

Review Form 1.7

Journal Name:	Asian Journal of Research in Computer Science
Manuscript Number:	Ms_AJRCOS_111124
Title of the Manuscript:	Machine learning based Classifier in Cybersecurity
Type of the Article	Method Article

Review Form 1.7

PART 1: Review Comments

	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)
<p>Compulsory REVISION comments</p> <p>1. Is the manuscript important for scientific community? (Please write few sentences on this manuscript)</p> <p>2. Is the title of the article suitable? (If not please suggest an alternative title)</p> <p>3. Is the abstract of the article comprehensive?</p> <p>4. Are subsections and structure of the manuscript appropriate?</p> <p>5. Do you think the manuscript is scientifically correct?</p> <p>6. Are the references sufficient and recent? If you have suggestion of additional references, please mention in the review form.</p> <p><u>(Apart from above mentioned 6 points, reviewers are free to provide additional suggestions/comments)</u></p>	<p>Yes, Machine learning has shown promise in identifying patterns and potential threats that might not be easily recognizable through traditional methods. The paper compares three different machine learning algorithms (Trees J48, Naive Bayes, and Decision Stump) in the context of cyber security. This comparative analysis provides valuable insights into the performance and effectiveness of these algorithms for threat detection and categorization.</p> <p>No, The Title Is Clear and Basic .As per my perspective my suggestions are</p> <ol style="list-style-type: none"> 1. Harnessing Machine Learning for Effective Cyber security Classifiers. 2. A Comparative Analysis of Cyber security Threat Identification Through Machine Learning Classifiers <p>Yes, It outlines the aim of the paper, suggesting that it proposes machine learning techniques to categorize data, emphasizing the potential benefits of this categorization in establishing correlations and uncovering hidden threats.</p> <p>No,Author can add an title “CYBER SECURITY AND ML”to analyse the impact of ML classifiers in Cyber security so far.</p> <p>Yes</p> <p>Yes</p>	<p>Changed Journal title to "Harnessing Machine Learning for Effective Cyber security Classifiers as suggested line 2-3</p>
<p>Minor REVISION comments</p> <p>1. Is language/English quality of the article suitable for scholarly communications?</p>	<ul style="list-style-type: none"> • The Proposed work does not provide the enormous current challenges and limitations faced during the application of machine learning techniques in cyber security. • How much data is considered as Benign and malignant data for analyzing the proposed method? <p>Yes</p>	<p>The datasets consist of benign, DNS, darknet,malware, spam, phishing datasets. After collecting datasets, it was found that some data were balanced (60:40%; benign: malicious). Whereas some were unbalanced (90:10%; benign: malicious line 146-148</p>
<p>Optional/General comments</p>	<p>J48 Algorithm can handle missing values by ignoring them during tree construction, this approach might lead to biased or incomplete decision-making if the missing data holds significant predictive value.</p>	<p>It was discovered during the simulation that, the TreesJ48 algorithm was able to identify the significant predictive values in the dataset. It was proficient in classifying significant from insignificant predictive values and not landing on biased end results. Line 241-243</p>

[Review Form 1.7](#)

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)	