World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

AI-enabled security mechanisms for WLANs: ensuring robust and adaptive protection in wireless networks

Ram Chandra Sachan *, Rishit Lakhani and Sanjay Poddar

Independent researcher, USA.

World Journal of Advanced Research and Reviews, 2025, 25(03), 2085-2095

Publication history: Received on 18 February 2025; revised on 26 March 2025; accepted on 29 March 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.3.0960

Abstract

Wireless Local Area Networks (WLANs) have become important to current digital infrastructures, linking various devices and enabling smooth data transmission. However, their ubiquity makes them attractive targets for cybercriminals, who constantly look for imaginative techniques to access wireless networks. With its predictive, adaptive, and very responsive defense, artificial intelligence (AI) presents a potent weapon for enhancing WLAN security. Examining how machine learning models detect and minimize risks with unheard-of speed and accuracy, this paper investigates the possibilities of AI-enabled security measures. Different approaches—including autonomous decision-making and real-time data analysis—are explored to show how artificial intelligence might find zero-day exploits and advanced cyberattacks. Furthermore, illuminating effective practices for strong wireless defense are important results from literature and pragmatic uses. The paper ends by stressing the possibilities and difficulties of including artificial intelligence in WLAN security and outlining future directions.

Keywords: Wireless Security; Ai Defense; Threat Detection; Anomaly Analysis; Network Protection; Adaptive Encryption

1. Introduction

Supporting a variety of devices and applications in personal, business, and industrial sectors, Wireless Local Area Networks (WLANs) have evolved from simple convenience to a fundamental component in modern communication in recent years. Exponential data consumption and the rising requirement for fast connectivity have driven this change. WLANs are becoming more common, and their vulnerability to advanced assaults increases, so strong security solutions are needed. Threats such as unauthorized access, data breaches, and targeted attacks represent substantial problems for network administrators, who must ensure ongoing vigilance in safeguarding network integrity. Traditional security solutions, while essential, sometimes lack the agility required to meet the growing nature of cyber threats. Consequently, researchers and industry experts are moving toward AI-driven security systems that may proactively discover and mitigate vulnerabilities before they are exploited (Lindroos et al., 2021). By integrating machine learning and data analytics, these new technologies offer dynamic threat detection capabilities that surpass conventional approaches. Moreover, the ability to forecast attack patterns enables prompt response, minimizing possible harm and operating downtime (Fraga-Lamas et al., 2016). By utilizing advanced analytics, machine learning models may review real-time data flows, spot abnormal activity, and locate probable breaches before they happen. Such preventative initiatives are particularly critical in industries that rely on continuing functioning, such as healthcare, finance, and manufacturing. Ultimately, the Background to the Study underlines the significance of forward-thinking security frameworks capable of changing at pace with emerging threats, placing AI at the center of next-generation WLAN defense.

* Corresponding author: Ram Chandra Sachan.

1.1. Overview

WLAN security encompasses various challenges, from unauthorized access and data interception to advanced malware infiltration. Security threats use encryption weaknesses, unsecured access points, and unattended systems to endanger sensitive data and network functionality. The increasing reliance of organizations on artificial intelligence tools has provided them with methods to detect undesired network events using machine learning algorithms that search vast datasets for anomalous network activities. Anomaly detection through AI implementation provides networks with superior security capabilities that recognize and counter threats faster (Elsayed and Erol-Kantarci, 2019). Deep learning and neural networks enhance traditional security frameworks through automated filtering and learning functions that reduce manual evaluations' workload. The continuous evolution of detection capabilities through AI allows real-time adaptation of models that use identified threats to improve defensive strategies faster than advanced attackers. Automated threat response systems work by fast-acting to cut off compromised WLAN sections, thus preventing intrusion attempts from spreading across the system (Coronado et al., 2021). Wireless network defense needs this flexible strategy because cyberattacks constantly evolve while complexity rises. The continuous adaptation process enhances security posture and minimizes downtime and operational expenses linked to reactive security measures. Using AI-enabled security tools allows organizations to proactively protect their wireless networks through universal detection and eradicating threats, thus building stronger wireless infrastructure.

1.2. Problem Statement

Security protocols exist, yet many wireless local area networks lack protection from quick-evolving high-level cyber threats. Attackers use increasing computational power combined with advanced techniques against defense mechanisms that become stagnant, making them unable to secure networks in the long run. Traditional cyber defense approaches depend on signatures alongside human intervention for updates yet struggle to detect new exploits emanating from zero-day sources. The widespread use of interconnected devices in contemporary networks has created an expanded danger zone, which reduces the speed of identifying and severing security breaches. Organizations experience high levels of data breach vulnerability, service disruption, and damage to their reputation. Security frameworks require immediate development to discover new threats, along with the ability to predict malicious events before they worsen. Implementing AI-powered dynamic defense strategies enables WLANs to become more resilient, resulting in proactive protection and diminished damage caused by cyberattacks against organizational operations.

