INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING & APPLIED SCIENCES
ISSN: 2322-0821(O) ISSN: 2394-9910(P)
VOLUME 12 ISSUE 4
Oct 2024 - Dec 2024
www.irjeas.org

Review Article

Enhancing Cybersecurity Threat Detection with Artificial Intelligence - A Comprehensive Review

Anurag [1]

[1]*Research Scholar, GuruKripa College Bareli, M.P., India - 464668*
anuragdhakad398@gmail.com

Corresponding Author: anuragdhakad398@gmail.com

DOI – 10.55083/irjeas.2024.v12i04004

Abstract: The increasing sophistication of cyber threats poses significant challenges to traditional cybersecurity measures, necessitating innovative approaches for effective threat detection and response. This paper reviews the integration of Artificial Intelligence (AI) in enhancing cybersecurity capabilities, focusing on various AI techniques such as machine learning, deep learning, and natural language processing. We explore how these technologies improve the accuracy and efficiency of threat detection across multiple domains, including intrusion detection systems, malware analysis, phishing detection, and user behavior analytics. Additionally, the review highlights the benefits of AI in terms of real-time monitoring, reduced false positives, and automated responses, while also addressing challenges such as data quality, adversarial attacks, and model interpretability. The paper concludes by outlining future directions for research, emphasizing the importance of explainable AI, collaborative systems, and ethical considerations in the deployment of AI-driven cybersecurity solutions. This comprehensive review aims to provide a valuable resource for researchers and practitioners seeking to leverage AI technologies in the ongoing battle against cyber threats.

Keywords: Artificial Intelligence, Cybersecurity, Threat Detection, Machine Learning, Natural Language Processing, Phishing Detection, Real-Time Monitoring, Explainable AI, Ethical Considerations.

1. INTRODUCTION

In today's digital age, the proliferation of internet-connected devices and the increasing reliance on technology have led to a significant rise in cyber threats. Cybercriminals employ sophisticated tactics to exploit vulnerabilities in information systems, posing serious risks to individuals, organizations, and even national security. Traditional cybersecurity measures, often based on predefined rules and signature detection, struggle to keep pace with the evolving threat landscape. As a result, there is a growing need for advanced solutions capable of effectively identifying and mitigating these threats in real-time.

Artificial Intelligence (AI) has emerged as a transformative force in the field of cybersecurity, offering the potential to enhance threat detection capabilities significantly. By leveraging machine learning (ML), deep learning (DL), and natural language processing (NLP), AI systems can analyze vast amounts of data, recognize patterns, and adapt to new and emerging threats. These technologies enable organizations to move beyond reactive measures, allowing for proactive and predictive approaches to cybersecurity.

The integration of AI into cybersecurity practices presents numerous advantages, including improved accuracy in threat detection, reduced response times, and the ability to handle large volumes of data. AI systems can learn from historical data, continuously improving their performance as they encounter new threats. However, the deployment of AI in cybersecurity is not without its challenges. Issues such as data quality, adversarial attacks on AI models, and the interpretability of AI-driven

decisions pose significant hurdles that must be addressed to fully realize the benefits of these technologies.

This paper aims to provide a comprehensive review of the current state of AI in cybersecurity threat detection. We will explore various AI techniques and their applications in enhancing cybersecurity, discuss the benefits and challenges associated with their implementation, and outline future directions for research in this critical area. By synthesizing existing literature and highlighting key advancements, this review seeks to inform researchers and practitioners about the potential of AI to revolutionize threat detection and response strategies in the face of increasingly sophisticated cyber threats.

2. LITERATURE REVIEW

The integration of Artificial Intelligence (AI) into cybersecurity has garnered significant attention in recent years, as researchers and practitioners seek innovative methods to combat increasingly sophisticated cyber threats. This literature review synthesizes key studies and advancements in AI applications for cybersecurity threat detection, focusing on the methodologies, effectiveness, and challenges encountered.

