|  |  |
| --- | --- |
| Journal Name: | [**Asian Journal of Research in Computer Science**](https://journalajrcos.com/index.php/AJRCOS) |
| Manuscript Number: | **Ms\_AJRCOS\_134182** |
| Title of the Manuscript: | **A Multi- Level Clustering Framework for Cybersecurity Risk Stratification in Healthcare: A Dynamic, Overlapping Approach to Threat Classification and Mitigation** |
| Type of the Article | Research |

|  |  |  |
| --- | --- | --- |
| **PART 1: Comments** | | |
|  | **Reviewer’s comment**  **Artificial Intelligence (AI) generated or assisted review comments are strictly prohibited during peer review.** | **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 ‘ *A Multi- Level Clustering Framework for Cybersecurity Risk Stratification in Healthcare: A Dynamic, Overlapping Approach to Threat Classification and Mitigation’* provides insights into a much needed mindset shift among healthcare organizations in how they think about financial allocation for cybersecurity. The proposed approach talks about the sophisticated nature of evolving threats in the current era and calls organisations to look into their financial spending including keeping their IT systems and technology up to date and compliant so as to safeguard their org from potential breaches. Therefore I believe this is a very important topic that our scientific community needs to highlight - as discussing the impact and its root cause could help organizations to reevaluate their current cybersecurity strategy and spending. |  |
| **Is the title of the article suitable?**  **(If not please suggest an alternative title)** | I think the title should also include aspects on the impact not just the threat classification. Correlation between the financial spending and how it is attributed to being ready to face and pass through more real time sophisticated threat vectors. |  |
| **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.** | I suggest adding the overall outcomes in the abstract section. This way we know how holistically the proposed approach brings things together from an impact perspective. I’d have enjoyed looking at more concrete financial data from healthcare organizations to make this more concrete. How is their spending look like and how has that correlated to the breach experiences that had. Although I understand that it’s not always easy to get such financial data, authors could have done reverse correlation. Eg: This is a breach that happened and the financial impact to restore (time and complexity) could have been considered together. This needs a lot more in-depth research given the manuscript talks about threat vectors, more real time sophisticated and intertwined nature, life cycle of IT systems and technology, Compliance frameworks, Financial impact.. |  |
| **Is the manuscript scientifically, correct? Please write here.** | Although the different threat vectors and their classifications are already well known in the industry, this is a good way of restating the obvious with a more emphasis on the fuzzy nature of how these interplay together. They are all one way or the other intertwined. For example: Phishing-malware-data exfiltration/ransomware forms one complete attack unit. The attacks are becoming more sophisticated in nature and evolving rapidly. |  |
| **Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.** | Yes I think references are good enough. |  |
| **Is the language/English quality of the article suitable for scholarly communications?** | Yes |  |
| **Optional/General** comments |  |  |

PART 2:

|  |  |  |
| --- | --- | --- |
|  | **Reviewer’s comment** | **Author’s comment** *(if agreed with the 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?** | No |  |

**Reviewer Details:**

**Priyanka Neelakrishnan, Enterprise Cybersecurity Product Leader and Independent Researcher, United States of America**