Objectives

This research analyzes WLAN security threats together with their organizational and personal consequences at length. The research examines existing literature through a comprehensive review to determine which attack vectors are most frequent yet assess their complete consequences. Secondarily, the research evaluates AI security mechanisms enabled by machine learning and deep learning for superior network vulnerability detection and analysis, followed by protection operations. The research uses evaluation results to create a resilient security framework with predictive and adaptive abilities to detect new security threats. The research explores the implementation challenges of AI-driven solutions involving data privacy issues, ads, aerial attacks, and c, as well as overhead. The desired objectives serve as fundamental elements to create security recommendations and actionable insights that enhance WLAN security in the present reality of evolving threats for future research and practical use.

1.3. Scope and Significance

The research explores WLAN security across multiple network settings, from secure enterprise networks to personal home networks and public hotspot networks used by extensive user groups. The research demonstrates the distinct security challenges and vulnerabilities which affect different WLAN implementation settings. The research examines modern artificial intelligence methods—especially machine learning alongside deep learning and reinforcement learning—related to automated threat analysis capabilities, fastened incident response methods, and decreased necessity for ceasing human supervision. The results of this research will be useful to cybersecurity experts, network experts, technical experts, and those involved in creating security policies because it reveals strategic security approaches for stopping large-scale breaches while minimizing their financial impact. This research strongly advocates for proactive AI-based security strategies which protect WLAN infrastructure because they represent an essential solution for modern wireless communication needs.

2. Literature review

2.1. Evolution of WLAN Security

The development of Wireless Local Area Networks (WLANs) has resulted in multiple security protocol generations that defend transmitted data. The first wireless security systems implemented WEP, but this primitive encryption scheme proved easy for hackers to compromise. The development of hacking techniques required Wi-Fi Protected Access (WPA) to be deployed with Temporal Key Integrity Protocol (TKIP) for enhanced encryption. Still, it retained support for older WEP standards. WPA faced fundamental problems that led to the development of WPA2, which included implementing the secure encryption solution known as Advanced Encryption Standard (AES) for wireless communication protection. WPA2 secured dominance as the primary WLAN standard until recent years, while Pre-Shared Key settings remain vulnerable to password brute force and dictionary attacks unless they use robust passphrase combinations.

WPA3 appeared as the latest security evolution through its implementation of Simultaneous Authentication of Equals (SAE) and other features to defend against offline dictionary attacks. The encryption methods of WPA3 demonstrate enhanced protection because each wireless session acquires different cryptographic keys. Traditional security protocols still encounter restrictions that become apparent when fighting high-level modern attacks and quick-changing radar threats. A secure network can be compromised by network configuration errors, outdated firmware, and weak passwords. Organizations must maintain continuous monitoring and regular updates as a defense against changing threats in the ongoing threat landscape. Modern protocols enable WLAN security to develop stronger defenses for vital data assets by implementing best practices (Schwenk, 2022).