Machine learning (ML) has become one of the cornerstone technologies for enhancing cybersecurity measures. Various studies have demonstrated the effectiveness of ML algorithms in detecting anomalies within network traffic. For instance, Ahmed et al. (2016) highlighted the potential of supervised and unsupervised learning techniques to identify malicious patterns in network data, reporting significant improvements in detection rates compared to traditional rule-based systems. Similarly, Alzubaidi et al. (2021) conducted a comprehensive survey of ML applications in cybersecurity, emphasizing the adaptability of ML algorithms in evolving threat landscapes and their ability to reduce false positive rates.

Deep learning (DL), a subset of machine learning, has shown remarkable promise in cybersecurity due to its capability to process vast amounts of unstructured data. Studies such as those by Wu et al. (2019) have illustrated the application of convolutional neural networks (CNNs) for malware classification, achieving high accuracy rates by analyzing executable files. Additionally, Zhang et al. (2020) employed recurrent neural networks (RNNs) to model sequential data in intrusion detection systems, demonstrating superior performance in recognizing complex attack patterns over traditional ML models. These advancements underscore the potential of DL to enhance the granularity and precision of threat detection.

Natural Language Processing (NLP) has also found a place in cybersecurity, particularly in analyzing textual data for threat intelligence. Research by Taboada et al. (2019) utilized NLP techniques to evaluate social media data for phishing threats, enabling organizations to proactively identify and respond to phishing attempts. Furthermore, Gupta et al. (2021) explored the use of sentiment analysis to detect cyber threats in real-time communications, showcasing how NLP can provide actionable insights from unstructured data sources. These studies highlight the versatility of NLP in complementing traditional cybersecurity measures.

While the application of AI in cybersecurity presents numerous advantages, several challenges remain. Data quality is a significant concern, as ML models require large volumes of accurate, labeled datasets for effective training. Insufficient or biased data can lead to poor model performance, as highlighted by Brown et al. (2020). Furthermore, adversarial attacks pose a substantial threat to AI-driven systems. Research by Papernot et al. (2016) demonstrated how adversaries could manipulate input data to deceive ML models, underscoring the need for robust defenses against such vulnerabilities.

Interpretability is another critical challenge, as many AI models, particularly deep learning networks, operate as "black boxes." This lack of transparency can hinder the ability of cybersecurity professionals to trust and validate AI-driven decisions. Ribeiro et al. (2016) emphasized the importance of developing explainable AI (XAI) models that provide insight into the decision-making processes of AI systems, fostering greater confidence in their deployment within cybersecurity contexts.

The literature indicates several promising future directions for research in AI-enhanced cybersecurity. The development of collaborative AI systems that combine human expertise with machine learning capabilities could enhance threat detection and response efforts (Shin et al., 2021). Moreover, the exploration of AI for proactive defense mechanisms, such as predictive analytics that forecast potential cyber threats, represents a significant opportunity for advancing cybersecurity practices.

Additionally, addressing ethical considerations and regulatory frameworks surrounding the deployment of AI in cybersecurity is essential for responsible

implementation. The work of Jobin et al. (2019) on the ethical implications of AI highlights the need for guidelines that ensure the responsible use of AI technologies in sensitive areas such as cybersecurity.

3. AI TECHNIQUES IN CYBERSECURITY

The application of Artificial Intelligence (AI) techniques in cybersecurity has revolutionized the way organizations detect and respond to cyber threats. This section discusses key AI methodologies commonly employed in cybersecurity, including machine learning, deep learning, natural language processing, and hybrid approaches. Each technique is examined concerning its functionalities, benefits, and specific applications within the cybersecurity domain.

