Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

AI-Driven Security Mechanisms for WLANs Networks: Streamlining, Performance and Reliability

Ayesha Rashid
Information Technology University of Gujrat, Pakistan
Email: ayesha.rashid.csit@gmail.com, 3932@uog.edu.pk

Amir Raza Khan
University of Gujrat, Pakistan
Email: mirzaaaamir@gmail.com

Junaid Ashraf
Directorate of IT Services, University of Gujrat, Pakistan
Email: junaidashraf@uog.edu.pk

Abstract
In this modern era of 21st century of global village where Wireless ecosystem has been developed everywhere, human survival depends on WIFI connections. Wireless Local Area (WLANs) are part and parcel to exchange of data and communication among various locally used devices. Where the spread of WLANs is widespread all around, its availability also has make it susceptible to exploitation by fraudulent and malicious agents. But, now the invention of AI has brought security system for WLANs and establish for it highly precise, scalable, adaptable and protective mechanism. This research focuses on this transformation from general to AI oriented WLANs. It examines the capabilities of machines, learning models and detect the possible threats due to its unprecedented accuracy and velocity. This research focuses and illuminate's effectiveness of AI's that how it sophisticatedly detects the levels of vulnerability by analyzing the different methods, real time data processing and self, autonomous data processing and decision making. The results and key findings highlights successful solutions for very effective and strong wireless defense system. As, IT anonymously detects, predict and analyze data, through its AI-power intrusion protocol system. This research concludes that integration of AI and WLANs security protocols, for example WEP and WAP3 provide full security fool proof framework. Finally, this research adds in the existing data by providing opportunities and challenging for integrating AI with WLANs networking streaming lining, reliability and performance. That is AI's function for WLANs 'threat in functioning. The research also suggests that companies and organizations using WLANs may secure their intranet connections, by providing security and protection themselves if they integrate AI with WLANs and may avoid cyber threats by applying AI-power solutions. Companies may improve their WLAN security posture and protect themselves from emerging cyber threats by implementing AI-powered solutions.

Key words: WLAN Security, Artificial Intelligence (AI), Machine Learning, Cyber Threats, Network Protection.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

Introduction

A Wireless Local Area Network (WLAN) is a network that uses radio waves to connect devices in a specific geographic area, such as a home or office, without the usage of physical cables. It's a type of local area network (LAN) in which devices communicate wirelessly, typically via Wi-Fi (AlShourbaji, 013). Wireless Local Area Networks (WLANs) have emerged as an essential component of modern communication, supporting a wide range of devices and applications in the personal, business, and industrial domains (Pahlavan & Krishnamurthy, 2009). This transition has been fuelled by the rapid growth of data consumption and the rising demand for fast connectivity. The growing use of WLANs has increased their vulnerability to complex threats, needing strong security measures (Yaseen, 2022). Network administrators must deal with serious threats such as targeted assaults, data breaches, and unauthorized access, all of which jeopardize network integrity and provide significant security difficulties (Aslan, Aktuğ, Ozkan-Okay, Yilmaz, & Akin, 2023).

Traditional security systems frequently fail to adapt to the ever-changing cyber threat scenario. As a result, academics and practitioners are increasingly turning to AI-powered security systems that can identify and mitigate vulnerabilities before they are exploited (Akhtar, Rawol, 2024). These new technologies use machine learning and data analytics to provide superior threat detection capabilities over older approaches. Predicting attack trends allows them to respond quickly, reducing potential harm and system downtime (Okoli, Obi, Adewusi & Abrahams, 2024). Machine learning models employ advanced analytics to assess real-time data flows, detect anomalies, and predict future breaches. This proactive approach enables organizations to respond promptly to emerging hazards, reducing downtime and safeguarding critical data (Sarker, 2023). In industries such as healthcare, finance, and manufacturing, where continuous operations are essential, predictive skills are critical for maintaining operational integrity, ensuring company continuity, and protecting against financial losses and reputational damage.

This study emphasizes the essential need to close the research gap for adaptive security frameworks capable of fast responding to emerging threats, establishing artificial intelligence (AI) as a cornerstone of next-generation Wireless Local Area Network (WLAN) defense. Organizations that integrate AI-driven solutions can leverage the power of predictive analytics and machine learning to identify and mitigate potential security vulnerabilities in real time (Aldawsari & Kouchay, 2023).

This forward-thinking strategy enables the development of buoyant and robust security systems capable of effectively combating sophisticated cyber-attacks while safeguarding the integrity and confidentiality of sensitive data. As the WLAN security landscape changes, strategic deployment of AI-powered security solutions will become more crucial in protecting against emerging risks and maintaining stakeholder trust (Sachan, Lakhani, & Poddar, 2025).

WLAN Security Landscape

WLAN security faces various challenges, including unauthorized access, data breaches, and sophisticated malware attacks. Threats use vulnerabilities including inadequate encryption, open access points, and unmonitored systems to compromise sensitive data and disrupt network operations (LUWONGO,

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

2023). Fortunately, in modern era, companies are increasingly using intelligent technology (AI) to strengthen their network safety, adopting predictive programs to detect undesired activities by analyzing vast datasets for unusual behavior. AI-powered anomaly detection allows networks to respond more quickly and efficiently to threats, providing increased security capabilities (Chander, Pal, De & Buyya, 2022). Deep learning and neural networks supplement traditional security frameworks by automating filtering and learning processes, which considerably reduces the workload associated with manual evaluations (Mawgoud, Taha, Abu-Talleb, & Kotb, 2022). The continuous advancement of AI-driven detection capabilities enables real-time model adaption, allowing defensive methods to stay ahead of sophisticated attackers by utilizing recognized risks (Muppalaneni, Inaganti, & Ravichandran, 2024). Furthermore, automated threat response systems isolate vulnerable WLAN segments quickly, effectively restricting intrusion attempts and preventing them from spreading throughout the network (Kumar, & Kumar, 2023). The constantly changing nature of cyber threats needs a dynamic and adaptable strategy to wireless network defense. As assaults get more sophisticated and complicated, a flexible security approach is critical for staying ahead of emerging threats (Mallick & Nath,2024). AI-powered security solutions enable organizations to proactively protect their wireless networks from a wide range of attacks, detecting and neutralizing threats before they do harm. This proactive strategy improves the overall security posture while reducing downtime and operating costs associated with reactive security measures (Manda, 2024). AI-powered security tools help organizations develop a strong and resilient wireless infrastructure that can survive the ever-changing threat landscape. Companies that use this proactive strategy can assure the confidentiality, integrity, and availability of their wireless networks, thereby safeguarding sensitive data and ensuring business continuity (Humayun, Tariq, Alfayad, Zakwan, Alwakid, & Assiri, 2024)

