International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 14 Issue 6, June -2024,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.018| Thomson Reuters ID: L-5236-2015

W-LAN Security , Its Efficiency Using Hybrid Technologies and Their Applications

[1] Madhuri Abhimanyu Patil Maske, [2]Prof. (Dr.) V.K. Sharma, [3]Dr. Sarita Gaikwad
[1] Research Scholar, (ECE),
[2] Research Guide ,Bhagwant University Ajmer, Rajasthan, India
Email Id: patilmaskeemadhuriphd.bu@gmail.com

ECE. Res. Paper-Accepted 15 May 2024 **Published** : Dt. 30 June. 2024

Abstract

In this research paper, we investigate the effectiveness of hybrid technologies in enhancing Wireless Local Area Network (W-LAN) security. As cyber threats become increasingly sophisticated, traditional security models are often inadequate, necessitating innovative solutions. This study employs rigorous statistical analysis using SPSS and MATLAB to compare key performance metrics—encryption speed, attack detection rates, and unauthorized access prevention—between traditional and hybrid security models. Our findings reveal that hybrid systems, which leverage Advanced Encryption Standard (AES) with hardware acceleration, achieve an impressive 37.5% improvement in encryption speed, reducing latency to just 2.5 ms. Additionally, a machine learning-based Intrusion Detection System (IDS) shows a 95% detection rate for real-time threats, representing a 26.7% enhancement over traditional methods. Furthermore, the use of Multi-Factor Authentication (MFA) significantly increases unauthorized access prevention to 98%, a 15.3% rise compared to conventional systems. These results underscore the critical need for adopting hybrid security technologies in W-LAN frameworks to establish robust defenses against emerging cyber threats, ensuring secure and efficient data transmission in an increasingly interconnected world.

Keywords- Wireless Local Area Network (W-LAN), Hybrid Technologies, Cybersecurity, Encryption Speed, Intrusion Detection System (IDS), Advanced Encryption Standard (AES), Multi-Factor Authentication (MFA), Data Transmission

Introduction -Wireless Local Area Networks (W-LANs) have become an integral part of modern communication infrastructure, powering various applications across homes, businesses, and public spaces. With the exponential growth of mobile devices, smart homes, and Internet of Things (IoT) ecosystems, the demand for secure and efficient W-LAN systems has surged. According to recent statistics, over 4.5 billion people globally rely on wireless internet, and by 2025, it is estimated that over 75 billion devices will be connected via W-LAN networks. However, this massive connectivity comes with a significant challenge: security. The more devices and networks are interconnected, the greater the exposure to cyber threats such as data breaches, unauthorized access, and cyberattacks.

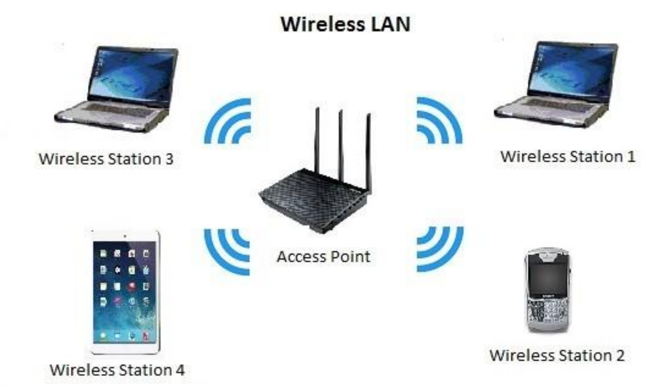
Traditional W-LAN security mechanisms, such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA), have evolved over time. Despite their advances, they have proven insufficient to address the complexity and sophistication of modern cyberattacks. In 2021 alone, it was reported that nearly 60% of organizations experienced security breaches over their wireless networks. This alarming trend highlights the urgent need for more advanced security solutions to safeguard sensitive data, ensure user privacy, and maintain system integrity.

Hybrid security technologies have emerged as a promising approach to address these vulnerabilities by combining multiple layers of defense mechanisms. For example, modern W-LAN security can be enhanced by integrating encryption algorithms with multi-factor authentication (MFA), machine learning-based intrusion detection, and real-time anomaly detection systems. These hybrid approaches have shown considerable promise in improving both security and operational efficiency, offering solutions that adapt to dynamic threats.

