Vimal Venkat.

Mrs. Penney.

ISM

20 October 2023

Annotated Bibliography

“Using Artificial Intelligence in Cybersecurity.” Balbix, 18 Dec. 2018. Web. 15 Oct. 2023

This article focuses on the growing role of Artificial Intelligence (AI) in enhancing cybersecurity. It emphasizes the increasing complexity of analyzing time-varying signals to accurately calculate cybersecurity risk, which has become a challenge beyond human-scale capabilities. The primary purpose is to inform a broad audience about the significance of AI and machine learning in improving cybersecurity posture. It outlines the iterative and dynamic nature of AI systems, distinguishing AI from data analytics. The article covers various aspects of AI, machine learning, expert systems, neural networks, and deep learning. The article remains relevant due to AI's enduring importance in cybersecurity. It lacks additional features but provides a foundational understanding of AI's role in addressing cybersecurity challenges. For research on the implications of AI in cybersecurity, this article serves as a valuable resource.

“AI and Cybersecurity: A New Era.” Morgan Stanley, 15 Sep. 2023. Web. 15 Oct. 2023

This article explores the relationship between Artificial Intelligence (AI) and cybersecurity. It begins by defining AI as the simulation of human intelligence in machines, highlighting its potential to outperform humans in various tasks. The article outlines the significant role AI plays

Mrs. Penney.

ISM

20 October 2023

in cybersecurity, from accurately detecting and prioritizing cyber threats to assisting in penetration testing. It also notes the anticipated growth of the AI-based cybersecurity market. However, the article also sheds light on how malicious actors can leverage AI to enhance their attacks. It discusses the use of AI in social engineering, password hacking, deepfakes, and data poisoning, highlighting the challenges these present to cybersecurity. The article concludes by emphasizing the growing concerns around data privacy and the absence of comprehensive AI legislation in the United States. It advises readers to review their cybersecurity measures, especially in areas like password security, data privacy, and social engineering. For research on AI's implications in cybersecurity, this article provides a concise yet informative overview of the subject.

Belani, Gaurav. “The Use of Artificial Intelligence in Cybersecurity: A Review.” IEEE Computer Society. 2022. Web. 17 Oct. 2023

This article explores the growing importance of artificial intelligence (AI) in cybersecurity, highlighting its role in addressing the expanding cyberattack surface in modern enterprises. It emphasizes the advantages of AI, such as its ability to swiftly detect new threats, combat bots, predict breach risks, and enhance endpoint protection. The article also provides insights from cybersecurity executives who believe AI is crucial for responding to cyberattacks and improving the efficiency of cyber analysts. While it underscores the potential benefits, it also acknowledges

downsides, including the resource-intensive nature of AI implementation and the possibility of cybercriminals using AI for malicious purposes. The article primarily aims to inform IT professionals, cybersecurity experts, and decision-makers in the cybersecurity field about the evolving role of AI. However, it lacks information about the author's authority, and its publication date is not provided, making it difficult to assess its currency. Despite these limitations, the article offers valuable insights for research on AI's implications in cybersecurity.

Trovato, Stephanie. “Everything You Need to Know About AI Cybersecurity.” Hubspot. 15 Aug. 2023. Web. 17 Oct 2023.

This article underscores the critical role of Artificial Intelligence (AI) in cybersecurity, particularly in predicting, identifying, and neutralizing potential cyber threats. It emphasizes the exponential growth of data and how AI can be harnessed to manage and analyze this overwhelming volume, making it indispensable for organizations of all sizes and industries. The article outlines the predictive capabilities, real-time response, enhanced accuracy, automated tasks, advanced threat intelligence, scalability, and other advantages that AI brings to cybersecurity. It also provides examples of companies such as Mastercard, BAE Systems, and PayPal successfully using AI for cybersecurity. The content mostly discusses fundamental principles of AI and cybersecurity hold. Therefore, this article, aimed at a general audience interested in technology and cybersecurity trends, serves as a useful introductory resource for a research paper on AI's implications in cybersecurity.

Mrs. Penney.

ISM

20 October 2023

Fowler, Bree. “The Biggest AI Trends in Cybersecurity.” CNET. 22 Sep. 2023. Web. 17 Oct. 2023

This article explores the evolving landscape of artificial intelligence (AI) in the cybersecurity industry. It begins by noting the historical use of AI, or more specifically, machine learning, in threat detection. The article emphasizes the significant shift in the accessibility of AI hacking tools, which can potentially empower less sophisticated cybercriminals to launch AI-powered cyberattacks. The article underlines the need for the cybersecurity industry and government agencies to prepare for this shift. It mentions initiatives such as the Defense Advanced Research Projects Agency's AI Cyber Challenge, involving key players like OpenAI, Google, and Microsoft. The article also discusses the dual nature of AI as both a threat and an opportunity, emphasizing the importance of industry involvement in shaping its future. Written for a general technology-aware audience, this article provides insights into the evolving AI landscape in cybersecurity and its potential implications, making it a valuable resource for research on the consequences of AI in cybersecurity.