The Challenge of Wireless Network Security

Wireless networks face a rising threat scenario, with cyberattacks becoming increasingly advanced and complicated. As organizations increasingly rely on wireless communication, the requirement for strong security measures has never been more critical. However, conventional safety procedures frequently struggle to keep up with the evolving threat landscape, leaving networks exposed to attack. As organizations increasingly rely on wireless communication, the requirement for strong security measures has never been more critical. This raises an important question: how can organizations defend their wireless networks from increasingly sophisticated cyber threats?

Problem Statement

Many wireless local area networks are still vulnerable to quickly emerging and powerful cyber-attacks. Attackers use increased processing power and new strategies to outmaneuver static defense systems, rendering them worthless for long-term network security. Conventional cyber defense solutions rely on signature-based detection and manual upgrades, but they frequently fail to detect innovative threats that exploit zero-day vulnerabilities. The growing number of networked devices in modern networks has greatly increased the attack surface, resulting in slower detection and reaction to security breaches. Companies are at

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

severe risk of data breaches, service disruptions, and reputational loss. To tackle these risks, security frameworks must be developed swiftly in order to detect emerging threats and anticipate hostile behavior before it escalates. AI-powered energetic defense solutions can boost WLAN resilience by enabling proactive protection and mitigating the impact of cyberattacks on organizational activities.

Aims and Objectives

The current study investigates WLAN security vulnerabilities in depth, focusing on the organizational and personal ramifications. The study analyses and evaluates the most common attack vectors using a thorough assessment of the current literature, establishing their overall impact and consequences. The current study delves further into WLAN security challenges, including both organizational and personal implications. The study assesses typical attack routes and AI-powered security methods, emphasizing machine learning and deep learning for improved network vulnerability identification and mitigation. The research focusses on developing a strong security framework with predictive and adaptive capabilities, as well as solving implementation obstacles for AI-driven solutions such as data privacy and operational issues. The research intends to improve WLAN security, address emerging threats, and drive future research activities, with the ultimate goal of strengthening wireless network security posture.

Scope of the Research

The study thoroughly analyzed WLAN security in a variety of network scenarios, identifying security difficulties and vulnerabilities while also offering a full understanding of wireless network threats and dangers. The study investigated the application of advanced artificial intelligence techniques such as machine learning, deep learning, and reinforcement learning to increase automated threat assessments, speed up incident response, and reduce human supervision.

Significance of the Research

The research analyses current literature to identify and analyse the most common attack routes, assessing their impact and implications. The study also looks at AI-powered security mechanisms that leverage machine learning and deep learning to enhance network vulnerability detection, analysis, and protection operations. AI-powered security solutions effectively defend wireless networks, enabling businesses to stay ahead of emerging threats. The research provided strategic security measures to prevent large-scale breaches and minimize costs. This influenced the formulation of security policies and recommendations for WLAN adoption and administration. The research also improved cybersecurity procedures to help organizations defend wireless networks and maintain data confidentiality, integrity, and availability. The study makes an essential contribution to the field of cybersecurity by giving practical solutions and strategic insights into protecting wireless networks in the face of growing threats.

Literature Review

The expansion of WLANs has hastened the development of several security methods to secure data in transit. Early WLAN security was based on Wired

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

Equivalent Privacy (WEP), a rudimentary encryption method with inherent security flaws that hackers may exploit (Yaseen, 2022). The rapid advancement of hacking tools disclosed WEP flaws, leading the development of Wi-Fi Protected Access (WPA). WPA used the Temporal Key Integrity Protocol (TKIP), which dynamically altered encryption keys to improve security (Firdus, Aghababayev, Aliyev, Mustafayeva, Mayilov, Sardarova, & Bakhshaliyeva, 2024). To enable a smooth transition, WPA maintained support for older WEP devices, allowing for interoperability but inheriting certain of WEP's security flaws (Afzal, Uzair, Javed, & Naqvi 2024).

Schepers (2023) stated that WPA's fundamental security constraints prepared the way for the creation of WPA2, which used the Advanced Encryption Standard (AES) to provide strong encryption for wireless communications. WPA2's use of AES significantly improved WLAN security, and it quickly became the dominant standard for wireless networks due to its superior security features (Adbeib, 2023). However, WPA2's Pre-Shared Key (PSK) mode, which is frequently used in home and small office networks, remains vulnerable to password cracking techniques such as brute force and dictionary attacks (Alhamry & Alomary, 2022).

The security of WPA2 in PSK settings was highly reliant on the strength of the chosen passphrase, emphasizing the importance of users selecting complicated and strong passwords to avoid unauthorized network access (Alamleh, Estremera, Arnob, & AlQahtani, 2025). WPA3, the most recent improvement in WLAN security, enhances wireless network security by using Simultaneous Authentication of Equals (SAE), also known as Dragonfly (Btoush et al., 2024). SAE offers a robust defense against offline dictionary attacks because it requires active engagement from both the client and the access point during the authentication process. This method prevents attackers from secretly accessing and Analysing authentication data, making successful password cracking significantly more difficult (Halbouni, Ong, & Leow, 2023).

