International Journal of
Science, Architecture, Technology and Environment

AI Based Intrusion Detection and Prevention System for Securing Wireless Communication Networks

Comfort Gyamea Acka[1*], Abosede Oluwabunmi Adelore[2], Emmanuel Toba Popoola[3], Saeed Hubairik Aliyu[4], Abdullateef Akorede Ademoye[5]

[1]*Department of Computer Science, Kumasi Technical University , Ghana*

[2]*Department of Computer Science, University of Ghana, Ghana*

[3]*Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Nigeria*

[4]*Department of Mechatronics and Robotics Engineering, South Ural State University, Russia*

[5]*Department of Computer Sciences, University of Lagos, Nigeria*

[*]*Corresponding author*

DOI: https://doi.org/10.63680/ijsate0725028.15

Abstract

As wireless communication networks become increasingly integral to modern infrastructure, they face a growing threat from sophisticated cyberattacks. This paper explores the development and implementation of AI based Intrusion Detection and Prevention Systems (IDPS) designed to secure wireless networks through intelligent, adaptive threat detection and mitigation. Leveraging advanced artificial intelligence (AI) and machine learning (ML) algorithms, these systems are capable of monitoring real time network traffic, identifying anomalies, and responding proactively to potential intrusions. Techniques such as supervised learning, deep learning, and ensemble methods enable the accurate classification of malicious behaviour, while explainable AI (XAI) helps address transparency and accountability concerns. Despite their promise, AI based IDPS face several challenges, including compliance with data protection regulations, the interpretability of complex models, and performance limitations in resource constrained environments. This paper discusses the current state, applications, challenges, and future directions of AI enabled IDPS, offering a comprehensive framework for enhancing the resilience of wireless communication systems.

Keywords: Intrusion Detection and Prevention System (IDPS), Wireless Network Security, Artificial Intelligence (AI), Machine Learning (ML), Deep Learning, Anomaly Detection

1.0 Introduction

An AI Based Intrusion Detection and Prevention System (IDPS) for securing wireless communication networks represents a cutting-edge approach to enhancing cybersecurity in an era where wireless technologies are

ubiquitous and increasingly vulnerable to cyber threats. These systems employ advanced artificial intelligence (AI) and machine learning (ML) techniques to continuously monitor network traffic, detect anomalies, and respond to potential intrusions in real time, thereby ensuring the integrity and confidentiality of transmitted data [1][2][3]. The importance of such systems is underscored by the growing sophistication of cyberattacks targeting wireless networks, which necessitate innovative and adaptive security measures to safeguard sensitive information [4][5][6].

The integration of AI into IDPS significantly enhances their detection capabilities by enabling the systems to learn from historical data, identify complex attack patterns, and adapt to evolving threats[7][8]. Prominent methods include supervised and unsupervised learning algorithms, which help differentiate between normal and malicious activities, as well as deep learning techniques that recognise intricate patterns within network traffic [9][10]. Despite these advancements, the field faces several challenges, including regulatory compliance, data quality issues, and the technical limitations of current AI models, all of which can impede the effectiveness of these systems [11][12].

Notably, controversies surrounding the deployment of AI in IDPS often focus on ethical considerations and transparency, particularly regarding the 'black box' nature of many AI models that complicates accountability and trust among security analysts [13][14]. Moreover, concerns about privacy and data protection laws, such as the General Data Protection Regulation (GDPR), add layers of complexity to the integration of these technologies in sensitive sectors like finance and healthcare [15]. As organisations increasingly adopt AI based IDPS, addressing these challenges and controversies will be essential to realise their full potential in securing wireless communication networks against ever evolving threats.

Background

Introduction to Wireless Security

As wireless networks become increasingly integral to everyday communication and data transfer, the necessity for robust security measures has escalated. Wireless Intrusion Detection and Prevention Systems (IDPS) are vital components of network security designed to protect against unauthorised access and cyber threats. These systems can identify suspicious activities in real time, enabling swift responses to potential breaches and ensuring the integrity of data transmitted over wireless channels [1][2].

