Validating Your Resources

Ryan Coon

UNV-507

Professor Tina Salata

July 10, 2024

|  |  |  |  |
| --- | --- | --- | --- |
| **Summary** | **Explanation of Scholarly Resources** | **Application to Research** | **APA Citations** |
| This article discusses an AI-driven cybersecurity system designed to detect and prevent network intrusions. It was presented at the 2024 IEEE International Conference on Computing, Power, and Communication Technologies. The system leverages artificial intelligence to enhance security measures against cyber threats, particularly in the context of network intrusion detection. | This article has multiple authors within the cyber security field. The article was also found from within the GCU Library. | Snippets of this article can be used to show how AI can be used to help prevent network intrusions. AI can take the place of having people monitor 24/7 without skipping a beat. | Anu Disney, D., Yugha, R., Karachi, S. B., Gangadevi, E., Balusamy, B., & Gite, S. (2024). An AI-Driven Based Cybersecurity System for Network Intrusion Detection System in Hybrid with EPO and CNNet-LAM. *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Computing, Power and Communication Technologies (IC2PCT), 2024 IEEE International Conference On*, *5*, 1397–1404. https://doi-org.lopes.idm.oclc.org/10.1109/IC2PCT60090.2024.10486517 |
| This article delves into the evolving role of Generative AI and Large Language Models in cybersecurity. The motivation behind this research is the rapid advancement of GenAI technologies and their potential implications for cybersecurity professionals. This work focuses on assessing how GenAI and LLMs influence cybersecurity practices, including both the opportunities and risks they present. | This article has multiple authors within the cyber security field. The article was also found from within the GCU Library. | This can be used to show pros and cons for introducing AI into Cybersecurity and how it helps. | Capodieci, N., Sanchez-Adames, C., Harris, J., & Tatar, U. (2024). The Impact of Generative AI and LLMs on the Cybersecurity Profession. *2024 Systems and Information Engineering Design Symposium (SIEDS), Systems and Information Engineering Design Symposium (SIEDS), 2024*, 448–453. https://doi-org.lopes.idm.oclc.org/10.1109/SIEDS61124.2024.10534674 |
| This article discusses AI-Based Cybersecurity Policies and Procedures.  It also provides guidelines to implement solutions to protect assets and safeguard the technology used. | This article has multiple authors within the cyber security field. The article was also found from within the GCU Library. | This can show the ever evolving practices and policy changes that allow AI to be slowly introduced into Cybersecurity. | Jawhar, S., Miller, J., & Bitar, Z. (2024). AI-Based Cybersecurity Policies and Procedures. *2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC), AI in Cybersecurity (ICAIC), 2024 IEEE 3rd International Conference On*, 1–5. https://doi-org.lopes.idm.oclc.org/10.1109/ICAIC60265.2024.10433845 |
| This article discusses the use of AI in the detection of complex attacks by hackers taking advantage of the Network Intrusion Detection System algorithms. This study offers a sophisticated method in using AI for supporting the Network Intrusion Detection System. | This article has multiple authors within the cyber security field. The article was also found from within the GCU Library. |  | Kumar, P. M., Vedantham, K., Selvaraj, J., & Kavin, B. P. (2024). Enhanced Network Intrusion Detection System Using PCGSO-Optimized BI-GRU Model in AI-Driven Cybersecurity. *2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC), AI in Cybersecurity (ICAIC), 2024 IEEE 3rd International Conference On*, 1–6. https://doi-org.lopes.idm.oclc.org/10.1109/ICAIC60265.2024.10443675 |
| This article provides insight for the state of the art of AI's potential to enhance cyber defense strategies in the field of cybersecurity. In addition, it highlights a variety of AI-based cybersecurity strategies that include anomaly detection, behavior analysis, and predictive modeling. Additionally, it explores the drawbacks and limitations of AI in cybersecurity, including data privacy issues and adversarial attacks, and offers suggestions for how to resolve these problems. | This article has multiple authors within the cyber security field. The article was also found from within the GCU Library. |  | M.Nour, S., & A.Said, S. (2024). Harnessing the Power of AI for Effective Cybersecurity Defense. *2024 6th International Conference on Computing and Informatics (ICCI), Computing and Informatics (ICCI), 2024 6th International Conference On*, 98–102. https://doi-org.lopes.idm.oclc.org/10.1109/ICCI61671.2024.10485059 |