Furthermore, WPA3's encryption mechanisms safeguard each wireless session with unique cryptographic keys, adding an extra layer of protection (Thakur, Hayajneh, Thakur, Kamruzzaman, & Ali, 2023). This means that even if an attacker manages to compromise the encryption key for one session, it will not jeopardize the security of subsequent sessions, considerably improving the overall security of wireless communications. Traditional security protocols, although their relevance, have inherent weaknesses that become obvious when dealing with modern and dynamic threats (Zheng, Li, Xu, & Zhao, 2022). Modern assaults, which are frequently distinguished by their intelligence and rapid evolution, can exploit vulnerabilities that traditional security measures may be unable to address. Furthermore, even networks with strong security frameworks can be jeopardized by simple mistakes and oversights (Abd-el-Kader, Amissah, Kinga, Mugerwa, Emmanuel, Mansour, & Prokop, 2024). Configuration mistakes, such as misconfigured firewalls or access controls, can generate vulnerabilities for attackers to exploit (Srinivasa, Pedersen, & Vasilomanolakis, 2021). Similarly, failing to update firmware can expose devices to known issues, whilst weak passwords provide an easy entry point for malicious actors (Bielawski, Gaynier, Ma, Lauzon, & Weimerskirch, 2020). These human and technical flaws underline the significance of continuous monitoring, regular security updates, and best network management practices for guaranteeing

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

wireless network integrity and security.
In today's changing threat landscape, organizations must adopt a proactive and continuing security strategy that emphasizes persistent monitoring and regular updates (Dine, 2024). This lets them to keep up with evolving threats, detect potential vulnerabilities, and remedy them before they are exploited. Modern WLAN security protocols aim to help organizations establish robust defenses for their critical data assets by delivering better security features and capabilities (Aggarwal & Gupta,2024). Implementing best practices such as regular security audits, patch management, and people training strengthens security posture and protects data from sophisticated attackers (Mohammed, 2023).
Using the newest security procedures and adhering to security principles assures data confidentiality, integrity, and availability, especially in the face of emerging threats (Akinade, Adepoju, Ige, & Afolabi, 2025).

Table 1:
Security Challenges in WLANSs: Conversion from WEP to WPA3

WEP	**WPA3**
Wireless Network Security Development	Brute Force and Dictionary Attacks: Description: Attackers use automated tools to guess passwords through repeated attempts or dictionary-based guessing Impact: Weak passwords can be easily compromised, allowing unauthorized network access
Protocol: WEP (Wired Equivalent Privacy) Description: Initial wireless encryption standard Security: Vulnerable to exploitation, weak security	Configuration Errors: Impact: Misconfigured networks can create security vulnerabilities, exposing systems to potential threats. Misconfigured Networks: Risk: Configuration errors can lead to security gaps, making networks susceptible to attacks and breaches
Protocol: WPA (Wi-Fi Protected Access) Description: Enhanced security with TKIP encryption Security: Improved over WEP, but retained compatibility with WEP devices	Outdated Firmware: Risk: Unpatched systems remain vulnerable to security threats and exploits. Unpatched Systems: Vulnerability: Failing to update firmware leaves systems exposed to security risks and potential breaches.
Protocol: WPA2 Description: Adopted AES encryption for robust security Security: Stronger than predecessors, but susceptible to brute-force attacks with weak passwords	Drives Need for: Future of WLAN Security: Key to Success: Ongoing monitoring and regular updates will provide robust defense against evolving threats.
Protocol: WPA3 Description: Utilizes Simultaneous	Securing WLAN's Future: Proactive Approach: Regular updates

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

Authentication of Equals (SAE) for enhanced security Security: Provides strong protection with unique session keys, defending against password guessing attacks	and continuous monitoring will strengthen defenses, ensuring resilience against new and emerging threats.

Suroto (2018) stated that WLAN security concerns have far-reaching ramifications for both organizations and people. When these risks occur, they can lead to information breaches, data corruption, and service outages (Spanca & Salihu, 2024). This not only affects corporate operations but also exposes crucial data, putting sensitive information at danger (Herath, Herath, Madhusanka, and Guruge, 2024). This not only affects corporate operations but also exposes crucial data, putting sensitive information at danger (Herath, Herath, Madhusanka, and Guruge, 2024). This can result in identity theft, financial losses, and reputational harm, emphasizing the importance of strong security measures for WLAN networks (Nazir, Laghari, Kumar, David, & Ali, 2021).

Man-in-the-Middle (MitM) attacks are a significant concern to network security because they intercept communication between legitimate devices and modify the data going through them (Fereidouni, Fadeitcheva, & Zalai, 2025). By positioning themselves between real devices, attackers can hijack ongoing sessions, insert malicious code, and steal critical user authentication information. Furthermore, rogue access points and evil twin attacks compound the danger by deploying false access points that mirror real ones, deceiving users into disclosing confidential information (Huang, Chi, & Hung, 2023). This can lead to unauthorized access, data breaches, and compromised security, emphasizing the need for effective security measures to prevent such attacks. Implementing strong encryption, secure authentication techniques, and regular network monitoring can help mitigate these risks and protect against MitM and rogue access point attacks (Bhadouria, 2022).

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks endanger wireless networks by overwhelming them with traffic and rendering them inaccessible to legitimate users (Gupta & Dahiya, 2021). This can lead to major disruptions, financial losses, and reputational damage. To effectively combat these threats, organizations must employ a complex strategy that includes ongoing network monitoring, risk assessments, and automated incident response systems (Tahmasebi, 2024). It is also necessary to implement robust security measures such as improved encryption protocols, enhanced authentication methods, and real-time threat detection technologies (Rao & Deebak, 2023). Organizations that use these preventative measures can mitigate the impact of DoS and DDoS attacks, ensure network availability and security, and safeguard critical assets from potential cyber threats (Dine, 2024).

Conventional WLAN security measures in Traditional WLAN security procedures are critical in high-risk contexts like hospitals and financial institutions, where service continuity is critical (Lindroos, Hakkala, & Virtanen, 2021). However, unauthorized access frequently jeopardizes WLAN security, which bad actors do by accessing inadequately secured accounts via password cracking or guessing (Alamleh, Estremera, Arnob, & AlQahtani, 2025). When hackers infiltrate the network, they can steal valuable information and deliver malware payloads, allowing them to penetrate further into the system and acquire control over more

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

resources (Jimmy, F. N. U., 2024). This emphasizes the importance of strong security measures such as strong password restrictions, multi-factor authentication, and frequent security audits in protecting WLANs from potential attackers and ensuring the integrity of important systems (Nwoye, 2024).