Importance of Intrusion Detection and Prevention Systems

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) form the backbone of cybersecurity in wireless networks. IDS actively monitors network traffic for anomalies and alerts administrators when potential threats are detected, while IPS goes a step further by actively preventing intrusions [3]. The implementation of machine learning based techniques within these systems enhances their capability to detect sophisticated threats, making them essential for maintaining security in the rapidly evolving landscape of wireless communication[4][5].

Advanced Techniques in Wireless Intrusion Prevention

Recent advancements in artificial intelligence and machine learning have significantly influenced the effectiveness of wireless intrusion prevention. Techniques such as machine learning based intrusion detection systems and AI powered security analytics are at the forefront of current research. These technologies analyse

network traffic patterns to identify deviations indicative of potential security threats, thus improving response times and accuracy in threat detection [6][4]. As cyber threats continue to evolve, the integration of advanced technologies in IDPS will be critical for safeguarding wireless networks from increasingly complex attacks [7][2].

The Role of Feature Importance in Machine Learning

Understanding feature importance is crucial for enhancing the interpretability of machine learning models used in wireless intrusion detection. SHAP (SHapley Additive exPlanations) values are employed to rank the significance of various features in predicting outcomes. For instance, features such as 'Flow IAT Max' and 'Flow Duration' have been identified as having substantial impacts on model predictions, demonstrating the importance of effectively analysing feature contributions to improve detection capabilities [7]. This analytical approach not only bolsters model performance but also provides insights that can inform further security enhancements.

AI Techniques in IDPS

AI techniques have revolutionised the development of Intrusion Detection and Prevention Systems (IDPS) by significantly enhancing their ability to identify and mitigate cyber threats in real time. The integration of machine learning (ML) and deep learning (DL) has enabled these systems to analyse vast amounts of data, detect complex attack patterns, and adapt to evolving security challenges.

Machine Learning Approaches

Machine learning forms the backbone of AI driven IDPS, utilising algorithms that can learn from historical data and improve their detection capabilities over time. Supervised learning algorithms such as Support Vector Machines (SVM), Decision Trees (DT), and Random Forests (RF) are commonly employed to classify network activities as either normal or malicious based on labelled datasets [8][9]. For instance, SVM, grounded in Statistical Learning Theory, seeks to identify hyperplanes that effectively separate different classes of data, thus enhancing classification accuracy in IDS [8].

In contrast, unsupervised learning techniques operate without predefined labels, allowing them to detect new and unknown threats. Methods such as K means clustering and anomaly detection are employed to identify deviations from established patterns of normal behaviour [10][9]. This capability is crucial for identifying previously unseen cyber threats, making unsupervised learning a valuable asset in modern IDPS.

Deep Learning Techniques

Deep learning, a subset of machine learning, further enhances the capabilities of IDPS by employing multi layered neural networks to identify intricate patterns in data[10][9]. Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) are particularly adept at handling sequential data and recognising complex features, thus improving the system's ability to detect sophisticated cyber threats[11]. For example, RNNs have been utilised to analyse time series data in network traffic, allowing for more effective intrusion detection.

Ensemble Methods

Ensemble methods, which combine multiple models to improve prediction accuracy, are also widely used in AI based IDPS. Techniques like Random Forest and Gradient Boosting aggregate the outputs of various models, leading to more robust performance in identifying threats[10][9]. This approach is particularly effective in commercial security systems where accuracy and reliability are paramount.

Explainable AI

A growing trend in the field of IDPS is the incorporation of Explainable AI (XAI) techniques, which aim to improve the transparency and interpretability of complex machine learning models [7]. As these models become increasingly sophisticated, their 'black box' nature can hinder trust among security analysts. Techniques such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model agnostic Explanations) provide insights into model predictions by highlighting which features were most influential in the detection process, thereby enhancing the system's credibility and usability [7].

Evaluation Metrics

To assess the performance of AI driven IDPS, several evaluation metrics are utilised, including accuracy, precision, recall, and F1 score. While accuracy measures the overall correctness of the model's predictions, it can be misleading in cases of class imbalance, where a model may achieve high accuracy by predominantly predicting the majority class[7]. Therefore, a combination of metrics is essential for a comprehensive evaluation of the model's effectiveness in detecting intrusions.

Architecture of AI Based IDPS

The architecture of AI based Intrusion Detection and Prevention Systems (IDPS) integrates various components that work collectively to enhance the security of wireless communication networks. This architecture typically encompasses data handling and processing, threat detection model development, and response mechanisms to identified threats.