| This paper explains how AI is revolutionizing cybersecurity techniques, contributing to a more secure and greater secure digital future. | This article has multiple authors within the cyber security field. The article was also found from withing the GCU Library. | This article can be used by explaining some of the techniques AI uses in Cybersecurity and how effective they are. | Mahfuri, M., Ghwanmeh, S., Almajed, R., Alhasan, W., Salahat, M., Lee, J. H., & Ghazal, T. M. (2024). Transforming Cybersecurity in the Digital Era: The Power of AI. *2024 2nd International Conference on Cyber Resilience (ICCR), Cyber Resilience (ICCR), 2024 2nd International Conference On*, 1–8. https://doi-org.lopes.idm.oclc.org/10.1109/ICCR61006.2024.10533072 |
| This paper is a study conducted by North Carolina A&T across two semesters in which the students engage in learning AI in the detection of cyberharrassment. I goes over the systems and the overall outcome of the study. What areas worked and what areas need work. | This paper is completed as a study at North Carolina A&T University. The study was also found from within the GCU Library. | This study can be used to note how effective/ineffective AI detection can be and how it can help in Cybersecurity. | Okpala, E., Vishwamitra, N., Guo, K., Liao, S., Cheng, L., Hu, H., Wu, Y., Yuan, X., Wade, J., & Khorsandroo, S. (2024). *AI-Cybersecurity Education Through Designing AI-based Cyberharassment Detection Lab*. |
| The article discusses an analytical approach towards cybersecurity using AI-enabled technologies. The focus is on enhancing cybersecurity through the application of artificial intelligence. Another aspect covered in the article is the prediction of total harmonics distortion at the point of common coupling. | This article has multiple authors within the cyber security field. The article was also found from within the GCU Library. | This can be used to discuss how AI can enhance Cybersecurity through the application of Artificial Intelligence. | Singh, A., Kanishka, & Dubey, S. K. (2024). Analytical Approach Towards Cybersecurity Through AI-Enabled Threat Intelligence. *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2024 11th International Conference On*, 1–6. https://doi-org.lopes.idm.oclc.org/10.1109/ICRITO61523.2024.10522422 |
| This article talks about cybersecurity vulnerabilities inherent to Artificial Intelligence(AI) and Machine Learning(ML) implementations within critical infrastructure domains of supply chain management and project management to explore how these weaknesses may be exploited. Further, they discuss ways AI and ML can be exploited by cybersecurity vulnerabilities within industry to compromise data and resources. | This article has multiple authors within the cyber security field. The article was also found from within the GCU Library. | I can use this article to highlight the vulnerabilities when using AI in Cybersecurity systems. Can also discuss how they can be exploited. | Squillace, J., Cappella, J., & Sepp, A. (2024). User Vulnerabilities in AI-Driven Systems: Current Cybersecurity Threat Dynamics and Malicious Exploits in Supply Chain Management and Project Management. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), 2024 ASU International Conference In*, 1760–1765. https://doi-org.lopes.idm.oclc.org/10.1109/ICETSIS61505.2024.10459480 |
| The article discusses AI-powered predictive cybersecurity for identifying emerging threats through machine learning. The focus is on utilizing artificial intelligence to enhance cybersecurity by predicting and identifying potential threats. The research emphasizes the use of machine learning in cybersecurity to proactively address emerging security challenges. | This article has multiple authors within the cyber security field. The article was also found from within the GCU Library. | This can be used to discuss the AI-predictive Cybersecurity systems used in detecting threats. | Wang, R. (2024). AI-Powered Predictive Cybersecurity in Identifying Emerging Threats through Machine Learning. *2024 IEEE 3rd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), Electrical Engineering, Big Data and Algorithms (EEBDA), 2024 IEEE 3rd International Conference On*, 819–825. https://doi-org.lopes.idm.oclc.org/10.1109/EEBDA60612.2024.10485789 |