Active security is a comprehensive protection strategy that incorporates numerous critical components to prevent unauthorized network access and malicious activity. Firewalls are in the forefront of this defense, regulating network traffic based on predefined rule sets (Zhao & Song, 2020). Firewalls use perimeter protection, which prevents all incoming and outgoing traffic except that which meets specific authorized communication requirements. This ensures that only valid data packets pass through while blocking suspicious or malicious traffic (Gudimetla & Kotha, 2017).

Active security incorporates additional measures such as intrusion detection and prevention systems, encryption, access controls, and regular security updates (Heidari & Jabraeil Jamali, 2023). These collective defenses work together to provide effective security against a variety of threats, insulating networks, data, and systems from cyber-attacks and guaranteeing the integrity of digital assets (Martin & Ibrahim, 2024). By integrating these qualities, active security creates a proactive and flexible defense mechanism capable of responding to new threats and weaknesses (Aminu et al., 2024). Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) operate together to ensure full network security.

IDS continuously monitors real-time network data for patterns that could indicate malicious activity, system vulnerabilities, or odd user behavior, and notifies administrators when anomalies are discovered. IPS secures the network by proactive approaches such as discarding malicious packets, blocking IP addresses, and minimizing threats. Combining IDS with IPS allows organizations to provide robust network layer protection that ensures both detection and prevention of potential threats (Singh, 2023). This integrated strategy allows for quick response to security problems and helps prevent assaults from jeopardizing network integrity (Chukwunweike, Adewale, & Osamuyi, 2024).

Legitimate users and devices connect to the network using a combination of authentication procedures and encryption technologies. The 802.1X protocols permit network authentication, while the WPA2 and WPA3 standards provide strong encryption mechanisms for network security. (Afzal, Uzair, Javed, and Naqvi, 2024). These security methods efficiently protect against dangers like eavesdropping and data manipulation. Singh, S. (2023). However, their performance is strongly dependent on exact configuration and strict passphrase policies. Proper implementation considerably minimizes the chance of a breach, but continuous monitoring is required to address emerging vulnerabilities and adapt to changing attack strategies (Farraj & Hammad, 2024).

The role of artificial intelligence in enhancing cybersecurity is Artificial intelligence (AI) is emerging as a transformative agent in cybersecurity, providing proactive techniques to identifying, evaluating, and mitigating a wide range of digital risks (Mahfuri, Ghwanmeh, Almajed, Alhasan, Salahat, Lee, and Ghazal, 2024). When it comes to detecting abnormalities in huge, real-time data streams, AI-driven solutions outperform conventional rule-based systems in early detection of hostile activity. AI-driven approaches outperform traditional rule-based systems in early detection of hostile activities, particularly when

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

detecting abnormalities in massive, real-time data streams (Patil 2024). Supervised machine learning algorithms, when trained on labelled data, are adept at detecting established assault patterns, increasing the speed and accuracy of threat detection (Paul, 2024). Unsupervised approaches, on the other hand, use grouping and analysis of aberrant behaviour patterns that differ from normal network activity to reveal hidden or developing dangers (Perumal, Sujatha, & Krishnan, 2025).

AI-powered behavioral analysis is critical in intrusion detection because it creates baseline profiles for users and devices and identifies deviations that may indicate potential breaches (Prince, Faheem, Khan, Hossain, Alkhayyat, Hamdache, & Elmouki, 2024). AI systems refine their detection capabilities and reduce false positives by self-learning from new instances of hostile behaviour (Mohamed, 2025). AI also coordinates automated threat containment solutions and network segmentation, hence improving incident response operations (Ismail, Kurnia, Brata, Nelistiani, Heo, Kim, & Kim, 2025). By automating common operations, AI enables security personnel to focus on complex risks and adopt strong organizational rules, hence increasing overall security posture (Sundaramurthy et al., 2022).

Implementing AI technology in cybersecurity necessitates tackling two major issues: computing costs for extended analysis and biased training inputs (Ozkan-Okay, Akin, Aslan, Kosunalp, Iliev, Stoyanov, & Beloev, 2024). Despite these challenges, research shows that AI's ability to alter cybersecurity makes it an essential component in developing resilient systems and networks (Ahsan et al., 2022). organizations can improve their entire cybersecurity posture by using the strengths of AI.

Table 2:
Cybersecurity in the AI Era: Applications, Hurdles, and Future Prospects

AI in Cybersecurity An Overview	Key AI Application in Cyber security	AI power threat detection, identifies anomalies in real time data detects hostile activity early.	
		Supervised Machine Learning Learners from labeled data recognizes known attack patterns	
		Unsupervised machine learning detects unknown threats, uses clustering and behavioral analysis.	
		AI in behavioral analysis, builds users and device baseline profiles detects deviations indicating breaches.	
		AI in incident response. Automates threats containment, managing network segmentation	
		Challenges in AI cyber security	High computational cost

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

			Extensive analysis requires sources
			Data Bias in Training Inaccurate training data impacts detection
		Future of AI in cyber security. Strengthening network defense reduces false positive and improves accuracy.	

AI-powered security solutions for WLANs use cutting-edge approaches to automatically detect and neutralize cyber threats. AI-powered intrusion detection systems use machine learning to detect potential security risks by analysing network data signatures.

Deep learning models increase packet data processing, enhancing accuracy in detecting zero-day attacks and subtle intrusions. Reinforcement learning enables AI systems to respond automatically, optimizing security procedures to protect devices without human intervention. Adaptive AI-powered encryption and authentication solutions modify cryptographic protocols based on threat intelligence, providing robust data protection against evolving threats. However, attackers employ machine learning to develop sophisticated attacks that circumvent AI defenses. To overcome this, it is necessary to maintain detection algorithms, provide reliable training data, and create strong architectural components. Adversarial machine learning exposes flaws in categorization methods, prompting researchers to create more robust algorithms.

AI security solutions are AI-based security systems that represent a game-changing method to defending WLANs from modern cyber threats by improving adaptability and complete protection. Implementing these technologies enables organizations to significantly reduce vulnerabilities in their wireless networks.