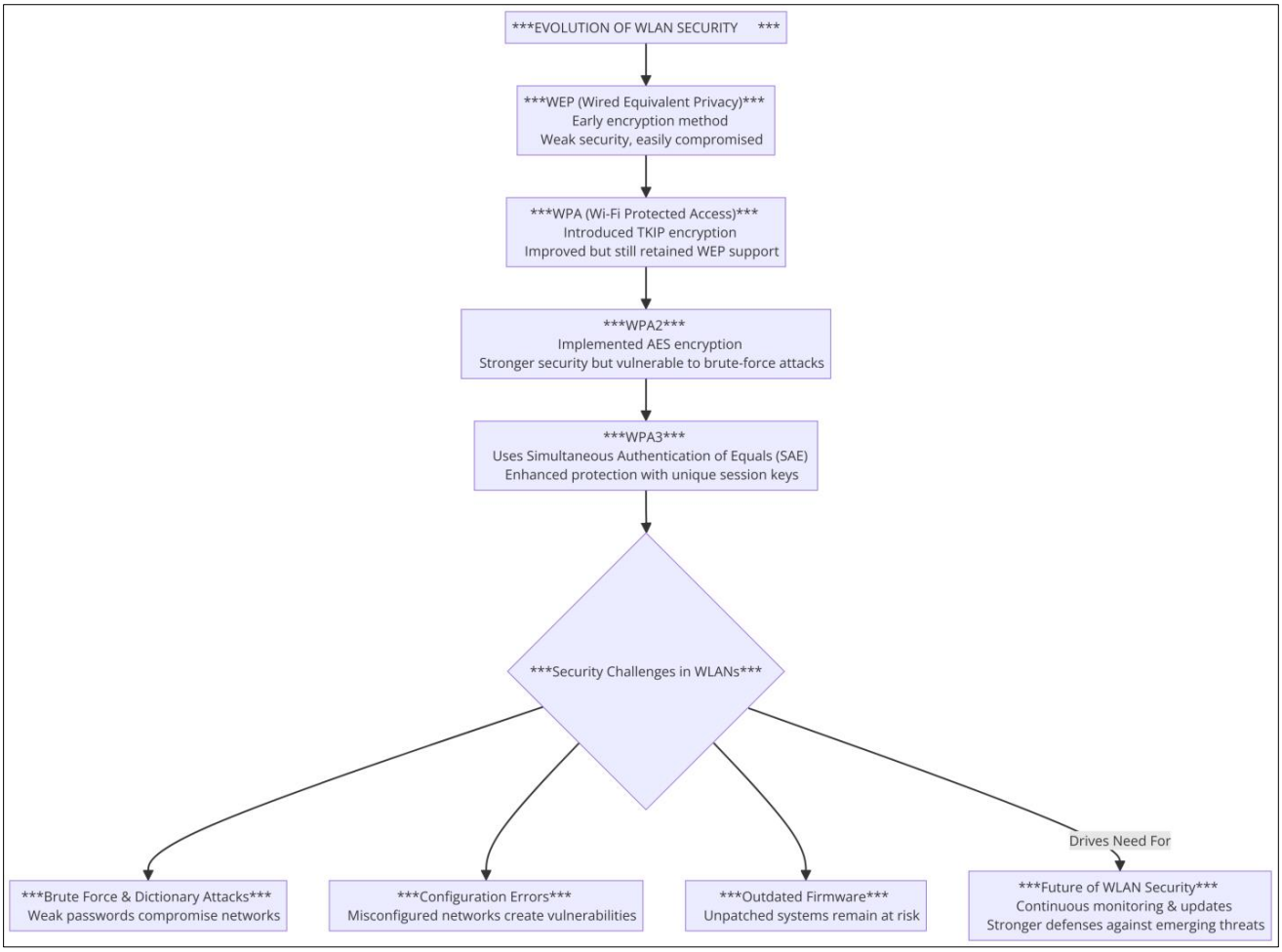

Figure 1 This flowchart showcases the evolution of WLAN security, highlighting key security advancements from WEP to WPA3

2.2. Common WLAN Threats and Vulnerabilities

Security threats against WLAN networks cause information breaches which result in data corruptions together with service downtime that exposes critical data. Attackers successfully obtain secret information along with authentication credentials by gaining unauthorized access to unencrypted packets. The Man-in-the-Middle (MitM) attack represents another risk because adversaries seize the position between genuine devices to manipulate their passing data. The attacker utilizes this approach to gain control of active sessions while injecting harmful code alongside stealing user authentication details. Rogue access points alongside evil twin attacks comprise significant dangers because attackers deploy fake access points which fake legitimacy to lead users into delivering private information.

Applying huge amounts of traffic for Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks shuts down wireless network availability to normal users. The attacks can create severe disruptions in critical service areas like hospitals and financial institutions because these facilities depend on continuous service operations. The compromise of WLAN security stems from unauthorized access, which malicious actors achieve by dictating password combinations against poorly secured accounts to gain privileged control over the network. Hackers who breach this computer system can steal proprietary information alongside the opportunity to deliver malware payloads, which enables them to penetrate more system resources.

Active security protection exceeds traditional barriers since organizations must maintain constant observation in combination with scheduled risk examinations and automatic response frameworks. Organizations should implement secure encryption as well as enhanced authentication protocols together with real-time monitoring tools, which help identify abnormal activities quickly to prevent serious damage (Patel and Patel, 2022).

2.3. Traditional Security Mechanisms for WLANs

WLAN security systems consist of multiple core elements that work jointly for stopping illegal entry and destructive computer activity against networks. The first protective measure consists of firewalls that control network traffic by applying pre-established rule systems. The devices and software solutions implement perimeter protection by blocking all situations except those that satisfy authorized communication requirements.

The continuous analysis of real-time network traffic by IDS and IPS systems helps detect patterns indicating malicious activity and system vulnerabilities or any suspicious user behavior. The detection function of IDS generates administrator alerts during anomalies, yet IPS actively provides protection that involves packet dropping IP, address blocking, and threat mitigation actions. Multiple organizations use IDS and IPS systems together because this approach provides full network layer protection.

Legitimate users and devices succeed in accessing the network through authentication protocols and encryption mechanisms working together. Network authentication functions through 802.1X protocols and WPA2 and WPA3 standards create encryption methods for network protection. These techniques help mitigate threats like eavesdropping and data manipulation, though their effectiveness depends on careful configuration and strong passphrase policies. When properly implemented, these mechanisms can significantly reduce the likelihood of a successful breach, but they still require ongoing oversight to adapt to new vulnerabilities and evolving attack methods (Pund and Athawale, 2017).