Data Handling and Processing

At the core of AI based IDPS is robust data handling and processing, which involves the collection, cleaning, and analysis of extensive data sets to identify potential threats. Key sources of data include network traffic logs, system event logs, and user activity records, complemented by real time threat intelligence collected through API integrations and automated scraping technologies [9].

Preprocessing Steps

Before training models, several preprocessing steps are vital to ensure data quality and relevance.

Data Cleaning: This involves removing duplicates and outliers, handling null values, and generalising field values for consistency. Techniques like z score can be employed to eliminate outliers [8].

Feature Selection and Engineering: Feature selection focuses on identifying the most relevant data attributes that contribute significantly to threat detection. Algorithms such as mutual information-based feature

selection are utilised to optimise model performance by discarding redundant features and engineering new ones from existing data [9][8].

Threat Detection Model Development

The development of threat detection models is a critical aspect of the AI based IDPS architecture. Models leverage machine learning algorithms that adapt and refine their parameters over time, significantly reducing false positive rates and enhancing detection accuracy. For instance, advanced models like HAEnID utilise ensemble learning techniques, integrating various classifiers such as Decision Trees (DT), Random Forests (RF), and LightGBM (LGBM) to improve detection efficacy [7].

Model Features

Stacking Ensemble Component: This component enhances diversity in the model by combining the outputs of different base classifiers, allowing the system to capture complex patterns in the data[7].

Adaptability and Robustness: The integration of components like Stacked Ensemble Method (SEM), Bayesian Model Averaging (BMA), and Classifier Ensemble Model (CEM) contributes to the model's robustness and adaptability, enabling it to respond effectively to evolving threats [7].

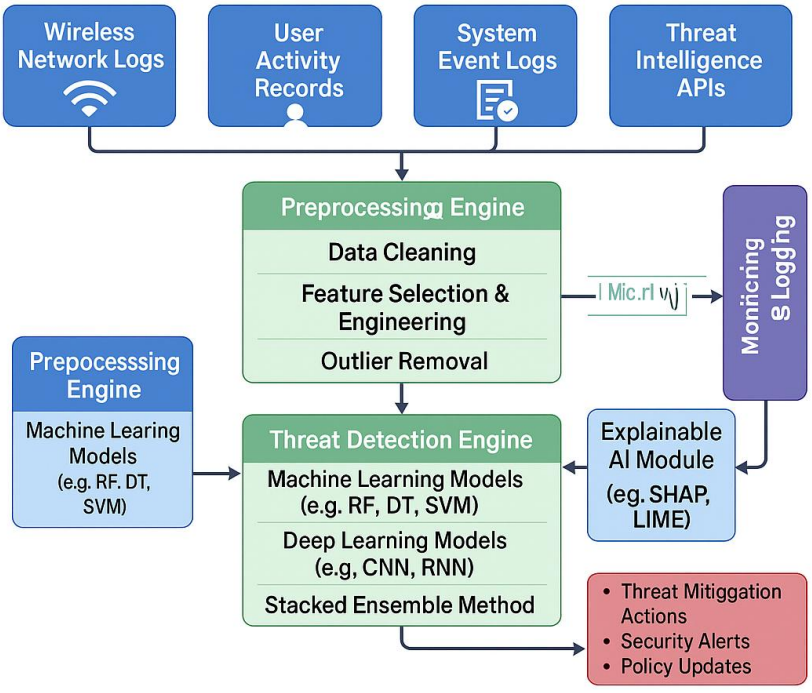

Figure 1: Architecture of AI Based Intrusion Detection and Prevention System (IDPS)

Response Mechanisms

AI based IDPS not only detects threats but also initiates responses to mitigate potential impacts. The

architecture incorporates automated response mechanisms that leverage real time data analysis to reduce response times significantly. Traditional systems might take minutes to react, while AI driven solutions can respond instantaneously, improving overall network security posture [10].

This architecture ensures that AI based IDPS is equipped to handle the complexities of modern wireless communication networks, adapting to new threats and maintaining high levels of security efficacy.