A methodical integration of security solutions yields powerful threat detection capabilities and automated protection systems that develop over time and respond to changing security vulnerabilities. AI-powered security solutions represent a huge step forward, allowing WLANs to transition from reactive to proactive defense, so increasing their defenses against sophisticated assaults. The combination of smart analytics and automation is important for safeguarding future wireless networks.

WLAN Security in the AI Era: A Comparative Analysis of Traditional WLAN security solutions, such as firewalls and signature-based intrusion detection systems, rely on predefined rules and manual configurations that are effective against known threats but frequently fail to detect emerging attack methods. In contrast, AI-powered detection systems that employ machine learning and data-driven approaches can detect abnormalities, increasing detection accuracy and

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

reducing false positives. This versatility is crucial for AI security, as models may learn from new threats and dynamically update their detection abilities. However, the advanced analytics used by AI models come at a cost, as training and deploying these systems requires enormous processing resources and memory capacity.

Key performance metrics, such as accuracy, false positive rate, and threat detection time, highlight the differences between traditional and AI-based security solutions. Conventional techniques may work well in predictable situations, but they typically fail to address innovative or large-scale challenges. In contrast, AI-based systems excel at identifying little anomalies in network traffic, but they require extensive training on a wide range of data to avoid biases and blind spots. Furthermore, AI models require ongoing maintenance to retain their performance, which involves constant retraining in response to new threats and changing network patterns.

Organizations must balance the benefits of adaptive AI-driven security with the potential constraints in resources and knowledge. A hybrid approach, which combines traditional security measures with machine learning capabilities, can create a robust, multi-layered protection plan that prioritises both dependability and reaction.

While AI techniques significantly improve WLAN security, their application raises ethical concerns that must be addressed. One major concern is the prospect of biased threat detection algorithms, which could lead to excessive false alerts for specific devices or user behaviors, compromising impartiality and eroding trust in AI-powered security systems. Furthermore, the computational needs of advanced AI models can place a strain on network infrastructure and hardware, providing a substantial barrier for organizations with limited resources or old equipment, complicating large-scale adoption.

The application of artificial intelligence in WLAN security raises questions regarding data privacy and compliance with security standards. AI models require huge datasets for optimal training, thus developers must ensure that sensitive information is handled properly and in accordance with legislation such as GDPR. Secure data collection, storage, and transmission are critical for avoiding data breaches and any legal ramifications. Furthermore, the growing threat of adversarial assaults on AI-powered security systems presents a huge problem, since attackers intentionally create tactics to avoid detection and compromise training data. To keep ahead of these challenges, we must develop novel defensive measures as well as effective countermeasures.

To solve these problems, organizations should implement best practices such as transparent AI, regular model assessments, and ongoing collaboration with regulatory bodies. This proactive strategy guarantees that emergent technologies are successfully integrated into established standards, facilitating the secure and responsible deployment of AI-driven WLAN solutions.

Methodology

Research Design

Creating effective AI-driven security solutions for WLANs frequently necessitates a mixed-methods approach that incorporates qualitative and quantitative research. Qualitative methods, such as interviews and observations, provide insights into organizational practices, user behaviors, and contextual factors that

ISSN Online: 3007-3154
ISSN Print: 3007-3146

influence network security, hence guiding hypothesis building and vulnerability detection. In contrast, quantitative methods use measurable performance measures such as detection rates, response times, and resource utilization to assess system efficacy.

Experimental design entails building controlled WLAN settings to evaluate alternative AI security strategies. Researchers create testbeds that simulate assaults, manage traffic, and design devices to capture a variety of scenarios. Investigators can assess the performance and operational capabilities of AI models by testing them under different threat complexities and network loads. This complete strategy tackles both the psychological and technical aspects of WLAN security, providing strong protection.

Data Collection

Data collection for AI-driven WLAN security research utilizes a variety of sources to achieve trustworthy and robust results. Public datasets such as CICIDS and NSL-KDD contain labelled attack logs that may be used to train and evaluate machine learning models. These datasets include a wide range of scenarios, allowing AI systems to distinguish between regular network behaviour and malicious activity, improving detection capabilities.

Researchers gather network traffic and historical data from operational WLAN configurations to inform their research. This ongoing research enables detection of current threat patterns, resulting in continuous model improvement. Data collection is mainly based on simulated cyberattacks, which allow researchers to assess AI defence skills against threats such as denial-of-service and rogue access points. By exposing AI models to a diverse set of potential threats, they can proactively defend WLAN systems.

A Case Research 1: Real-World Application: Fortinet's AI-Driven WLAN Security

Fortinet's FortiGate and FortiAnalyzer use AI-powered technologies to detect network traffic irregularities in real time, preventing large-scale corporate WLAN breaches. Automating threat detection and response allows organizations to lessen reliance on manual involvement, resulting in faster responses to targeted cyber threats. Fortinet's powerful analytics capabilities enable the detection of compromised devices, effective blocking of malicious activity, and continuous threat monitoring within enterprise networks.

Case Research 2: Palo Alto Networks AI-Driven Threat Detection

Palo Alto Networks' AI-powered threat detection identifies vulnerabilities in corporate WLANs via continuous monitoring. Using threat intelligence automation, users can identify irregularities in access points and respond to suspected DDoS attacks. The predictive method improves safety and system uptime, allowing administrators to respond rapidly to alerts issued by AI-powered solutions. The platform's detection standards are constantly updated in response to user feedback, minimizing false positives and enhancing accuracy. When the system detects suspicious activity, it initiates countermeasures such as rate-limiting or access control to ensure enterprise WLAN security.

Performance Metrics calculation

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

When evaluating WLAN security solutions that incorporate AI, several essential performance criteria must be considered. Accuracy is defined as the system's ability to correctly recognize risks and typical traffic patterns. Precision and recall metrics provide additional insight into system accuracy by measuring the capacity to reduce false warnings while detecting actual assaults. High accuracy implies fewer false positives, and high recall indicates excellent threat detection.
False positive and false negative rates are critical performance indicators. Excessive false alarms overload security professionals, while false negatives result in undetected vulnerabilities. Real-time defence systems require efficient performance. AI-powered protection should sustain network speeds while adjusting to changing workloads without sacrificing operational speed. Furthermore, the system's value is in its ability to react to new security threats, which necessitates continuous upgrades and dynamic training processes to maintain proactive defense.