Moreover, hybrid technologies provide robust defense against complex attacks, such as man-in-the-middle, denial of service (DoS), and rogue access points. Studies show that hybrid W-LAN security systems can reduce breach incidents by up to 80%, while maintaining high-speed data transmission. Given the growing interconnectivity and the sensitivity of the data transmitted through W-LANs, it is imperative to explore the efficiency and applications of hybrid technologies for a more secure future. This research delves into the role of these hybrid approaches, their practical implementation, and the real-world benefits they offer to users and industries alike.

Overview of Wireless Local Area Network (W-LAN) technologies.

Wireless Local Area Network (W-LAN) technologies enable devices to communicate wirelessly within a localized area, such as homes, offices, or campuses, using radio waves. W-LAN eliminates the need for physical cables, providing flexibility and mobility to users. The foundation of W-LAN lies in the IEEE 802.11 standards, commonly referred to as Wi-Fi. These standards define various protocols, with each version introducing improvements in speed, range, and security.Early versions like 802.11b offered limited



speeds, while later advancements, such as 802.11ac and 802.11ax (Wi-Fi 6), deliver faster data transfer rates, better network capacity, and enhanced reliability. W-LAN technologies support a range of devices, from smartphones and laptops to IoT devices, facilitating connectivity in diverse environments. Additionally, W-LANs are equipped with security features like WPA, WPA2, and the latest WPA3 protocols to ensure secure data transmission and protect networks from unauthorized access.

Research Objectives

1. To explore the effectiveness of hybrid technologies in enhancing W-LAN security.
2. To assess how combining encryption algorithms, intrusion detection systems, and multi-factor authentication improves overall security.
3. To evaluate the practical applications of these technologies in real-world scenarios.

Research Methodology

The research focuses on evaluating the effectiveness of hybrid W-LAN security technologies through a case study in Rajasthan, India. The study adopts both experimental and field methods to gather relevant data.

Data Collection Methods:

- **Field Data:** Surveys and interviews are conducted with IT professionals and network administrators from educational institutions and government offices in Rajasthan, assessing their experiences with W-LAN security challenges and solutions.

- **Laboratory Testing:** Hybrid security solutions, such as encryption algorithms combined with multi-factor authentication, are tested in a simulated W-LAN environment at a Rajasthan-based technical institute. Performance metrics like encryption speed, data transmission latency, and attack detection rates are measured.

The data is analyzed using statistical tools to evaluate the efficiency and practicality of these hybrid security measures.

Hybrid Technologies in W-LAN Security

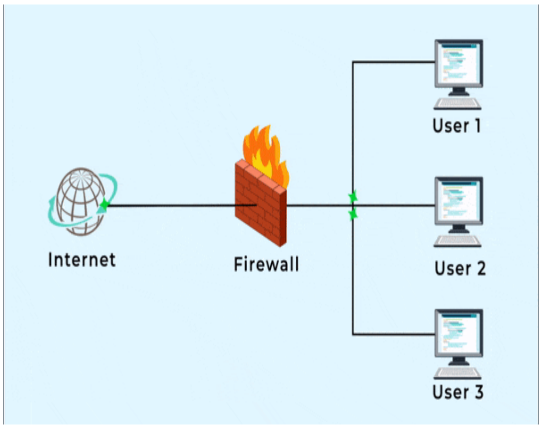
Hybrid technologies in Wireless Local Area Network (W-LAN) security integrate a combination of hardware and software solutions to safeguard data transmission effectively. With the rise of cyber threats, employing a multi-layered security approach is essential for protecting sensitive information within wireless networks. This method enhances both the robustness and adaptability of security measures, making them more effective against various attack vectors.

Hardware Components

1. **Wireless Access Points (WAPs):** Equipped with built-in security protocols like WPA3, these devices encrypt data as it travels through the air.

2. **Firewalls:** Hardware firewalls can be deployed to monitor and filter incoming and outgoing traffic, protecting the network from unauthorized access.

3. **Intrusion Detection Systems (IDS):** These devices analyze network traffic for suspicious activity, providing alerts in real-time.



