Review Form 3

_

Journal Name:	Asian Journal of Research in Computer Science
Manuscript Number:	**Ms_AJRCOS_130459**
Title of the Manuscript:	**A Review of Machine Learning's Roles in Enhancing Cybersecurity**
Type of the Article	

PART 1: Comments

	Reviewer's comment	**Author's Feedback** *(Please correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Please write a few sentences regarding the importance of this manuscript for the scientific community. A minimum of 3-4 sentences may be required for this part.	**This manuscript holds significant importance for the scientific community as it delves into the transformative role of machine learning in advancing cybersecurity. By highlighting the strengths of machine learning over traditional human-operated methods, it underscores its potential to revolutionize threat detection and mitigation. The comprehensive analysis of challenges and practical applications provides valuable insights into bridging the gap between theoretical advancements and real-world implementation. Furthermore, this study serves as a vital resource for researchers and practitioners, guiding future developments in safeguarding critical assets and sensitive information in an increasingly digital world.**	
Is the title of the article suitable? **(If not please suggest an alternative title)**	**No** **Advancing Cybersecurity Through Machine Learning: Bridging Gaps, Overcoming Challenges, and Enhancing Protection**	

Review Form 3

Is the abstract of the article comprehensive? Do you suggest the addition (or deletion) of some points in this section? Please write your suggestions here.	**The abstract provides an overarching view of machine learning's role in cybersecurity but has several shortcomings. Firstly, it lacks clarity and precision in articulating the specific objectives and contributions of the research. While it mentions the "void" in the field and the challenges of comprehending machine learning's role, it does not explicitly outline the research questions or gaps the study addresses. This vagueness might leave readers unsure of the study's unique contributions. Moreover, terms like "void" and "contemporary technology" are too general, making the abstract less impactful. The absence of concrete examples or references to specific machine learning techniques or cybersecurity threats weakens the abstract's ability to connect with the reader's understanding of practical applications.** **Secondly, the abstract does not effectively engage the audience with compelling insights or novel findings. While it emphasizes the relevance of machine learning and its advantages over human-operated detection methods, it does not provide evidence or data to support these claims. Additionally, the abstract mentions fundamental issues affecting real-world applications but does not specify what these issues are. This lack of detail diminishes the abstract's ability to establish a foundation for the research's importance. Furthermore, the keywords are overly broad and lack focus, which may hinder discoverability and fail to capture the essence of the study. Overall, the abstract misses an opportunity to present a concise, targeted, and evidence-driven overview of the research's significance and findings.**	
Is the manuscript scientifically, correct? Please write here.	The manuscript appears scientifically sound in its exploration of machine learning applications in cybersecurity. It demonstrates a well-structured approach, covering theoretical foundations, practical applications, and challenges in the domain. The inclusion of various real-world examples, such as anomaly detection, malware identification, and cloud security, enhances its relevance and practicality. Moreover, the manuscript references diverse and credible sources, indicating a robust literature review that aligns with current advancements in machine learning and cybersecurity. However, the scientific correctness could be improved by clarifying specific methodologies and providing empirical results where applicable. While the manuscript discusses various machine learning techniques and their applications, it lacks quantitative analysis or case studies that could validate the claims made. Additionally, certain sections rely on generalized statements that would benefit from more detailed explanations or examples. Addressing these areas would strengthen the manuscript's contribution to the scientific community.	
Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.	The references in the manuscript are largely sufficient and relevant, covering a wide range of topics in machine learning and cybersecurity. Many of the cited works are recent, with several publications from 2020 to 2023, ensuring the manuscript reflects current advancements in the field. However, there are areas where additional references could enhance the depth and breadth of the discussion. **Suggestions for Additional References:** 1. **Emerging Trends in Machine Learning for Cybersecurity:** o Include more recent studies on adversarial machine learning, which is crucial for understanding and countering evolving cyber threats. For example: ▪ X. Yuan, P. He, Q. Zhu, and X. Li, "Adversarial Examples: Attacks and Defenses for Deep Learning," IEEE Transactions on Neural Networks and Learning Systems, 2019, DOI: 10.1109/TNNLS.2018.2886017. 2. **Integration of AI and IoT in Cybersecurity:** o Expanding the discussion on IoT security could benefit from additional references: ▪ Z. Qin, Q. Xu, J. Wu, and Z. Qin, "How AI and IoT Change the Future of Cybersecurity," IEEE Communications Magazine, 2022, DOI: 10.1109/MCOM.2021.012221. 3. **Comprehensive Reviews on ML in Cybersecurity:** o A systematic review of machine learning approaches in cybersecurity can add more depth: ▪ B. Biggio and F. Roli, "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning," Pattern Recognition, 2018, DOI: 10.1016/j.patcog.2018.07.023. 4. **Case Studies in Specific Applications:**	

