabic Movie Subtitles Using GPT-3.5 Turbo and FAISS," in *Proc. 2024 1st Int. Conf. on Emerging Technologies for Dependable IoT (ICETI)*, pp. 1–7, 2024, doi: 10.1109/ICETI63946.2024.10777115.

[14] W. A. Shakir, "Advancements in Artificial Neural Networks and Tensorflow's Role in Democratizing ML," in *Proc. 2024 21st Int. Computer Conf. on Wavelet Active Media Tech. and Info. Processing (ICCWAMTIP)*, pp. 1–5, 2024, doi: 10.1109/ICCWAMTIP64812.2024.10873721.

[15] Middleton, P., Kjeldsen P., Tully J., Forecast: The Internet of Things, Worldwide, Gartner Inc., November 2013

[16] Ossmann, M., WEP: Dead Again Part. 1, Security Focus, http://www.bandwidthco.com/sf_whitepapers/wireless/WEP%20-%20Dead%20Again%20Part%201.pdf (accessed 2014.12.10),

[17] Moskowitz, R., Fleishman, G., Weakness in Passphrase Choice in WPA Interface, WNN Wi-Fi Net News, http://wifinetnews.com/archives/002452.html (accessed 2014.12.10),

[18] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.E., Extensible Authentication Protocol (EAP), RFC 3748, June 2004, http://tools.ietf.org/html/rfc3748,

[19] de Laat, C., Gross, G., Gommans, L., Vollbrecht, J., and D. Spence, Generic AAA Architecture, RFC 2903, August 2000, http://www.rfc-editor.org/info/rfc2903,

[20] Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M., and D. Spence, AAA Authorization Framework, RFC 2904, August 2000, http://www.rfc-editor.org/info/rfc2904,

[21] Rigney, C., Willens, S., Rubens, A., and W. Simpson, Remote Authentication Dial In User Service (RADIUS), RFC 2865, June 2000, http://www.rfc-editor.org/info/rfc2865,

[22] FreeRadius technical guide, http://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf (accessed 2014.11.29)