4.0 Applications

AI based intrusion detection and prevention systems (IDPS) have seen a significant increase in their application across various sectors, particularly in enhancing the security of wireless communication networks. These systems leverage advanced machine learning (ML) and artificial intelligence (AI) techniques to identify and mitigate potential cyber threats in real time.

4.1 Financial Sector

In high stakes environments such as banks and financial institutions, the need for robust security measures is paramount. Organisations like JPMorgan Chase utilise AI driven IDPS to monitor network traffic and detect anomalies that could signify potential breaches. These systems not only alert security teams but also analyse patterns to reduce unauthorised access attempts and protect sensitive customer data and financial information effectively [12][10]. The integration of AI into these systems has proven to significantly enhance the security posture of financial institutions, making them more resilient against cyberattacks.

4.2 Healthcare Facilities

Healthcare facilities, which handle vast amounts of sensitive personal and medical data, are also increasingly adopting AI based IDPS. These systems provide critical protection against data breaches, ensuring compliance with stringent regulatory requirements regarding patient privacy and data security. The ability of AI to analyse and learn from patterns in data allows these systems to detect even the most sophisticated threats that traditional security measures might overlook [13][10].

4.3 Cloud Data Storage

The adoption of AI in cloud data storage systems has also been notable. For instance, Talib et al. proposed a multi agent system architecture that utilises agent-oriented methodologies for securing cloud environments. Their model integrates various agents that operate independently to enhance security and respond to threats in real time. By improving scalability and reducing bottlenecks, this architecture addresses complex challenges associated with cloud security effectively [7][14].

4.4 Wireless Networks

AI technologies are being utilised to enhance the efficiency and security of wireless networks through various innovative applications. The implementation of AI algorithms in wireless environments allows for better detection of intrusions and faster response times. Moreover, AI's capacity for unsupervised learning enables the identification of unknown threats by analysing network behaviour and anomalies, making it a powerful tool for maintaining network integrity [13][10].

4.5 Challenges

AI based intrusion detection and prevention systems (IDPS) face several significant challenges that can impact their effectiveness and adoption in securing wireless communication networks.

4.6 Regulatory Compliance and Accountability

In many industries, especially those that are heavily regulated, such as finance, healthcare, and government, there are strict regulatory requirements mandating transparency and accountability in decision making processes. AI models, particularly black box systems, often lack the necessary transparency to provide auditable explanations of their decisions. This lack of clarity can lead to compliance challenges and potential legal liabilities, making it critical for organisations to choose interpretable models that can meet these regulatory standards [14].

4.7 Resistance to Adoption and Integration

The integration of AI technologies into existing security frameworks can be met with resistance due to various factors, including organisational culture, resource constraints, and the complexity of the technology. Organisations must evaluate their unique needs and available resources when selecting between different types of intrusion detection systems (IDS), whether host based or network based, and consider whether a standalone or integrated approach is best suited for their environment [17]. The challenge lies not only in selecting the right technology but also in effectively integrating it into the existing security infrastructure.

4.8 Data Quality and Ethical Concerns

Implementing AI powered IDPS involves significant challenges related to data quality and ethical considerations. AI systems require high quality data for training; thus, issues such as data bias and incompleteness can severely limit their performance. Additionally, ethical concerns arise from the potential misuse of data, particularly personal data collected during intrusion detection processes. Compliance with data protection regulations like the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) is imperative, necessitating clear consent and stringent data handling practices [10][2].

4.9 Technical and Reliability Issues

AI and machine learning (ML) models can encounter technical challenges, such as data integration and reliability concerns. For instance, IoT devices, often used in wireless communication networks, are typically resource constrained, possessing limited power and processing capabilities. These limitations can hinder the effectiveness of AI algorithms, especially when dealing with large datasets or complex attack patterns. Furthermore, the evolving nature of cyber threats demands continuous updates and improvements to the detection algorithms, which can strain the resources of organisations [12][18][19].

4.91 Security and Privacy Risks

The deployment of AI in IDPS introduces new security risks, including vulnerabilities to data breaches and model inversion attacks. Protecting sensitive information and ensuring compliance with privacy regulations is essential for maintaining user trust. Organisations must adopt robust encryption methods and secure data

storage practices to safeguard against potential breaches while also considering the implementation of privacy preserving techniques, such as federated learning, to maintain data confidentiality [20][2].