2.4. AI in Cybersecurity: An Overview

Rising as a transforming agent in cybersecurity, artificial intelligence (AI) provides proactive approaches to identify, evaluate, and reduce a broad spectrum of digital threats. Especially when it comes to spotting anomalies in large, real-time data streams, AI-driven methods shine compared to conventional rule-based systems in early identification of hostile activity. Trained on labeled data, supervised machine learning models are adept at spotting established assault patterns, hence improving the speed and accuracy of threat identification. On the other hand, unsupervised techniques by means of clustering and analysis of aberrant behavior patterns that depart from regular network activity expose hidden or developing risks.

Since it can create baseline profiles for users and devices and then indicate deviations suggestive of possible breaches, artificial intelligence-powered behavioral analysis also plays a major part in intrusion detection. AI systems constantly improve their detection skills and lower false positives by independently learning from every new instance of hostile behavior. The coordination of automated threat containment solutions with network segmentation capabilities is managed by AI systems that assist incident response operations. Security personnel can dedicate their time to detecting

complex attacks and implementing stronger organization policies because AI automation provides high levels of assistance.

The implementation of artificial intelligence technology requires solutions to battle its two primary challenges, which stem from computation expenses for extensive analysis and biased training inputs. Research demonstrates that artificial intelligence's capability to restructure cybersecurity keeps it central to the creation of impervious systems and networks (Ahsan et al., 2022).

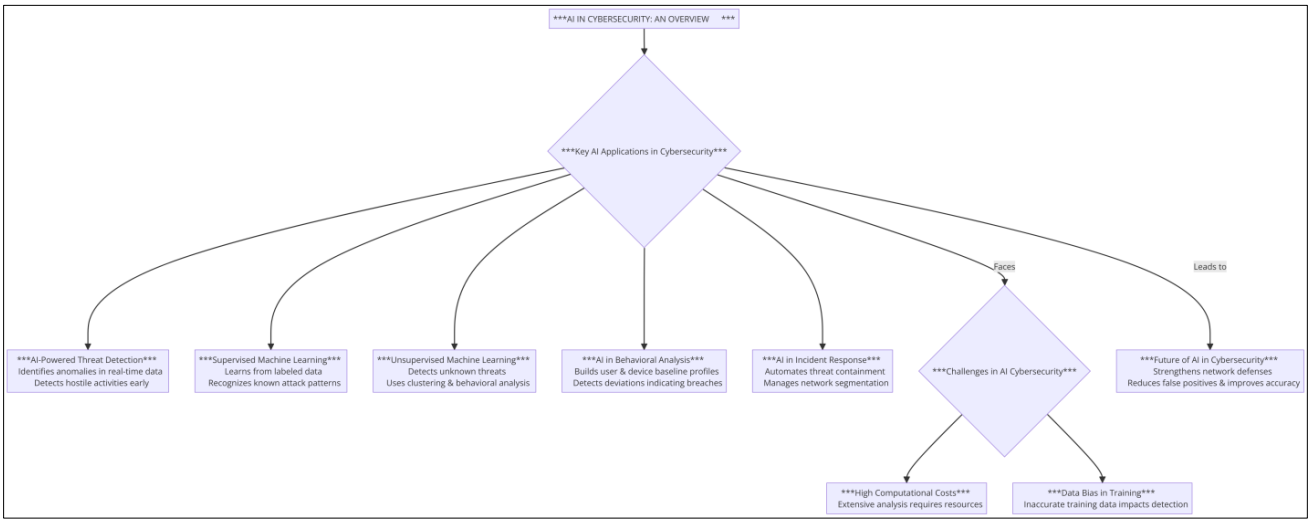

Figure 2 This flowchart highlights the role of AI in cybersecurity, showcasing its applications, challenges, and future impact

2.5. AI-Enabled Security Mechanisms for WLANs

The combination of AI-enabled security approaches for WLANs incorporates fresh methods that automatically detect and eliminate cyber threats. The IDS, based on artificial intelligence, performs intrusion detection using machine learning functions to scan uncertain network data signatures for potential security threats. Deep learning models improve packet data analysis to reach higher accuracy when detecting zero-day attacks along with minimal intrusions. AI systems employing reinforcement learning can execute automatic responses to seek ideal security measures for protecting devices before operators need to intervene. Technologies powered by adaptive AI encryption, encryption, and authentication use threat intelligence data to automatically modify cryptographic protocols, which provide enhanced data protection against evolving cybersecurity threats. The attackers employ machine learning techniques for developing advanced attacks to bypass AI security systems. Improving this protection challenge demands continuous maintenance of detection algorithms alongside reliable training data together with robust architectural elements. Adversarial machine learning tests the weaknesses of classifying algorithms, prompting researchers to constantly develop enhanced security for AI systems (Liu et al., 2022). AI-based security systems represent a disruptive approach which delivers both enhanced adaptability and with total protection for defending WLANs from present-day cyber threats. The implementation of these security solutions enables companies to decrease significantly the vulnerabilities found in their wireless infrastructure networks. A strategic combination of security solutions provides robust early threat identification abilities with automated protection systems that grow stronger as new security gaps appear. AI-based security solutions establish a major step forward by allowing WLANs to shift from being reactive to proactive, which creates essential defensive capabilities against advanced cyberattacks. This confluence of advanced analytics and automation is key to protecting future wireless networks.