Results and Data Presentation

Table 3:
WLAN Security Performance Evaluation: 72-Hour Comparative Research

Metric	**AI-Driven Security**	**Traditional Security**
Test Duration (hours)	75	75
Number of Devices	5,500	5,500
Overall Detection Rate (%)	94%	73%
Increase in Detected Suspicious Activities	+27%	Baseline
Peak Attack Occurrences	65% during peak hours	Not Specified
High-Risk Threat Proportion	13% of flagged threats	Not Specified

Findings

Table 3 compares the performance of AI-driven and traditional WLAN security over 75 hours, illustrating the improved detection capabilities, accurate threat identification, and superior peak attack awareness achieved by AI-powered security systems.
Practical WLAN security installations provide important insights into the advantages and disadvantages of AI-powered solutions. Organizations that use AI-powered monitoring solutions see fewer undiscovered breaches and faster incident reaction times. Automated detection systems discover anomalies fast, resulting in much shorter response times. This allows security personnel to focus on more difficult investigations while automated systems perform ordinary traffic analysis.
In enterprise environments, AI-powered solutions optimize resource allocation by dynamically changing defenses in response to real-time threat levels. However, case studies show the importance of continual retraining of AI models to meet evolving dangers, which requires regular updates to be successful. When implementing AI-driven security solutions, organizations must balance computing costs and security benefits. Finally, case studies show that AI

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

dramatically improves WLAN security.

Comparative Analysis

Different AI security systems offer advantages and disadvantages in terms of performance, accuracy, and adaptability. Machine learning systems are superior at detecting anomalies beyond standard traffic patterns, surpassing signature-based methods and shortening detection times. However, these modern technologies require a large amount of processing power, which can put a strain on current infrastructure, especially in high-traffic regions.

AI-driven models can achieve high detection accuracy and low false positive rates, however the results vary depending on the algorithm and training data quality. AI security systems are adaptable and can learn from new threats through retraining, making them effective in dynamic contexts. In contrast, static rule-based systems lack flexibility. When integrating AI, company leaders must assess the expenses against the potential security benefits, such as fewer breaches and better protection. The choice of AI approach is determined by the network's specific security requirements.

Discussion and Interpretation of Results

AI security systems outperform traditional methods in crucial areas. AI systems can detect subtle dangers that rule-based techniques frequently miss by using machine learning algorithms on massive datasets and real-time network feedback. This increased detection capability allows for faster and more accurate threat identification. Furthermore, AI systems automatically update threat models, allowing them to respond swiftly to new assaults and reduce network vulnerability.

AI's quick processing and automation skills narrow the window of vulnerability to attacks. AI-powered security frameworks can recognize dangerous tendencies and quickly execute countermeasures, such as isolating segments and banning questionable IP addresses. This proactive method greatly reduces response times, offering organizations a competitive advantage in preventing invasions. Experimental results show that AI-driven security solutions beat traditional methods for improving WLAN protection efficacy.

Future Implications

WLAN security can be considerably improved in a variety of circumstances by adopting the findings of this study. Network administrators and cybersecurity teams may add AI-powered threat detection to their existing infrastructure, supplementing traditional firewalls and intrusion detection systems with data-driven insights. This technique enables a seamless transition to AI-enhanced security while retaining familiar interfaces for ongoing maintenance.

To maximize AI's effectiveness, it is critical to implement continuous model training with new data and threat signatures, allowing businesses to stay ahead of changing threats and reduce the chance of breaches. Fine-tuning alert levels is also necessary to ensure that human operators receive timely warnings for critical circumstances while not being swamped by low-risk notifications. By finding this equilibrium, AI improves security while minimizing complexity and operator burnout. A well-thought-out integration strategy is critical to the long-term success of AI-based WLAN security.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

Challenges and Limitations

While AI-driven security solutions show promise, they confront substantial difficulties that may prevent mainstream implementation. One important concern is the possibility of false alerts, especially if AI models are trained on insufficient or biased data. High false alarm rates can strain resources, cause alert fatigue, and undermine trust in automated systems. Furthermore, ethical and legal considerations occur when AI analyses massive amounts of personal network data, which may violate user privacy. Balancing thorough monitoring with data privacy compliance is a delicate challenge.

The cost and scalability of AI technologies are important considerations. Implementing AI-driven security frequently necessitates specialized gear and extensive computational capacity, resulting in significant upfront expenses. This might be a barrier for smaller organizations or those with tight budgets, making it difficult to justify the investment despite the obvious security benefits. AI-driven WLAN security requires careful planning and resource allocation to balance performance and cost-effectiveness.

Future Recommendations

To improve AI-powered WLAN security, businesses should take a tiered strategy that blends AI solutions with traditional security controls. For example, combining machine learning-based intrusion detection with powerful firewall systems results in comprehensive coverage and in-depth analysis. Furthermore, ongoing model retraining is required, including updates based on new threats or network behaviors to ensure the AI remains successful at detecting emerging assaults.

Future research should focus on federated learning, which allows for collaborative AI training across many networks while ensuring data privacy. Creating lightweight AI models for edge devices may also address scalability and cost issues. Furthermore, creating open rules and user education programs can help to address ethical concerns by empowering stakeholders to understand data usage and security. By taking a staged approach to AI-driven security, businesses can fine-tune their strategy, reduce disruptions, and greatly improve WLAN protection.

Conclusion

WLAN security is a top priority due to ongoing threats from a variety of attack vectors, including rogue access points, advanced malware, and sophisticated intrusions. Traditional security measures frequently fall short of tackling the complexity and quick evolution of emerging threats, emphasizing the necessity for more dynamic and proactive approaches. AI-driven security provides a significant edge by employing superior pattern recognition and automatic response capabilities to effectively combat threats in real time.