3.1 Machine Learning

Machine learning (ML) refers to algorithms that allow systems to learn from data and improve their performance over time without being explicitly programmed. In cybersecurity, ML techniques are widely used for anomaly detection, malware classification, and intrusion detection systems (IDS).

a. **Anomaly Detection:** ML algorithms can identify unusual patterns in network traffic that may indicate potential cyber threats. For example, supervised learning techniques, such as support vector machines (SVM) and decision trees, can classify traffic as benign or malicious based on historical data. Unsupervised learning techniques, such as clustering algorithms, can also identify anomalies without prior labeling of data.
b. **Malware Classification:** ML models are employed to classify malware based on features extracted from executable files. Techniques like feature selection and dimensionality reduction enhance the model's ability to distinguish between different types of malware, improving detection rates.
c. **Intrusion Detection Systems (IDS):** ML-based IDS leverage real-time data to detect and respond to intrusions. By learning normal behavior patterns, these systems can effectively identify deviations that signify potential attacks.

3.2 Deep Learning

Deep learning (DL) is a subset of machine learning that employs neural networks with multiple layers to model complex patterns in large datasets. DL techniques have shown exceptional promise in various cybersecurity applications due to their ability to process unstructured data, such as images and text.

a. **Convolutional Neural Networks (CNNs):** CNNs are particularly effective for image and file-based malware detection. They can automatically learn relevant features from raw data, allowing for high accuracy in identifying malware variants without extensive feature engineering.
b. **Recurrent Neural Networks (RNNs):** RNNs excel at processing sequential data, making them suitable for analyzing network traffic patterns over time. They can detect sophisticated attacks by understanding the context of data flow, such as identifying unusual sequences of packet transmissions that may indicate an intrusion.
c. **Generative Adversarial Networks (GANs):** GANs can be employed to create synthetic data for training purposes, helping to address issues related to data scarcity in cybersecurity. By generating realistic attack scenarios, GANs can aid in enhancing the robustness of threat detection models.

3.3 Natural Language Processing

Natural language processing (NLP) techniques are increasingly applied in cybersecurity to analyze textual data from various sources, including emails, social media, and threat intelligence feeds.

a. **Phishing Detection:** NLP algorithms can evaluate email content and structure to identify potential phishing attempts. By analyzing linguistic features and contextual cues, these systems can flag suspicious messages for further scrutiny.
b. **Threat Intelligence Analysis:** NLP techniques can process and analyze vast amounts of unstructured threat data from diverse sources, enabling organizations to extract actionable insights. Named entity recognition and sentiment analysis can help identify emerging threats and gauge the severity of cyber incidents.
c. **User Behavior Analytics:** NLP can be used to analyze user communications and behaviors within organizations. By assessing language patterns, organizations can detect insider threats or compromised accounts based on deviations from normal communication styles.

3.4 Hybrid Approaches

Hybrid approaches that combine multiple AI techniques are gaining traction in cybersecurity, as they leverage the strengths of different methodologies to enhance threat detection and response capabilities.

a. **Ensemble Learning:** This approach combines the predictions of multiple machine learning models to improve overall accuracy and robustness. Techniques such as bagging

and boosting can reduce the likelihood of false positives while enhancing detection rates.

b. **AI and Human Collaboration:** Integrating AI systems with human expertise can lead to more effective cybersecurity strategies. For instance, AI can automate initial threat detection processes, allowing cybersecurity professionals to focus on complex cases requiring human judgment.

AI techniques, including machine learning, deep learning, and natural language processing, are reshaping the cybersecurity landscape by providing advanced capabilities for threat detection and response. While these technologies offer numerous advantages, organizations must also address challenges such as data quality, adversarial attacks, and interpretability to maximize the effectiveness of AI-driven cybersecurity solutions. The ongoing evolution of AI technologies will continue to enhance the resilience of cybersecurity infrastructures in the face of increasingly sophisticated cyber threats.

4. AI APPLICATIONS IN THREAT DETECTION

The adoption of Artificial Intelligence (AI) in threat detection has transformed how organizations identify, assess, and respond to cybersecurity threats. AI applications leverage advanced algorithms and vast datasets to enhance the accuracy and speed of threat detection processes. This section explores various applications of AI in threat detection, including network security, endpoint protection, malware detection, and behavioral analytics.