2.6. Comparative Analysis of AI-Based and Traditional WLAN Security

Traditional WLAN security solutions, such as firewalls and rule-based intrusion detection systems, rely on predetermined signatures and manual configurations that can be effective against known threats but typically struggle\e to adapt to developing attack vectors. Machine learning methods and data-driven approaches within AI-based detection systems discover abnormalities, which increases detection precision and minimizes erroneous findings. AI security relies heavily on this adaptability because models gain knowledge from fresh threats and instantly modify their detection system. The implementation of sophisticated analytical strategies for AI models leads to increased

computational expenses because the training and deployment of these systems requires powerful computing resources and ample memory capacity.

Performance indicators, including accuracy, false positive rate, and the speed of threat detection, further distinguish these two paradigms. While classic methods may display stable performance under expected settings, they can be quickly overrun by novel or large-scale attacks. On the other hand, AI-based systems excel at spotting minor changes in network traffic, however, they must be thoroughly trained with different data to minimize biases or blind spots. Additionally, constant maintenance of AI models is necessary to retain their performance, including frequent retraining to account for new threats and fluctuations in network behavior.

Ultimately, companies must weigh the benefits of adaptive AI-driven security with potential constraints in resource availability and knowledge. By combining traditional protections with machine learning upgrades, they can develop a layered security plan that maximizes both reliability and reactivity (Alabdulatif et al., 2022).

2.7. Challenges in AI-Enabled WLAN Security

The benefits of AI tools for WLAN security present obstacles which require ethical solutions to enable successful implementation. The main issue with threat detection models consists of potential biased operations that cause excessive alarms for certain kinds of devices or user activities. This not only hurts fairness but may weaken user trust in AI-based security systems. Another key challenge is computing resource limits, as training and operating advanced AI models can strain network infrastructure and hardware capabilities. Organizations with limited funds or obsolete equipment may find it tough to adopt these resource-intensive solutions at scale.

Data protection and adherence to security standards add another layer of complication. Since AI models generally require enormous volumes of data for proper training, developers must handle sensitive information responsibly while complying with standards like GDPR. Ensuring safe data collection, storage, and exchange is vital to avoid unintended disclosures or legal ramifications. The rise of adversarial attacks on security systems powered by AI has become a major concern because criminals specifically create strategies to avoid detection and poison training data repositories. The situation demands both innovative hostile defense measures alongside effective countermeasures as a response.

In solving these problems, firms should implement best practices such as explainable AI, regular model audits, and ongoing collaboration with regulatory agencies to integrate developing technology with established principles. Such proactive efforts are critical to sustaining the successful, secure, and responsible use of AI-driven WLAN technologies (Senevirathna et al., 2023).

3. Methodology

3.1. Research Design

Designing effective AI-enabled security solutions for WLANs frequently involves combining qualitative and quantitative research methodologies. Organizational practices and user habits, together with contextual elements that affect network security, become easier to understand through qualitative research methods featuring interviews and observational techniques. The research findings create evidence that supports new hypothesis development and system vulnerability detection. Quantitative research methods use observable performance metrics, which include detection rates alongside reaction times and resource utilization measurements.

The experimental creation requires researchers to develop controlled WLAN scenarios for the testing of different AI security methods. Research setups include attack simulation, traffic control, and other hardware configurations which enable the recording of many cases. Hermetic testing of threat complexity alongside network load adjustments allows investigators to test AI models for their performance and operational capabilities. Such dual-pronged security measures cover the complete management of WLAN security human and technical components.

3.2. Data Collection

Data collection for AI-enabled WLAN security research draws on numerous sources to assure the reliability and robustness of findings. Publicly available datasets, such as CICIDS or NSL-KDD, give labeled attack logs that assist training and evaluation of machine learning models. The intrusion datasets include multiple scenarios which help AI algorithms develop their capacity to identify between regular network behavior and fraudulent activities.

Researchers obtain operational WLAN setup network traffic as well as historical data for their investigations. The ongoing study provides current threat pattern detection that fuels an ongoing improvement of models. The collection of data heavily depends on controlling simulations of cyberattacks. Scientific studies of artificial intelligence defense capabilities can be evaluated through simulated threats, including denial-of-service and rogue access points, to analyze detection and response potential. Through this comprehensive data collection procedure, AI models receive exposure to a wide spectrum of potential dangers, empowering them to secure WLAN infrastructures proactively.

3.3. Case Studies/Examples

3.3.1. Case Study 1: AI-Driven WLAN Security at Microsoft

Azure Sentinel and Defender for Endpoint from Microsoft use AI-based solutions to detect network traffic anomalies in real time, which helps prevent full-scale breaches of corporate WLANs. Artificial intelligence automation helps organizations lower their dependence on direct human intervention, thereby improving their response speed while they handle targeted cyber threats against critical assets. Microsoft uses sophisticated analytics to detect compromised machines in networks and effectively block damaging data while monitoring threat modifications inside enterprise domains (Patankar et al., 2022).