By addressing these multifaceted challenges through careful planning and strategic implementation, organisations can enhance the security and effectiveness of AI based intrusion detection and prevention systems within wireless communication networks.

Future Trends

5.1 Integration of AI and Machine Learning

The future of AI based intrusion detection systems (IDS) is poised for significant advancements driven by the integration of artificial intelligence (AI) and machine learning (ML) technologies. Continuous improvements in these fields are expected to enhance detection and response capabilities, resulting in more intelligent and adaptive security systems for wireless communication networks [10]. As organisations increasingly adopt these technologies, they must prioritise ongoing learning and stay abreast of emerging trends to navigate the evolving cybersecurity landscape effectively [21].

5.2 Ethical and Regulatory Considerations

With the incorporation of AI and ML in security systems, ethical considerations and regulatory compliance become paramount. Stakeholders must ensure that these technologies are developed responsibly, maintaining public trust and adhering to legal standards [10]. As AI systems are implemented, it is crucial to design them in a manner that avoids biases and promotes fairness in security measures. This necessitates rigorous testing and refinement of algorithms to prevent the perpetuation of historical biases that could lead to unfair targeting [21].

5.3 Advances in Wireless Security Technologies

Several emerging technologies are anticipated to reshape the future of wireless security, including the proliferation of 5G and the Internet of Things (IoT). The adoption of these technologies will introduce new security challenges and opportunities, necessitating innovative approaches to intrusion detection [20]. For instance, the complexity introduced by 5G and IoT devices will require the development of more sophisticated and dynamic security protocols [20].

Moreover, advancements in quantum computing could potentially undermine current encryption methods, prompting the need for new strategies to secure wireless communications against evolving threats [20].

5.4 Ensemble based Intrusion Detection Systems

The future of IDS will likely see a growing emphasis on ensemble-based methods that combine multiple machine learning models to improve detection accuracy and reduce false alarm rates. Techniques such as stacking ensemble learning will enable systems to leverage the strengths of various classifiers while minimising weaknesses, enhancing overall system robustness [7]. These methods, including the use of classifiers like Random Forest (RF), Decision Trees (DT), and k Nearest Neighbours (k NN), are expected to deliver better performance across diverse datasets and scenarios [7][2].

5.5 Explainable AI in Security Systems

As AI technologies become integral to security frameworks, the demand for transparency and interpretability in AI models will increase. Future developments are likely to focus on explainable AI (XAI) techniques, which aim to provide clarity and justifications for AI driven decisions in intrusion detection systems. By enhancing understanding and trust among operators and analysts, XAI can facilitate more effective collaboration between human users and AI systems [2]. This will be critical in establishing a reliable framework that empowers security teams to make informed decisions based on AI insights.

6.0 Conclusion

The increasing dependence on wireless communication networks, coupled with the escalating sophistication of cyber threats, necessitates the deployment of intelligent and adaptive security solutions. This study explored the integration of Artificial Intelligence (AI) techniques including machine learning (ML), deep learning (DL), ensemble models, and explainable AI within Intrusion Detection and Prevention Systems (IDPS) to enhance wireless network security. Through the evaluation of current methodologies, architectures, and application domains, it is evident that AI driven IDPS offers significant improvements in real time threat detection, adaptability to emerging attack patterns, and precision in identifying anomalies.

Despite these advantages, the implementation of AI based IDPS is not without challenges. Issues such as data quality, interpretability, regulatory compliance, and resource limitations in wireless environments must be addressed to ensure effective deployment. Moreover, ethical considerations and the need for explainable decision-making models are crucial to fostering trust and accountability among cybersecurity professionals and stakeholders.

Looking ahead, the evolution of 5G, IoT, and quantum computing will introduce both new opportunities and vulnerabilities, making continuous innovation in IDPS architecture imperative. Embracing ensemble learning, federated learning, and transparent AI frameworks will be key to advancing the robustness and trustworthiness of these systems. By proactively addressing existing challenges and aligning with ethical and regulatory standards, AI based IDPS can play a transformative role in fortifying the next generation of wireless communication networks.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

The author received no financial support for the research, authorship and publication of this article.