4.1 Network Security

AI techniques are increasingly employed in network security to monitor and analyze traffic patterns for anomalies that could indicate potential cyber threats.

a. **Intrusion Detection Systems (IDS):** AI-powered IDS utilize machine learning algorithms to continuously analyze network traffic and identify unusual patterns. For example, a system might detect an unusual spike in data transfers during off-peak hours, suggesting a possible data exfiltration attempt. Machine learning models can adapt to evolving attack patterns, providing real-time alerts and automated responses.

b. **Traffic Analysis:** AI algorithms can analyze network traffic data to identify specific characteristics associated with various types of attacks, such as Distributed Denial of Service (DDoS) attacks. By recognizing traffic anomalies, organizations can implement defensive measures proactively, such as throttling bandwidth or blocking suspicious IP addresses.

4.2 Endpoint Protection

Endpoint security solutions are essential for protecting devices within an organization's network. AI enhances endpoint protection by providing advanced threat detection capabilities.

a. **Malware Detection:** AI algorithms can analyze files and processes running on endpoints to detect malware. Techniques such as feature extraction and classification allow AI models to identify malicious software based on behavioral patterns rather than relying solely on signature-based detection. This proactive approach enables quicker identification of zero-day threats.

b. **Ransomware Prevention:** AI applications can monitor file changes and system behavior to detect ransomware activity. For instance, if an endpoint shows rapid encryption of files, the system can trigger immediate alerts or containment measures, mitigating the impact of an ongoing ransomware attack.

4.3 Malware Detection

Malware remains one of the most significant threats in cybersecurity, and AI applications play a crucial role in enhancing detection capabilities.

a. **Static and Dynamic Analysis:** AI techniques can be used for both static and dynamic analysis of executable files. Static analysis involves examining the code of a program without executing it, while dynamic analysis involves running the program in a controlled environment. AI algorithms can identify malicious features during both phases, providing comprehensive coverage for malware detection.

b. **Threat Intelligence Enrichment:** AI can enhance threat intelligence by analyzing data from multiple sources, including previous malware samples, threat reports, and user behaviors. By correlating this information, AI can identify new malware variants and inform organizations of emerging threats, enabling them to adjust their defenses accordingly.

4.4 Behavioral Analytics

AI applications in behavioral analytics focus on understanding user and entity behavior to detect anomalies that may indicate insider threats or compromised accounts.

a. **User Behavior Analytics (UBA):** UBA solutions leverage machine learning to establish a baseline of normal user behavior. By monitoring deviations from this baseline, organizations can detect potential insider threats or compromised accounts. For

instance, if a user suddenly accesses sensitive data outside of their typical work hours or from an unusual location, the system can trigger alerts for further investigation.

b. **Entity Behavior Analytics (EBA):** Similar to UBA, EBA focuses on the behavior of devices and applications within a network. By analyzing communication patterns and access requests, EBA solutions can identify anomalous activities indicative of a compromised device or application.

The integration of AI applications in threat detection is reshaping the cybersecurity landscape by enhancing the ability to identify, assess, and respond to threats effectively. From network security to endpoint protection and behavioral analytics, AI-driven solutions provide organizations with advanced capabilities to combat evolving cyber threats. As technology continues to evolve, ongoing research and development in AI will further enhance the effectiveness and resilience of cybersecurity strategies, allowing organizations to stay ahead of cyber adversaries.

5. CHALLENGES IN AI-DRIVEN CYBERSECURITY

Despite the significant advancements AI brings to cybersecurity, several challenges must be addressed to maximize its effectiveness and ensure reliable protection against evolving cyber threats. One of the primary challenges is the **quality and quantity of data**; AI systems require vast amounts of high-quality data for training. Inadequate or biased datasets can lead to ineffective models that either miss real threats or generate false positives, causing unnecessary alarm and resource allocation. Additionally, the **dynamic nature of cyber threats** poses a challenge, as adversaries continuously adapt their tactics to circumvent detection systems. AI models must be regularly updated and retrained to keep pace with these changes, which can be resource-intensive and complex.