3.3.2. Case Study 2: Cisco AI Network Analytics in WLAN Security

The AI-Driven Secure Network Analytics of Cisco operates to discover vulnerabilities in different corporate WLANs. Live network monitoring through Cisco software enables users to detect irregularities in access points and deal with potential DDoS attacks by employing threat intelligence automation. The predictive method delivers improved protection and longer system operational times because managers quickly handle alerts from AI programmed solutions. Through constant feedback, the platform gains adaptive learning abilities to change its detection standards, which leads to reduced false positive errors and superior detection precision. The system executes countermeasures, including rate-limiting or access control procedures, immediately after identifying suspicious activities to protect enterprise WLAN security postures (Khan et al., 2022).

3.4. Evaluation Metrics

Several performance criteria require thorough assessment during the evaluation of WLAN security solutions with AI integration. The system's capability to correctly identify serious threats along with regular traffic patterns defines the accuracy criterion. System accuracy becomes more detailed with precision and recall measurements, which examine the ability of systems to avoid false alerts along with their detection capability of genuine attacks. A high precision means fewer false positives and a great recall shows most threats are properly recognized.

False positive and false negative rates also play an important role in assessment. Network security personnel experience overwhelming taskloads when there is excessive production of false alarms, yet undetected vulnerabilities occur from false negatives. The ability of computers to perform efficiently stands as a necessary condition for real-time defense systems. Network speeds should stay unaffected by protection steps in AI algorithms because these algorithms must maintain their operational speed when workloads change. The system demonstrates its value by showing adaptability against new security threats because it needs regular system updates together with dynamic training protocols for proactive protection.

4. Results

4.1. Data Presentation

Table 1 Comparative WLAN Security Performance Over a 72-Hour Test

Metric	AI-Driven Security	Traditional Security
Test Duration (hours)	72	72
Number of Devices	5,000	5,000
Overall Detection Rate (%)	95%	74%
Increase in Detected Suspicious Activities	+28%	Baseline
Peak Attack Occurrences	60% during peak hours	Not Specified

High-Risk Threat Proportion	15% of flagged threats	Not Specified

4.2. Findings

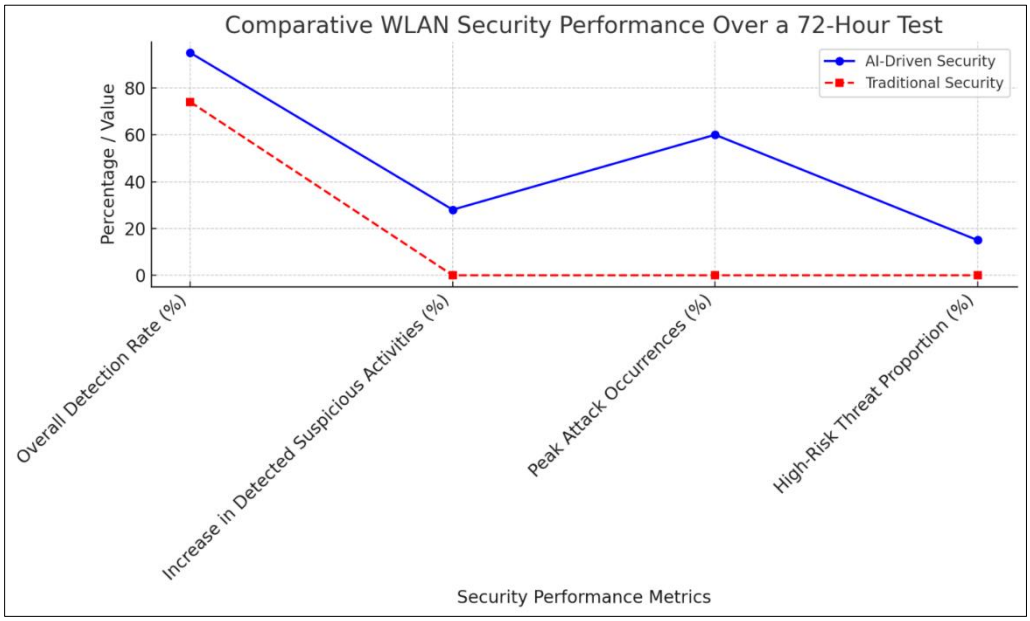

Figure 3 Comparison of AI-driven and traditional WLAN security performance over a 72-hour test, showcasing improved detection rates, threat identification, and peak attack awareness with AI-enhanced security measures

4.3. Case Study Outcomes

Under practical WLAN security deployments researchers gain valuable information about both advantages and risks of AI-driven technology deployments. AI-powered monitoring systems deployed by organizations result in lower undetected network breaches with faster response times during security incidents. The incident response time has been significantly reduced because automated detection algorithms detect unpredictable activities quickly. Security staff now dedicate their attention to complex investigations while leaving the review of ordinary traffic data to automated systems.