Ravichandran, Hari. “How AI Is Disrupting And Transforming The Cybersecurity Landscape.” Forbes. 15 Mar. 2023. Web. 17 Oct. 2023.

Mrs. Penney.

ISM

20 October 2023

This article addresses the growing influence of AI in cybersecurity, discussing its potential benefits and risks. It highlights the increased adoption of AI and machine learning in IT budgets, driven by the need to analyze vast amounts of data and combat cyber threats. The article emphasizes that AI is becoming indispensable for defending against cybercrime. Notably, it points out that business leaders should be aware of the potential dangers and ethical implications of AI in cybersecurity. While discussing the potential use of AI by malicious actors, the article notes that AI-generated code often requires human refinement for complete functionality. It encourages recognizing the positive aspects of AI in cybersecurity, such as automating incident response, continuous monitoring, identifying false positives, strengthening access control, and mitigating insider threats. The article's purpose is to inform business leaders and the general public, and it provides a balanced view of the topic. The content is highly relevant, making it a useful source for research on the implications of AI in cybersecurity.

Pradeesh, Jai. “Artificial Intelligence In Cybersecurity: Unlocking Benefits And Confronting Challenges.” Forbes. 25 Aug. 2023. Web. 17 Oct. 2023.

This article discusses the pivotal role of AI in cybersecurity, focusing on its benefits and associated challenges. It emphasizes the need for innovative solutions to combat evolving cyber threats, highlighting AI's capacity to process vast data from diverse sources for enhanced threat detection. Practical applications, including AI-powered reactive solutions, Security Information

And Event Management (SIEM) systems, threat intelligence platforms, and automated remediation, are explored. The article aims to inform readers about the integration of AI into cybersecurity, catering to professionals, IT specialists, and decision-makers in the field. While the author's qualifications aren't explicitly stated, the content suggests expertise in cybersecurity and AI. For a research paper on AI's implications in cybersecurity, this source offers valuable insights into the advantages and challenges of AI adoption, making it useful for understanding the broader impact of AI in the field.

Prins, Michiel. “How generative AI changes cybersecurity.” InfoWorld. 25 Sep. 2023. Web. 19 Oct. 2023.

The article delves into the impact of Large Language Models (LLMs) and generative artificial intelligence (GenAI) on the field of cybersecurity. It examines the potential benefits and drawbacks of these technologies. The article begins by highlighting the transformative nature of AI in the technology landscape, particularly with the introduction of OpenAI's ChatGPT in 2022. It emphasizes the need for a comprehensive understanding of AI's implications for cybersecurity and the responsible handling of these tools. The article's content is divided into three sections: the "good," the "bad," and the "ugly" aspects of AI in cybersecurity. The "good" section discusses AI and automation tools' positive impact on breach detection and containment. The "bad" section highlights the potential for misuse by inexperienced programmers, leading to

vulnerabilities and incorrect information. The "ugly" section introduces a proof-of-concept malware called BlackMamba, which poses a significant threat to cybersecurity. The target audience likely includes professionals in the cybersecurity field, IT decision-makers, and tech enthusiasts. The article provides valuable insights into AI's implications for cybersecurity, making it a useful resource for research on this topic.

“Artificial Intelligence for Cybersecurity.” BlackBerry. Web. 19 Oct. 2023.

The article introduces AI's role in cybersecurity, emphasizing the need for proactive threat detection due to the expanding attack surface and the limitations of traditional methods. It discusses various AI technologies, the importance of data analysis, and use cases in cybersecurity, including intrusion detection and endpoint security. The article also touches on innovations and the evolving role of AI in mitigating risks. It mentions the influence of AI-powered chatbots in cybersecurity. Guidance on selecting a cybersecurity AI platform is provided, stressing seamless integration, clear benefits, and adaptability to different scenarios. The article offers a useful starting point for understanding AI's significance in cybersecurity, making it valuable for research on the implications of AI in cybersecurity.

“The Role of Artificial Intelligence in Cybersecurity.” Booz | Alen | Hamilton. Web. 19 Oct. 2023.

Mrs. Penney.

ISM

20 October 2023

This article explores the evolving role of artificial intelligence (AI) in cybersecurity. It highlights the historical challenges of manual and time-intensive cybersecurity efforts and discusses how AI can automate key functions, transforming cyber workflows into more efficient and protective processes. The article emphasizes the benefits of AI in cybersecurity, including improved protection, faster incident response, and enhanced workforce satisfaction by reducing manual tasks. The article serves an informational purpose, targeting government and business leaders responsible for cybersecurity. For a research paper on the implications of AI in cybersecurity, this article provides valuable insights into how AI can enhance security, making it a useful resource to understand the benefits and potential applications of AI in the cybersecurity landscape.