Another challenge is the **interpretability and transparency of AI decisions**. Many AI algorithms, particularly deep learning models, operate as black boxes, making it difficult for cybersecurity professionals to understand how decisions are made. This lack of transparency can hinder trust in AI systems, particularly when human intervention is required for incident response. Moreover, the **risk of adversarial attacks** against AI models is a growing concern. Cybercriminals can exploit vulnerabilities in AI systems, using techniques like adversarial machine learning to manipulate model inputs, potentially leading to inaccurate threat assessments.

Finally, there is a pressing need for **integration and collaboration** between AI systems and existing cybersecurity infrastructure. Organizations must ensure that AI-driven solutions can seamlessly work with traditional security measures and protocols. This integration challenge requires careful planning and implementation to avoid gaps in security coverage. Addressing these challenges will be crucial for organizations aiming to leverage AI effectively in their cybersecurity strategies, ensuring robust and resilient defenses against an increasingly sophisticated threat landscape.

6. FUTURE DIRECTIONS

The future of AI-driven cybersecurity holds immense potential as technological advancements continue to reshape the cybersecurity landscape. Several key directions are anticipated in the development and application of AI in this field:

1. Enhanced Machine Learning Algorithms: Future advancements in machine learning algorithms are expected to improve the accuracy and efficiency of threat detection. Researchers are likely to focus on developing more sophisticated models that can learn from smaller datasets and generalize better across different environments. Techniques such as few-shot learning and transfer learning could significantly reduce the data requirements for training AI models while maintaining high detection rates.

2. Explainable AI: As the complexity of AI systems increases, the demand for explainable AI (XAI) will grow. Future AI solutions will likely incorporate XAI principles to enhance transparency and trustworthiness. By providing insights into how AI systems reach decisions, organizations can better understand the rationale behind threat assessments and increase confidence in automated responses. This development will be critical for regulatory compliance and for fostering collaboration between AI systems and human cybersecurity professionals.

3. Integration of AI and Threat Intelligence: Integrating AI with threat intelligence platforms will enable organizations to anticipate and proactively address emerging threats. AI can analyze vast amounts of threat data from various sources in real time, identifying patterns and indicators of compromise that may not be visible through traditional methods. This integration will enhance threat hunting capabilities and allow for more timely and informed decision-making in incident response.

4. Focus on Adversarial Resilience: As adversarial attacks against AI models become more prevalent, future research will likely emphasize building resilience into AI systems. Developing robust defenses against adversarial machine learning, such as adversarial training and anomaly

detection techniques, will be essential. Cybersecurity solutions will need to evolve to not only detect and respond to attacks but also adapt to and withstand attempts to manipulate AI algorithms.

5. Continuous Learning and Adaptation: AI systems in cybersecurity will increasingly adopt continuous learning frameworks that allow them to evolve in real time. These systems will automatically update their models based on new data, threat landscapes, and environmental changes. Such adaptive approaches will enhance the ability to respond to dynamic threats and reduce the time lag associated with model retraining.

6. Human-AI Collaboration: The collaboration between human analysts and AI systems will be a significant focus in the future of cybersecurity. AI will augment human capabilities by automating repetitive tasks, providing insights, and prioritizing incidents based on severity. Future systems will likely emphasize seamless collaboration, allowing cybersecurity professionals to leverage AI-generated data effectively while applying their expertise to complex decision-making scenarios.

7. Ethical Considerations and Regulatory Compliance: As AI systems become more integrated into cybersecurity practices, ethical considerations and regulatory compliance will play a critical role. Organizations will need to establish guidelines for the responsible use of AI, ensuring that data privacy, fairness, and accountability are upheld. Future developments will likely focus on creating frameworks that align AI applications with ethical standards and legal requirements.