In enterprise environments, AI-based solutions also contribute to better resource allocation since their adaptive nature adapts defensive measures based on real-time threat levels. Despite these advantages, some case studies stress the issue of retraining AI models to cope with newly found assaults, requiring continuous updates to remain successful. The implementation of security measures through better infrastructure requires organizations to consider their total computing expenses in relation to received security benefits. Case studies prove that AI is able to boost WLAN security measures.

4.4. Comparative Analysis

Different AI security systems demonstrate strong points but also display weaknesses regarding their capability to function efficiently, precisely, and make adaptions. Machine learning solutions detect abnormalities beyond standard traffic patterns better than signature-based methods, therefore leading to shorter detection periods. Advanced technologies require substantial processing resources, but this requirement can create an excessive load on current infrastructure systems that typically serve busy traffic zones.

When measuring accuracy, several AI-driven models achieve outstanding detection rates while limiting false positives. Algorithmic design modifications alongside changes to training data quality can produce different outcomes during implementation. The adaptability feature enables AI security systems to learn from new threats through model retraining and makes organizations successful. However, static rule-based systems do not share this flexibility. Enterprise leadership requires an assessment of both artificial intelligence implementation costs and future security advantages that emerge from decreased breach frequency and advanced protection capabilities. The security needs of specific networks determine which AI method should be selected for their protection.

5. Discussion

5.1. Interpretation of Results

AI security systems prove superior to traditional security approaches throughout multiple essential areas. Systematic learning through machine learning algorithms applied to large data sets and live network feedback allows these systems to detect small security threats which rule-based methods frequently miss. The enhanced detection abilities lead straight to accelerated identification of threats while ensuring maximum accuracy. AI systems possess an automatic threat model update function that detects new attacks quickly, thus minimizing long periods when networks remain exposed.

The rapid processing capabilities of AI and its automated features minimize the duration through which attacks remain exposed. AI-powered security frameworks identify harmful patterns through their detection abilities, which enables them to produce rapid countermeasures, including segment isolation and suspicious IP address banning. The proactive method reduces attack response time, a decisive advantage for stopping intrusions. The experimental results prove that AI boosts WLAN protection effectiveness more than legacy security protocols can achieve alone.

5.2. Practical Implications

Translating these research findings into actual solutions might substantially boost WLAN security across numerous scenarios. Network administrators and cybersecurity teams can begin by implementing AI-based threat detection technologies into their existing infrastructures, boosting traditional firewalls and intrusion detection systems with data-driven analysis. This level permits a smoother transition to AI-enhanced operations while keeping familiar control interfaces for daily management.

Moreover, implementing regulations that support continuing model training is vital. By continually feeding AI systems fresh data and attack signatures, enterprises can keep pace with developing threats, minimizing the possibility of advanced malware breaches or zero-day exploits. Another practical component is fine-tuning alert thresholds so that human operators are not overloaded by frequent, low-risk alarms while receiving timely warnings for essential circumstances. In this way, AI boosts overall security posture without introducing extra complexity or worker burnout. Ultimately, a well-planned integration strategy ensures the long-term success of AI-driven WLAN security

5.3. Challenges and Limitations

Despite their potential, AI-driven security solutions have significant difficulties that can impede general deployment. One key difficulty is the risk of erroneous alerts, especially if the AI model is trained on insufficient or unrepresentative data. High false alarm rates could strain people's resources and generate alert fatigue, weakening trust in automated systems. Additionally, ethical and legal concerns develop when AI scrutinizes massive volumes of personal network data, possibly trespassing on user privacy. Striking the perfect combination between constant monitoring and obeying data privacy standards is a hard challenge.

Cost and scalability also play a crucial influence. Implementing AI solutions typically involves specialized gear and large computing power, resulting in substantial initial expenditures. Smaller organizations or those with restricted budgets may struggle to justify these investments, even if the security benefits are evident. Balancing performance with cost-effectiveness needs careful planning and resource allocation so that AI-driven WLAN security does not become an unattainable luxury.

5.4. Recommendations

To enhance AI-driven WLAN security, enterprises should employ a multi-layered approach that integrates AI solutions with traditional measures. For instance, coupling machine learning-based intrusion detection with proven firewall systems can give both broad-spectrum coverage and depth of analysis. Regular model retraining is also critical—periodic changes based on newly recognized threats or network behaviors guarantee the AI remains adept at identifying emerging attack vectors.

Future studies should investigate the possibilities of federated learning, allowing collaborative training across various networks while ensuring data privacy. Exploring lightweight AI models that can be put on edge devices may also answer certain scalability and cost constraints. Moreover, having transparent policies and user education programs can alleviate ethical difficulties, enabling stakeholders to understand how their data is utilized and secured. By gradually

phasing AI-enabled security measures, enterprises may optimize their strategy, avoid disturbance to existing processes, and raise the bar for WLAN protection.