	o Recent case studies on ML in detecting specific cyber threats: ▪ M. Rigaki and S. Garcia, "Bringing a GAN to a Knife-fight: Adversarial Attack on Neural Networks Using GANs," IEEE Transactions on Information Forensics and Security, 2021, DOI: 10.1109/TIFS.2021.3120039. By incorporating these additional references, the manuscript would present a more comprehensive and up-to-date perspective on the subject. This would enhance its scientific rigor and relevance for both researchers and practitioners in the field.	

Review Form 3

Is the language/English quality of the article suitable for scholarly communications?	The language quality of the manuscript is generally suitable for scholarly communication, but there are areas where it could be refined to enhance clarity, coherence, and academic tone. The manuscript demonstrates a strong command of technical vocabulary and appropriately uses domain-specific terms related to machine learning and cybersecurity. However, some sentences are overly general or lack precision, which may dilute the impact of the arguments presented. **Observations:** 1. **Clarity and Conciseness:** o Certain phrases, such as "a void exists in the field" and "contemporary technology has rendered it challenging," are vague and should be replaced with more specific language to clearly articulate the gaps or issues being addressed. 2. **Sentence Structure:** o Some sentences are long and complex, which can hinder readability. Breaking these into shorter, more concise statements would improve the flow of the text. 3. **Grammar and Syntax:** o Minor grammatical inconsistencies were noted, such as the misuse of articles ("advantage of in cybersecurity") and awkward phrasing in some parts. These should be corrected for better readability. 4. **Academic Tone:** o While the manuscript maintains a scholarly tone overall, certain sections, particularly the abstract and introduction, include phrases that could be more formal and precise. **Recommendations:** • Conduct a thorough proofreading to address minor grammatical errors and inconsistencies. • Simplify complex sentences while retaining technical accuracy. • Replace vague expressions with precise descriptions of the research's contributions and findings. Enhancing these aspects will ensure that the manuscript meets the high standards required for scholarly communication and effectively conveys its scientific significance to the audience.	
<u>Optional/General</u> comments	Based on the provided content of the manuscript, there do not appear to be any overt ethical issues. The manuscript discusses the application of machine learning in cybersecurity, focusing on methods, benefits, challenges, and future directions. It does not involve experimental research on human subjects, sensitive personal data, or any controversial practices that would raise ethical concerns. Ethical Considerations: 1. Appropriate Attribution: o The manuscript includes a comprehensive list of references, and ideas are attributed to their original sources, which aligns with ethical standards in scholarly writing. o No instances of plagiarism or misrepresentation of data have been observed. 2. Responsible AI and ML Use: o While the manuscript discusses the benefits of machine learning in cybersecurity, it could briefly address the ethical implications of its use, such as potential biases in algorithms or the misuse of ML technologies by malicious actors. Including such a discussion would strengthen the manuscript's ethical considerations. 3. Transparency in Claims: o The claims about the capabilities and effectiveness of machine learning are general but not exaggerated or misleading. Providing more concrete examples or empirical data would further support ethical and scientific rigor. Suggestions: • Add a brief discussion on the ethical implications of machine learning in cybersecurity, including considerations for bias, transparency, and accountability in AI systems. • Ensure that all referenced studies comply with ethical research standards. By incorporating these considerations, the manuscript can further enhance its ethical robustness and contribute responsibly to the academic discourse.	

Review Form 3

PART 2:

	Reviewer's comment	**Author's comment** *(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Are there ethical issues in this manuscript?	*(If yes, Kindly please write down the ethical issues here in details)*	

Reviewer Details:

Name:	**Joseph Chukwunweike**
Department, University & Country	**UK**