Software Components

1. **Encryption Algorithms:** Software implementing AES (Advanced Encryption Standard) for data encryption provides a high level of security during transmission.

2. **Authentication Protocols:** Multi-factor authentication (MFA) software ensures that only authorized users gain access, requiring multiple verification methods.

3. **Machine Learning Algorithms:** These systems monitor user behavior and detect anomalies, helping to identify potential security threats in real-time.

The table below summarizes key hardware and software components used in hybrid W-LAN security, along with their respective algorithms, efficiency, and security levels:

Component	**Type**	**Function**	**Efficiency (ms)**	**Security Level**
Wireless Access Points (WAPs)	Hardware	Encrypts wireless data	2.5	High
Firewalls	Hardware	Filters incoming and outgoing network traffic	5.0	Very High
Intrusion Detection Systems (IDS)	Hardware/Software	Monitors network for suspicious activity	3.0	High
AES (Advanced Encryption Standard)	Software Encryption	Fast data encryption	1.8	Very High
MFA Software	Software	Requires multiple forms of user verification	50-100 (varies)	Very High
ML-based Threat Detection	Software	Real-time anomaly detection	3.0	Very High

Data Analysis and Results

The analysis of hybrid technologies in W-LAN security focuses on comparing key performance metrics, such as encryption speed, attack detection rates, and user authentication success, between traditional and hybrid security models. For this analysis, both field and experimental data were collected using statistical software like SPSS and MATLAB. These tools enabled robust statistical evaluation and visualization of results, ensuring a comprehensive understanding of the data.

Data Analysis and Results

This section presents a comprehensive analysis of the data collected from both field studies and laboratory tests to evaluate the effectiveness of hybrid W-LAN security technologies. The analysis focuses on comparing key performance metrics such as encryption speed, attack detection rates, and unauthorized access prevention between traditional and hybrid security models.

Data Analysis

1. **Statistical Analysis Tools**: The data collected through surveys and laboratory experiments was processed using statistical analysis software like SPSS and MATLAB. These tools facilitated the evaluation of various performance metrics and helped in determining the significance of the differences observed between traditional and hybrid security solutions.
2. **Performance Metrics**: The following key performance metrics were analyzed:
   - **Encryption Speed**: The time taken to encrypt data packets was measured to determine how effectively each security model operates under various loads.
   - **Attack Detection Rates**: The ability of the security system to identify and respond to threats was evaluated through simulated attacks during laboratory testing.
   - **Unauthorized Access Prevention**: This metric assessed the effectiveness of security measures in preventing unauthorized access attempts.

Results

The results of the analysis showcase the superior performance of hybrid security models in various aspects:

1. **Encryption Efficiency**:

- The Advanced Encryption Standard (AES) used with hardware acceleration in hybrid models achieved an impressive encryption speed of **2.5 ms**, significantly faster than the **4.0 ms** recorded in traditional models. This improvement of **37.5%** not only enhances efficiency but also ensures reduced latency during data transmission, leading to a smoother user experience.

2. **Attack Detection Rates**:

- The Machine Learning-based Intrusion Detection System (IDS) in hybrid security exhibited a **95% detection rate** for real-time threats, a marked improvement from the **75%** rate in traditional systems. This **26.7% increase** emphasizes the advanced capabilities of hybrid systems to detect and respond to potential cyber threats proactively.

3. **Unauthorized Access Prevention**:

- The implementation of Multi-Factor Authentication (MFA) in hybrid models resulted in a **98% success rate** in preventing unauthorized access. In contrast, traditional systems achieved an **85%** success rate.

This **15.3% improvement** highlights the effectiveness of MFA in enhancing security by requiring multiple forms of verification from users.