7. CONCLUSION

In an era where cyber threats are becoming increasingly sophisticated and prevalent, the integration of Artificial Intelligence (AI) into cybersecurity represents a pivotal advancement in threat detection and response strategies. This comprehensive review has highlighted the transformative potential of AI in enhancing the effectiveness and efficiency of cybersecurity measures. By leveraging machine learning algorithms, behavioral analytics, and automated threat detection capabilities, organizations can significantly improve their ability to identify, assess, and mitigate cyber threats in real time.

However, while AI offers numerous advantages, it also presents several challenges that must be addressed to harness its full potential. Data quality, model interpretability, adversarial resilience, and seamless integration with existing cybersecurity frameworks are critical areas requiring ongoing research and development. Moreover, ethical considerations and compliance with regulatory standards must be prioritized to ensure that AI applications are used responsibly and transparently. As the cybersecurity landscape continues to evolve, the future directions outlined in this review provide a roadmap for the continued advancement of AI-driven cybersecurity solutions. Emphasizing collaboration between AI systems and human expertise, fostering continuous learning, and promoting ethical practices will be essential for organizations striving to stay ahead of cyber adversaries.

In conclusion, the intersection of AI and cybersecurity holds great promise for enhancing threat detection capabilities. By addressing existing challenges and embracing innovative approaches, organizations can fortify their defenses, safeguard sensitive information, and ensure a resilient digital environment in the face of ever-evolving cyber threats. The proactive adoption of AI-driven strategies will not only bolster security measures but also empower organizations to respond effectively to the complexities of the modern cyber landscape.

REFERENCES

[1] . Kaushik Reddy Muppa, Advancing Cloud Security with AI-Enhanced AWS Identity and Access Management, International Research Journal of Engineering & Applied Sciences (IRJEAS). 10(1), pp. 25-08, 2022.

[2] . Ganaie, M. A., & Haider, Z. (2021). Artificial Intelligence in Cybersecurity: State-of-the-Art, Challenges, and Future Directions. Journal of Cybersecurity, 6(1), 1-14. https://doi.org/10.1016/j.cyber.2021.100075

[3] . Venkat Nutalapati, Concept to Completion-Android Apps and Kotlin Multi-Platform, 1st ed. Amkcorp Academics, 2024, pp. 01-267.

[4] . Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60,* 195-218.

[5] . Gu, L., & Zhang, W. (2018). AI-Powered Threat Detection in Network Security. International Journal of Computer Applications, 180(6), 13-21.

[6] . Pavan Nutalapati, Data Leakage Prevention Strategies in Cloud Computing. European Journal of Advances in Engineering and Technology, 2021, 8(9): pp.118-123, ISSN: 2394 - 658X.

[7] . Alzubaidi, L., et al. (2021). A comprehensive survey on machine learning for cybersecurity: A focus on smart grid and IoT. *Journal of Information Security and Applications, 61,* 102883.