AI can swiftly identify anomalies, isolate affected devices, and reduce false warnings, improving incident response. Studies regularly show that AI improves threat detection, response times, and network resilience while lowering security costs. As a result, AI-driven techniques are poised to transform WLAN security by offering intelligent, adaptive protection that keeps up with the changing cyber threat landscape.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

Future Recommendations

The future of WLAN security will most likely involve a greater integration of AI and sophisticated technologies such as quantum security. Quantum cryptography may provide strong encryption, making it extremely difficult for attackers to intercept or decipher wireless data. Furthermore, continued advances in AI-driven anomaly detection will improve proactive threat identification, with powerful machine learning models capable of identifying even the most covert attacks.

The introduction of 6G networks, with their ultrafast data transfer speeds and widespread device connectivity, will present new opportunities and difficulties for WLAN security. AI-powered solutions will need to expand to manage rising traffic volume and device diversity while maintaining accuracy and speed. The combination of AI, quantum security, and upcoming network standards will eventually define the future of WLAN defence, allowing for more robust, adaptive, and resilient solutions to secure wireless infrastructures.

References

Abd-el-Kader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D. E. A., ... & Prokop, L. (2024). Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. *Results in Engineering,* 102647.

Adbeib, K. A. (2023). Comprehensive study on wi-fi security protocols by analyzing wep, wpa, and wpa2. *African Journal of Advanced Pure and Applied Sciences* (AJAPAS), 385-402.

Afzal, F., Uzair, A., Javed, M. A., & Naqvi, S. A. A. (2024). An Enhanced Approach for Wi-Fi Security and Authentication Protocols: A Systematic Approach towards WEP, WPA, WPA2, and WPA3. *Spectrum of Engineering Sciences*, 2(5), 379-403.

Aggarwal, V., & Gupta, H. (2024). A Comprehensive Analysis of Emerging Threats in the Digital Era. In 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 1-4). IEEE.

Akhtar, Z. B., & Rawol, A. T. (2024). Enhancing cybersecurity through AI-powered security mechanisms. *IT Journal Research and Development,* 9(1), 50-67.

Akinade, A. O., Adepoju, P. A., Ige, A. B., & Afolabi, A. I. (2025). Cloud security challenges and solutions: *A review of current best practices. Int J Multidiscip Res Growth Eval,* 6(1), 26-35.

Alamleh, H., Estremera, L., Arnob, S. S., & AlQahtani, A. A. S. (2025). Advanced Persistent Threats and Wireless Local Area Network Security: An In-Depth Exploration of Attack Surfaces and Mitigation Techniques. *Journal of Cybersecurity and Privacy,* 5(2), 27.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

Aldawsari, H., & Kouchay, S. A. (2023). Integrating AI and Machine Learning Algorithms in Cloud Security Frameworks for Enhanced Proactive Threat Detection and Mitigation. *Journal of Emerging Threat Management*.

Alhamry, M., & Alomary, A. (2022, October). Exploring Wi-Fi WPA2-PSK protocol weaknesses. In 2022 International Conference on Data Analytics for Business and Industry (ICDABI) (pp. 190-195). IEEE.

AlShourbaji, I. (2013). An overview of wireless local area network (WLAN). *arXiv preprint arXiv:*1303.1882.

Aminu, M., Akinsanya, A., Dako, D. A., & Oyedokun, O. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*, 13(8), 11-27.

Bhadouria, A. S. (2022). Study of: impact of malicious attacks and data breach on the growth and performance of the company and few of the world's biggest data breaches. International Journal of Scientific and Research Publications, 10(10), 1-11.

Btoush, A., Abadleh, A., Alkasasbeh, A. A., & Alghamdi, M. (2024). *The Intrusion Detection and Recovery of DE authentication Frame in WPA3 SAE.*

Chander, B., Pal, S., De, D., & Buyya, R. (2022). Artificial intelligence-based internet of things for industry 5.0. *Artificial Intelligence-Based Internet of Things Systems,* 3-45.

Chukwunweike, J. N., Adewale, A. A., & Osamuyi, O. (2024). Advanced modelling and recurrent analysis in network security: Scrutiny of data and fault resolution. *World Journal of Advanced Research and Reviews*, 23(2), 2373-2390.

Dine, F. (2024). Cyber Threat Analysis and the Development of Proactive Security Strategies for Risk Mitigation.

Farraj, A., & Hammad, E. (2024). Noise-Based Active Defense Strategy for Mitigating Eavesdropping Threats in Internet of Things Environments. *Computers,* 14(1), 6.

Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2025). IoT and man-in-the-middle attacks. *Security and Privacy*, 8(2), e70016.

Firdus, E., Aghababayev, R., Aliyev, V., Mustafayeva, G., Mayilov, R., Sardarova, I., & Bakhshaliyeva, S. (2024). WiFi from past to today, consequences that can cause and measures of prevention from them, WiFi security protocols. In E3S Web of Conferences (Vol. 474, p. 02004). EDP Sciences.

Gudimetla, S., & Kotha, N. (2017). Firewall Fundamentals-Safeguarding Your

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Digital Perimeter. *NeuroQuantology,* 15(4), 200-207.

Gupta, B. B., & Dahiya, A. (2021). Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures. CRC Press.

Halbouni, A., Ong, L. Y., & Leow, M. C. (2023). Wireless security protocols wpa3: A systematic literature review. IEEE Access, 11, 112438-112450.

Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing,* 26(6), 3753-3780.

Herath, H. M. S. S., Herath, H. M. K. K. M. B., Madhusanka, B. G. D. A., & Guruge, L. G. P. K. (2024). Data protection challenges in the processing of sensitive data. In Data Protection: The Wake of AI and Machine Learning (pp. 155-179). Cham: Springer Nature Switzerland.

Huang, C. J., Chi, C. J., & Hung, W. T. (2023). Hybrid-AI-based iBeacon indoor positioning cybersecurity: Attacks and defenses. Sensors, 23(4), 2159.

Humayun, M., Tariq, N., Alfayad, M., Zakwan, M., Alwakid, G., & Assiri, M. (2024). Securing the Internet of Things in artificial intelligence era: A comprehensive survey. IEEE Access, 12, 25469-25490.