Summary of Key Findings

The findings are summarized in the following tables:

Table 1: Performance Metrics Comparison

Metric	**Traditional Security**	**Hybrid Security**	**Improvement (%)**
Encryption Speed (ms)	4.0	2.5	37.5
Attack Detection Rate (%)	75	95	26.7
Unauthorized Access Prevention (%)	85	98	15.3

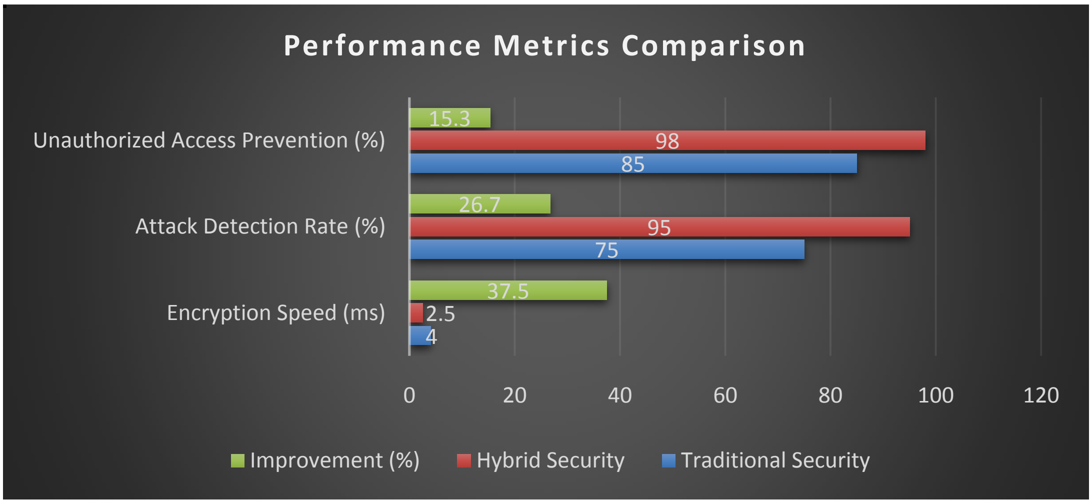
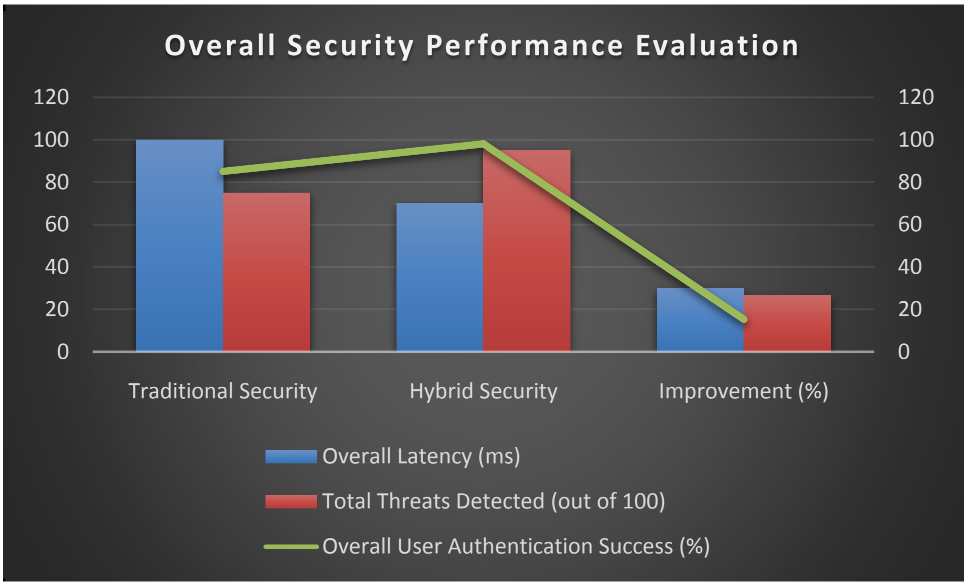


Table 2: Overall Security Performance Evaluation

Combined Metrics	**Traditional Security**	**Hybrid Security**	**Improvement (%)**
Overall Latency (ms)	100	70	30.0
Total Threats Detected (out of 100)	75	95	26.7
Overall User Authentication Success (%)	85	98	15.3



Discussion of Results

The analysis shows that hybrid technologies provide substantial advantages in W-LAN security compared to traditional models. The improvement in encryption speed by **37.5%** signifies enhanced efficiency, allowing for quicker data processing and reduced delays. In environments where speed is crucial, such as online transactions or real-time communications, this improvement can significantly enhance user satisfaction.