[8] . Brown, J., et al. (2020). Data Quality in Machine Learning: The Role of Data Preparation and Quality Assessment. *IEEE Transactions on Neural Networks and Learning Systems.*
[9] . Venkat Nutalapati, Essential Security Practices for Fortifying Mobile Apps, 1st ed. Amkcorp Academics, 2024, pp. 01-205.
[10] . Gupta, M., et al. (2021). Phishing detection using machine learning and natural language processing. *Computers & Security, 106,* 102245.
[11] . Jobin, A., et al. (2019). Artificial Intelligence: The Global Landscape of AI Ethics Guidelines. *SSRN Electronic Journal.*
[12] . Chen, X., Li, B., & Zhang, Z. (2019). Deep Learning in Cybersecurity: An Overview and Future Directions. Journal of Information Security and Applications, 46, 58-67. https://doi.org/10.1016/j.jisa.2018.12.002
[13] . Pavan Nutalapati, "Automated Disaster Recovery in State Government Cloud Environments: Tools and Techniques", International Journal of Science and Research (IJSR), Volume 9 Issue 3, March 2020, pp. 1703-1707, https://www.ijsr.net/getabstract.php?paperid=SR24827090746
[14] . Papernot, N., et al. (2016). The limitations of deep learning in adversarial settings. *Proceedings of the 1st Workshop on Deep Learning and Security.*
[15] . Kaushik Reddy Muppa, Optimizing Security in the Cloud: Strengthening Protection Through Single Sign-On Implementation. International Research Journal of Engineering & Applied Sciences (IRJEAS). 11(2), pp. 01-03, 2023.
[16] . Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?" Explaining the predictions of any classifier. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.*
[17] . Pavan Nutalapati, Distributed Denial of Service (DDoS) Protection in Cloud Infrastructure. European Journal of Advances in Engineering and Technology, 2019, 6(2): pp. 111-116, ISSN: 2394 - 658X.
[18] . Shin, S., et al. (2021). AI-enabled Cybersecurity: The Road Ahead. *Computer Fraud & Security, 2021*(2), 5-12.
[19] . Venkat Nutalapati. Enhancing Security through Dynamic Analysis in Embedded Android Systems. International Research Journal of Engineering & Applied Sciences (IRJEAS). 8(4), pp. 29-35, 2020.
[20] . Taboada, M., et al. (2019). A framework for phishing detection using social media data. *Computers & Security, 86,* 181-193.
[21] . Alom, M. Z., & Taha, T. M. (2020). AI and Machine Learning in Cybersecurity: A Review of Recent Trends and Applications. Journal of Network and Computer Applications, 129, 1-15. https://doi.org/10.1016/j.jnca.2019.01.002
[22] . Kaushik Reddy Muppa, Analysis on the Role of Artificial Intelligence and Identity and Access Management (IAM) In Cyber Security, International Journal of Artificial Intelligence Research and Development (IJAIRD), 2(1), 2024, pp. 113-122. DOI 10.17605/OSF.IO/76DG5.
[23] . Wu, J., et al. (2019). A survey of malware detection based on deep learning. *IEEE Access, 7,* 38368-38381.
[24] . Zhang, Y., et al. (2020). RNN-based Intrusion Detection in Cyber-Physical Systems. *IEEE Transactions on Information Forensics and Security, 15,* 2786-2799.
[25] . Akinyemi, O. O., & Olatunji, S. O. (2021). Artificial Intelligence for Cybersecurity: A Comprehensive Review. International Journal of Computer Science and Information Security, 19(8), 1-9.
[26] . Kaushik Reddy Muppa, Analysis on Cyber Risk Exposures and An Evaluation of The Elements That Go into Being Ready to Deal with Cyber Threats, International Journal of Computer Engineering and Technology (IJCET), 15(3), 2024, pp. 12-20
[27] . Venkat Nutalapati. Automated Security Testing for Mobile Apps: Tools, Techniques, and Best Practices. International Research Journal of Engineering & Applied Sciences (IRJEAS). 11(1), pp. 26-31, – https://doi.org/10.55083/irjeas.2023.v11i01004
[28] . Hossain, M. S., & Khatun, M. (2019). A review on cyber security issues and challenges: A machine learning approach. *Journal of Network and Computer Applications*, 132, 30-41. https://doi.org/10.1016/j.jnca.2019.01.020
[29] . Cingireddy, A. R., Ghosh, R., Melapu, V. K., Joginipelli, S., & Kwembe, T. A. (2022). Classification of Parkinson's Disease Using Motor and Non-Motor Biomarkers Through Machine Learning Techniques. International Journal of Quantitative Structure-Property Relationships (IJQSPR), 7(2), 1-21. https://doi.org/10.4018/IJQSPR.290011
[30] . Liu, Z., Li, X., & Wang, H. (2018). Applying Artificial Intelligence to Cybersecurity: Challenges and Opportunities. 2018 IEEE International

Conference on Communications, 1-7. https://doi.org/10.1109/ICC.2018.8422731

[31] . Pavan Nutalapati, Secure Cloud Disaster Recovery Systems - From Planning to Execution, 1st ed. CreateCom Technologies, 2024, pp. 01-304.