Ismail, Kurnia, R., Brata, Z. A., Nelistiani, G. A., Heo, S., Kim, H., & Kim, H. (2025). Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic Artificial Intelligence. Information, 16(5), 365.

Jain, V., & Mitra, A. (2025). Enhancing Resilience in Business Continuity Management: Strategies and Best Practices. In Enhancing Resilience in Business Continuity Management (pp. 1-30). IGI Global Scientific Publishing.

Jimmy, F. N. U. (2024). Cyber security vulnerabilities and remediation through cloud security tools. *Journal of Artificial Intelligence General Science* (JAIGS) ISSN: 3006-4023, 2(1), 129-171.

Kumar, Y., & Kumar, V. (2023). A Systematic Review on Intrusion Detection System in Wireless Networks: *Variants, Attacks, and Applications*. Wireless Personal Communications, 133(1), 395-452.

Lindroos, S., Hakkala, A., & Virtanen, S. (2021). A systematic methodology for continuous WLAN abundance and security analysis. *Computer Networks,* 197, 108359.

LUWONGO, R. (2023). Assessment of the Security Threats Facing Protection of Wireless Lan Users in Public Institutions (Doctoral dissertation, IAA).

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Mahfuri, M., Ghwanmeh, S., Almajed, R., Alhasan, W., Salahat, M., Lee, J. H., & Ghazal, T. M. (2024, February). Transforming Cybersecurity in the Digital Era: The Power of AI. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-8). IEEE.

Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News,* 190(1), 1-69.

Manda, J. K. (2024). AI-powered Threat Intelligence Platforms in Telecom: Leveraging AI for Real-time Threat Detection and Intelligence Gathering in Telecom Network Security Operations. Available at SSRN 5003638.

Martin, S., & Ibrahim, M. (2024). Cybersecurity Paradig, Threats Innovative Strategies for Protecting Digital Assets. *Advances in Computer Sciences,* 7(1), 1-7.

Mawgoud, A. A., Taha, M. H. N., Abu-Talleb, A., & Kotb, A. (2022). A deep learning based steganography integration framework for ad-hoc cloud computing data security augmentation using the V-BOINC system. *Journal of Cloud Computing*.

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems, 1-87.

Mohammed, A. (2023). SOC Audits in Action: Best Practices for Strengthening Threat Detection and Ensuring Compliance. *Baltic Journal of Engineering and Technology,* 2(1), 62-69.

Muppalaneni, R., Inaganti, A. C., & Ravichandran, N. (2024). AI-Driven Threat Intelligence: Enhancing Cyber Defense with Machine Learning. *Journal of Computing Innovations and Applications*, 2(1), 1-11.

Mwenja, J. M. (2017). Framework for securing wireless local area network (Doctoral dissertation).

Nazir, R., Laghari, A. A., Kumar, K., David, S., & Ali, M. (2021). Survey on wireless network security. *Archives of Computational Methods in Engineering,* 1-20.

Nwoye, C. C. (2024). Next-generation protection protocols and procedures for securing critical infrastructure. *International Journal of Research Publication and Reviews*, 5(11), 4830-4845.

Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews,* 21(1), 2286-2295.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. IEEE Access, 12, 12229-12256.

Pahlavan, K., & Krishnamurthy, P. (2009). Networking fundamentals: *Wide, local and personal area communications*. John Wiley & Sons.

Patil, D. (2024). Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Prevention Mechanisms Through Machine Learning and Data Analytics. Available at SSRN 5057410.

Paul, J. (2024). Comparative Analysis of Supervised vs. Unsupervised Learning in API Threat Detection.

Perumal, S., Sujatha, P. K., & Krishnan, M. (2025). Clusters in chaos: A deep unsupervised learning paradigm for network anomaly detection. *Journal of Network and Computer Applications*, 235, 104083.

Prince, N. U., Faheem, M. A., Khan, O. U., Hossain, K., Alkhayyat, A., Hamdache, A., & Elmouki, I. (2024). AI-powered data-driven cybersecurity techniques: Boosting threat identification and reaction. Nanotechnology Perceptions, 20, 332-353.

Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in internet of things: *Challenges, countermeasures, and future directions*. Ad Hoc Networks, 146, 103159.

Sachan, R. C., Lakhani, R., & Poddar, S. (2025). AI-enabled security mechanisms for WLANs: ensuring robust and adaptive protection in wireless networks. World J. Adv. Res. Rev, 25(3), 2085-2095.

Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science,* 10(6), 1473-1498.

Schepers, D. (2023). Towards Rapid Prototyping for Wi-Fi Security Research (Doctoral dissertation, Northeastern University).

Singh, S. (2023). Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) For Network Security: A Critical Analysis. Advanced Journal in Wireless and Mobile Communication, 123.

Spanca, F., & Salihu, A. (2024). Unveiling the Consequences of Data Breaches: Risks, Impacts, and Mitigation in the Digital Age. In 2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE) (pp. 1-8). IEEE.

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 6 (June) (2025)

Srinivasa, S., Pedersen, J. M., & Vasilomanolakis, E. (2021, November). Open for hire: attack trends and misconfiguration pitfalls of IoT devices. In Proceedings of the 21st ACM Internet Measurement Conference (pp. 195-215).

Suroto, S. (2018). WLAN security: threats and countermeasures. JOIV: *International Journal on Informatics Visualization*, 2(4), 232-238.

Tahmasebi, M. (2024). Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises. *Journal of Information Security*, 15(2), 106-133.

Thakur, H. N., Al Hayajneh, A., Thakur, K., Kamruzzaman, A., & Ali, M. L. (2023). A Comprehensive Review of Wireless Security Protocols and Encryption Applications. In 2023 IEEE World AI IoT Congress (AIIoT) (pp. 0373-0379). IEEE.

Yaseen, A. (2022). Successful Deployment of Secure Intelligent Connectivity for LAN and WLAN. Journal of Intelligent Connectivity and Emerging Technologies, 7(4), 1-22.

Zhao, G., & Song, J. (2020). Network security model based on active defense and passive defense hybrid strategy. Journal of Intelligent & Fuzzy Systems, 39(6), 8897-8905.

Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks, 8(4), 422-435.