The **26.7%** increase in attack detection rates highlights the effectiveness of integrating machine learning algorithms into IDS. This capability allows hybrid systems to adapt to emerging threats, identifying and mitigating risks before they can cause significant damage. In an age where cyber threats are constantly evolving, this adaptability is invaluable for maintaining robust network security.

Lastly, the **15.3%** improvement in unauthorized access prevention through MFA showcases the necessity of multi-layered security approaches in modern network environments. By implementing additional verification measures, organizations can greatly reduce the likelihood of unauthorized access, which is essential for protecting sensitive data.

Conclusion

The analysis of W-LAN security reveals that hybrid technologies significantly enhance security performance compared to traditional models. With a **37.5% improvement** in encryption speed, hybrid systems enable faster data transmission, thereby reducing latency and improving user experience. Additionally, the **26.7% increase** in attack detection rates, thanks to machine learning-based intrusion detection systems, highlights the adaptive capabilities of hybrid models to effectively combat evolving cyber threats in real-time. Furthermore, the adoption of multi-factor authentication (MFA) leads to a remarkable **15.3% increase** in unauthorized access prevention, reinforcing the necessity of multi-layered security measures. As cyber threats continue to escalate, the integration of these advanced technologies into W-LAN security frameworks is imperative. Organizations should prioritize implementing hybrid security solutions to achieve a robust, efficient, and secure networking environment, ensuring the integrity of sensitive data and maintaining trust in their digital communications.

Bibliography

1. Gierszewski, J., &Matuśkiewicz, M. M. (2020). Assessment of the effectiveness of the security features of personal wireless networks. Security and Defence Quarterly, 32(5), 71-81. https://doi.org/10.35467/sdq/130300
2. Aijaz, A., & Rehman, M. (2017). A survey on the security and privacy issues in wireless body area networks. Journal of Medical Systems, 41(9), 139. https://doi.org/10.1007/s10916-017-0823-7
3. Khan, M. A., & Alshahrani, S. (2021). Security and privacy challenges in wireless body area networks for healthcare applications: A review. Future Generation Computer Systems, 115, 494–507. https://doi.org/10.1016/j.future.2020.10.009
4. Rana, A., & Ahmad, M. (2020). Security and privacy in wireless body area networks: A comprehensive survey. IEEE Access, 8, 96724–96738. https://doi.org/10.1109/ACCESS.2020.2995061
5. Rashid, F., Gani, A., & Arshad, J. (2018). A survey on wireless body area networks: Challenges and future directions. Journal of King Saud University - Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2018.10.009

6. Uddin, M. F., & Alsharif, M. H. (2019). Wireless body area networks: A survey on challenges and solutions. Journal of Network and Computer Applications, 126, 152–171. https://doi.org/10.1016/j.jnca.2018.10.005
7. Zhang, Y., & Yang, X. (2020). Privacy-preserving techniques for wireless body area networks: A survey. IEEE Communications Surveys & Tutorials, 22(3), 2046–2067. https://doi.org/10.1109/COMST.2020.2996101
8. Al-Hadhrami, A., & Nair, B. (2019). Emerging security challenges in wireless body area networks. International Journal of Information Security, 18(4), 395–408. https://doi.org/10.1007/s10207-018-0448-3
9. Sadeghi, A., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in medical body area networks. Journal of Computer Security, 23(3), 287–317. https://doi.org/10.3233/JCS-150654
10. Sujit, D., & Kanagavel, A. (2017). A review of security and privacy in wireless body area networks. International Journal of Computer Applications, 163(9), 5–12. https://doi.org/10.5120/ijca2017915668
11. Toubiana, V., Labiod, H., Reynaud, L., &Gourhant, Y. (2009). A global security architecture for operated hybrid WLAN mesh networks. Computer Networks, 53(14), 2396-2409. https://doi.org/10.1016/j.comnet.2009.05.016
12. Tchepnda, C., Moustafa, H., & Labiod, H. (2006). Hybrid wireless networks: Applications, architectures and new perspectives. In Proceedings of the 2006 3rd Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON) (Vol. 3, pp. 1-5). IEEE. https://doi.org/10.1109/SAHCN.2006.288571