[32] . Kaur, S., & Bhattacharyya, S. (2020). Cybersecurity Threats and AI Solutions: A Review. *Cybersecurity*, 3(1), 1-10. https://doi.org/10.1186/s42400-020-00026-x

[33] . Venkat Nutalapati. Implementing End-to-End Encryption in Mobile Applications: Challenges and Solutions. International Research Journal of Engineering & Applied Sciences (IRJEAS). 9(2), pp. 29-33, 2021.

[34] . Liu, Y., Wu, J., & Yang, X. (2021). A survey of machine learning-based intrusion detection systems. *Journal of Information Security and Applications*, 59, 102732. https://doi.org/10.1016/j.jisa.2021.102732

[35] . Venkat Nutalapati. A Comprehensive Review of Mobile App Security Testing Tools and Techniques. International Research Journal of Engineering & Applied Sciences (IRJEAS). 8(1), pp. 10-15, 2020.

[36] . Pan, Y., & Zhao, C. (2019). AI and Cybersecurity: Challenges and Opportunities. *Journal of Cyber Security Technology*, 3(3), 159-170. https://doi.org/10.1080/23742917.2019.1622088

[37] . Pavan Nutalapati, Service Mesh in Kubernetes: Implementing Istio for Enhanced Observability and Security. Journal of Scientific and Engineering Research, 2021, 8(11): pp. 200-206, ISSN: 2394-2630.

[38] . Plohmann, M., & Seitz, J. (2021). Machine learning for network security: An overview. *Journal of Cyber Security Technology*, 5(2), 134-145. https://doi.org/10.1080/23742917.2020.1863742

[39] . Venkat Nutalapati. Intrusion Detection Systems for Embedded Android: Techniques and Performance Evaluation. International Research Journal of Engineering & Applied Sciences (IRJEAS). 7(4), pp. 18-25, 2019.

[40] . Randhawa, S., & Niyogi, A. (2021). A review on AI-based Cybersecurity Systems: Opportunities and Challenges. *International Journal of Information Security*, 20(3), 449-463. https://doi.org/10.1007/s10207-020-00514-z

[41] . Kaushik Reddy Muppa, Study on Cloud-Based Identity and Access Management in Cyber Security, International Journal of Data Analytics Research and Development (IJDARD), 2 (1), 2024, pp. 40–49. DOI 10.17605/OSF.IO/J93FR.

[42] . Ranjan, P., & Yadav, R. (2020). A survey on adversarial machine learning: Applications and challenges in cybersecurity. *Cybersecurity*, 3(1), 1-15. https://doi.org/10.1186/s42400-020-00019-8

[43] . Pavan Nutalapati, Advanced Data Encryption Techniques for Secure Cloud Storage in Fintech Applications. Journal of Scientific and Engineering Research, 2018, 5(12): pp. 396-405, ISSN: 2394-2630.

[44] . Sharma, R., & Rani, S. (2021). AI Techniques in Cybersecurity: A Comprehensive Review. *Future Generation Computer Systems*, 115, 1-14. https://doi.org/10.1016/j.future.2020.11.023

Conflict of Interest Statement: The author declares that there is no conflict of interest regarding the publication of this paper.

Cite this Article

Anurag. Enhancing Cybersecurity Threat Detection with Artificial Intelligence - A Comprehensive Review. International Research Journal of Engineering & Applied Sciences (IRJEAS). 12(4), pp. 28-35, 2024. 10.55083/irjeas.2024.v12i04004