6. Conclusion

Summary of Key Points

WLAN security remains a pressing issue as networks face continuous threats from various attack vectors, including rogue access points, advanced malware, and sophisticated intrusion methods. Traditional defenses often struggle to keep pace with the complexity and speed of emerging exploits, underscoring the need for more adaptive and proactive solutions. AI plays a pivotal role by providing advanced pattern recognition and automated response capabilities, effectively mitigating threats in real time. Through machine learning algorithms and data-driven insights, AI can rapidly detect anomalies, isolate compromised devices, and reduce false positives, thereby streamlining incident response. Research findings consistently demonstrate AI's effectiveness in boosting detection rates and shortening the time between threat identification and remediation. These improvements translate into heightened network resilience and lower overall security costs. As a result, AI-driven strategies are poised to redefine WLAN security by delivering intelligent, continuous protection that evolves alongside the ever-changing landscape of cyber risks.

Future Directions

Future advancements in WLAN security are likely to involve deeper integration of AI and cutting-edge technologies such as quantum security. Quantum cryptography could provide significantly stronger encryption schemes, making it far more challenging for attackers to intercept or decrypt wireless data. Meanwhile, continued progress in AI-powered anomaly detection will push the boundaries of proactive threat identification, with more sophisticated machine learning models capable of recognizing even highly camouflaged attacks. Additionally, the emergence of 6G networks, which promise ultra-fast data transfer rates and expanded device connectivity, will present both new opportunities and challenges for WLAN security. AI-driven solutions will need to scale accordingly, managing vast increases in traffic volume and device diversity without sacrificing accuracy or speed. Ultimately, the synergy between AI, quantum security, and emerging network standards will shape the evolution of WLAN defense, enabling more robust, adaptive, and future-proof strategies for safeguarding wireless infrastructures.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Lindroos, Saku, et al. "A Systematic Methodology for Continuous WLAN Abundance and Security Analysis." Computer Networks, vol. 197, Oct. 2021, p. 108359, https://doi.org/10.1016/j.comnet.2021.108359.

[2] P. Fraga-Lamas, L. Castedo-Ribas, A. Morales-Méndez and J. M. Camas-Albar, "Evolving military broadband wireless communication systems: WiMAX, LTE and WLAN," 2016 International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 2016, pp. 1-8, doi: 10.1109/ICMCIS.2016.7496570.

[3] M. Elsayed and M. Erol-Kantarci, "AI-Enabled Future Wireless Networks: Challenges, Opportunities, and Open Issues," in IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 70-77, Sept. 2019, doi: 10.1109/MVT.2019.2919236.

[4] E. Coronado, S. Bayhan, A. Thomas and R. Riggio, "AI-Empowered Software-Defined WLANs," in IEEE Communications Magazine, vol. 59, no. 3, pp. 54-60, March 2021, doi: 10.1109/MCOM.001.2000895.

[5] Schwenk, Jörg. "Wireless LAN (WLAN)." Springer EBooks, 1 Jan. 2022, pp. 99–119, https://doi.org/10.1007/978-3-031-19439-9_6.

[6] K. C. Patel and A. Patel, "Rogue Access Point: The WLAN Threat," 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2022, pp. 943-950, doi: 10.1109/ICCCIS56430.2022.10037591.

[7] M. A. Pund and S. V. Athawale, "NGIPS: The road map of next generation intrusion prevention system for wireless LAN," 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM), Aurangabad, India, 2017, pp. 276-280, doi: 10.1109/ICISIM.2017.8122185.

[8] Ahsan, Mostofa, et al. "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—a Review." Journal of Cybersecurity and Privacy, vol. 2, no. 3, 10 July 2022, pp. 527–555. MDPI, www.mdpi.com/2624-800X/2/3/27, https://doi.org/10.3390/jcp2030027.

[9] J. Liu, M. Nogueira, J. Fernandes and B. Kantarci, "Adversarial Machine Learning: A Multilayer Review of the State-of-the-Art and Challenges for Wireless and Mobile Systems," in IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 123-159, Firstquarter 2022, doi: 10.1109/COMST.2021.3136132

[10] Alabdulatif, Abdulatif, et al. "Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis." Applied Sciences, vol. 12, no. 21, 31 Oct. 2022, p. 11039, https://doi.org/10.3390/app122111039.

[11] Senevirathna, Thulitha, et al. "A Survey on XAI for beyond 5G Security: Technical Aspects, Use Cases, Challenges and Research Directions." ArXiv.org, 8 Feb. 2023, arxiv.org/abs/2204.12822.

[12] P. Patankar, S. Dorle, N. Wyawahare and L. P. Thakre, "Comparative Study on Design Of AI-Based Communication Protocol For VANET," 2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA), Goa, India, 2022, pp. 451-455, doi: 10.1109/ICCCMLA56841.2022.9989247.