References

[1] A. PUS, "Intrusion Detection and Prevention Systems and Techniques." [Online]. Available: https://www.amu.apus.edu/area of study/information technology/resources/intrusion detection and prevention systems and techniques/

[2] S. A. Khan et al., "Machine learning based network intrusion detection for big and cloud data," J. Big Data, vol. 11, 2024. [Online]. Available: https://journalofbigdata.springeropen.com/articles/10.1186/s40537 024 00886 w

[3] Rapid7, "Intrusion Detection and Prevention System (IDPS)," 2024. [Online]. Available: https://www.rapid7.com/fundamentals/intrusion detection and prevention systems idps/

[4] Number Analytics, "Advanced Wireless Intrusion Prevention Techniques," 2024. [Online]. Available: https://www.numberanalytics.com/blog/advanced wireless intrusion prevention techniques

[5] GeeksforGeeks, "Intrusion Detection System Using Machine Learning Algorithms," 2023. [Online]. Available: https://www.geeksforgeeks.org/machine learning/intrusion detection system using machine learning algorithms/

[6] MDPI Electronics Journal, "Application of Artificial Intelligence in Wireless Communications," Special Issue. [Online]. Available: https://www.mdpi.com/journal/electronics/special_issues/UYR45D5PRN

[7] N. Aslam et al., "Explainable AI based innovative hybrid ensemble model for intrusion detection," J. Cloud Comput., vol. 13, no. 1, 2024. [Online]. Available: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677 024 00712 x

[8] Insights2TechInfo, "AI Based Intrusion Detection Systems," 2023. [Online]. Available: https://insights2techinfo.com/ai based intrusion detection systems/

[9] Palo Alto Networks, "What Is the Role of AI in Threat Detection?" Cyberpedia, 2023. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/ai in threat detection

[10] TrueHomeProtection, "Leveraging AI and Machine Learning for Advanced Intrusion Detection," 2023. [Online]. Available: https://www.truehomeprotection.com/leveraging ai and machine learning for advanced intrusion detection in commercial security systems/

[11] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Intrusion Detection Systems Based on Machine Learning Algorithms," in Proc. IEEE, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9495897/

[12] M. A. Talib et al., "AI enabled intrusion detection systems in IoT networks," Int. J. Sci. Res. Arch., vol. 3, no. 2, pp. 76–88, 2023. [Online]. Available: https://ijsra.net/sites/default/files/IJSRA 2023 0316.pdf

[13] 5G Americas, "Advances in Trust and Security in Wireless Cellular Networks," White Paper, 2025. [Online]. Available: https://www.5gamericas.org/wp content/uploads/2025/01/Advances in Trust and Security AI.pdf

[14] M. Ahmad et al., "Evaluating machine learning based intrusion detection systems with explainable AI techniques," Front. Comput. Sci., vol. 6, 2025. [Online]. Available: https://www.frontiersin.org/journals/computer science/articles/10.3389/fcomp.2025.1520741/full

[15] A. O. Adeyemi et al., "Intrusion detection systems for wireless sensor networks using deep learning," Cybersecurity, vol. 6, 2023. [Online]. Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400 023 00161 0

[16] A. K. Sharma and B. R. Khare, "A Comparative Study on AI IDS Artificial Intelligence Based Intrusion Detection System," Int. J. Eng. Res. Technol., vol. 11, no. 6, 2022. [Online]. Available: https://www.ijert.org/a comparative study on ai ids artificial intelligence based intrusion detection system

[17] Clearnetwork, "Top 10 Intrusion Detection and Prevention Systems," 2023. [Online]. Available: https://www.clearnetwork.com/top intrusion detection and prevention systems/

[18] Palo Alto Networks, "What Are the Barriers to AI Adoption in Cybersecurity?" Cyberpedia, 2023. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what are barriers to ai adoption in cybersecurity

[19] Quora, "What Are the Limitations of AI in Cybersecurity?" [Online]. Available: https://www.quora.com/What are the limitations of AI in cybersecurity

[20] Number Analytics, "Advanced Wireless Intrusion Detection Techniques," 2023. [Online]. Available: https://www.numberanalytics.com/blog/advanced wireless intrusion detection techniques

[21] Palo Alto Networks, "What Are the Steps to Successful AI Adoption in Cybersecurity?" Cyberpedia, 2023. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/steps to successful ai adoption in cybersecurity