**ANALYZING A JOURNAL ARTICLE 4**

NAME: Sushmitha.S   DATE: 11-04-2022

JOURNAL ARTICLE TITLE: MACHINE LEARNING BASED INTRUSION DETECTION SYSTEM.

**Step 1. What is the purpose/hypothesis/aim/objective of the study?**

|  |  |
| --- | --- |
| a. Write down the exact statement in which the  authors describe what they were testing. (Hint:  This information may be provided in the article as  a purpose statement or as a hypothesis). Include  quotation marks around the exact wording, and  indicate page number(s). | In order to improve the performance, different techniques have been used in recent works. Analyzing huge network traffic data is the main work of intrusion detection system. A well-organized classification methodology is required to overcome this issue. This issue is taken in proposed approach. Machine learning techniques like Support Vector Machine (SVM) and Naïve Bayes are applied.(Page number: 916) |
| b. Now describe the purpose of the study (as you  understand it) in your own words. | IDS has the ability to detect both known and unknown attacks, but encounters a high false alarm rate. |
| c. What was the “gap” in the research that the  authors were trying to fill by doing their study? | Various machine learning techniques are incorporated to decrease false alarm rate. |

**Step 2. What is/are the major finding(s) of the study?**

|  |  |
| --- | --- |
| a. Make some notes about the authors’ major conclusions or findings as written in the article.  Include quotation marks whenever you use their exact wording, and indicate page number(s). | The analysis deals with machine learning algorithms like SVM and Naïve Bayes. It proposes while dealing with 19,000 instances SVM outperforms Naïve Bayes.(Page number: 920) |
| b. Now write those conclusions (as you  understand them) in your own words. | It deals with building an more effective model based on well-organised classifiers which are capable to categorise new attacks with better performance. |

**Step 3. How did the authors test their hypothesis?**

|  |  |
| --- | --- |
| a. Briefly summarize the main steps or  measurements that the authors used in their  methods. Try to explain in your own words as  much as possible. | A. Intrusion Detection System B. Machine Learning  C. Support Vector Machine  D. Naive Bayes |
| b. Do the authors suggest any problems or  limitations with their methodology? Do you see  any problems or limitations with their  methodology? | Accuracy problem.. |
| c. How did the authors analyse their data? What  test/s did they use? | A. Pre-Processing  B. Methodology  Example:  INPUT: Preprocessed Data  OUTPUT: Output Classes |

**Step 4. How reliable are the results?**

|  |  |
| --- | --- |
| a. Do the authors suggest any problems with the  study that could lead to unreliable results? | Accuracy problem.Future work deals with large volume of data, a hybrid multi-level model will be constructed to improve the accuracy. |

**Step 5. Based on your analysis, are the claims  made in this journal article accurate?**

|  |  |
| --- | --- |
| a. Do the conclusions made (about the results) by  the author make sense to you? Are the  conclusions too broad or too narrow based on  what was actually done in the study? | Yes the conclusions make sense and too narrow. |
| b. Based on the accuracy of the methodology and  the reliability of the results as described in Steps 3  and 4, do you think the conclusions can be  believed? | Partially believed. |

**Step 6. What is the importance of this scientific work?**

|  |  |
| --- | --- |
| a. Write (in your own words) the significant  contributions of the experimental work in this  journal article as reported by the authors. | The authors tried to experiment Machine Learning Based Intrusion Detection System. |
| b. Re-read your notes and explain why you think  this is  o a strong or weak scientific article  o a strong or weak scientific study | It is a weak scientific study and a weak scientific article. |