Incorporation of Peer Review Feedback Report

CSE 543 - Group 16

Saud-1-2. “The methodology shows good analytical depth in comparing multiple ML approaches. This strong foundation could be further enhanced by adding a quantitative analysis of processing speeds and resource requirements for each technique.”, Defense: Valid. A quantitative analysis of processing speeds would be a good addition to our paper; one member of our team can run all of the models on one machine to find a useful comparison of processing speeds.
Saud-2-1. “ The presentation of each ML technique is clear and well structured. To make this even stronger, consider standardizing the presentation format across all models to facilitate easier comparison.”, Defense: Valid. Our team is making changes such as ensuring that the same metrics are presented for every model and that the metric scores are given in the same format for every model.
Saud-2-2. “Results are presented with strong attention to detail. Consider enhancing this by adding a consolidated summary table comparing all model metrics accuracy, precision, recall, F1-score, processing time.”, Defense: Valid. Our team is adding a table comparing the metrics and processing times of all models.
Saud-3-2. “The practical implications are well considered. Enhance this by expanding the discussion of real-world deployment challenges, particularly focusing on integration with existing security infrastructure.”, Defense: Valid. Our team is adding more background information about real-world deployment challenges for these types of systems to give context to the usefulness of the solution.
Saud-3-3. “The performance analysis is thorough. Consider strengthening it by including detailed analysis of trade-offs between model complexity, detection speed, and accuracy for real-time applications.”, Defense: Valid. As stated above, our team will add a comparison of processing speeds and an analysis of the relationship between processing speeds and metrics.

Melanie-?-1. “Acronym ROC, IDS/IPS, NIPS are mentioned in Literature Review but isn't defined.”, Defense: Valid. The acronyms have been fixed to be defined the first time they are used.

Shrajal-1-1. “The research paper shows a detailed understanding of the topic, however, in the research topic it is also mentioned that the implementation of these techniques into supply chains, if details regarding this can be added to the paper.”, Defense: Valid. The paper talked about implementing this method in supply chain networks but never elaborated on it. More details on how this solution can be implemented in the supply chain domain have been added to the paper.
Shrajal-5-1. “Just one point regarding this is a little inconsistency in the writing while explaining different techniques in results section, for ex: when talking about the accuracy in the results

section the LR results are in percentage, the Naive Bayes is in decimal, CNN contains a lot of details and parameters which are missing in few others.”, Defense: Valid. The different models used had inconsistency in terms of results being showcased. More evaluation metrics have been added for each algorithm.

Kumar-1-1. “While the research covers a broad range of models, there are some areas where the analysis could go further especially in analyzing the trade-offs specific to DDoS detection. For example, discussing the computational cost and real-time applicability of each model (especially CNN and ANN) would add depth. A comparison of computational efficiency could be relevant for real-world applications where processing speed is critical.”, Defense: Valid. As stated above, a quantitative analysis of processing speeds would be a good addition to our paper; one member of our team can run all of the models on one machine to find a useful comparison of processing speeds.
Kumar-3-1. “The paper includes original insights on the practical implications of using ML models in supply chains and network security. However, the originality is somewhat limited in terms of proposing novel model configurations or hybrid approaches specifically tailored to DDoS detection. Including unique approaches or proposing specific modifications to enhance model accuracy or efficiency in DDoS detection could enhance originality. Suggestions for novel combinations of models or optimization techniques would further strengthen this area.”, Defense: Valid. Suggesting and testing specific modifications to existing models designed for DDoS protection would strengthen the paper, but this is outside the scope of our project as our project focuses on comparing existing models as they exist in a general form.

Pravalikka-1-1. “The paper demonstrates a solid understanding of DDoS attack detection using various machine learning techniques. However, it could explore additional perspectives or details: The literature review is comprehensive, but could benefit from more critical analysis of cited works. The paper lacks a detailed discussion on the limitations of the CICIDS2017 dataset. There's limited exploration of potential biases in the dataset or models.”, Defense: Valid. Our team will add analysis of the limitations listed in cited works and of the CICIDS2017 dataset to explore potential biases in the field and in the data.
Pravalikka-2-2b. “The Results section varies in depth and structure across different models.”, Defense: Valid. Our team will ensure that the same metrics are given in the results section for each model, which will help to standardize their depths and structures.

Sai-3-1. “While the paper delves into multiple machine learning algorithms run regarding this application, based on confusion matrices presented in the paper it seems that the models are run on different variations of the data which invalidates the point of comparison between the prediction models. ”, Defense: Valid. All models will be checked to ensure that preprocessing is performed the same way for all models, and confusion matrix generation will be standardized so all confusion matrices use the same format.

Sai-5-1b: “The title of Figure 2 seems to be Linear Regression while the graph represents Logistic Regression.”, Defense: Valid. The title of the figure has been fixed.

Kashyap-1-1. “However, the paper could benefit from a more in-depth discussion of the CICIDS2017 dataset's characteristics and why it was chosen over other datasets”, Defense: Valid. More details regarding the CICIDS2017 dataset, its characteristics, and its advantages over other datasets will be included.

Kashyap-2-3. “Some sections (e.g., methodology for Random Forest) lack detail compared to others.”, Defense: Valid. While some methodology sections are shorter than others due to the relative simplicity of some models, the methodology section for Random Forest in particular is lacking in detail. Our team will add more detail about our specific implementation to that section.