Reviewer #8

1. **Organise the paper in conference format.**

   Yes, this Paper can be organised in the paper format only.
2. **No recent paper is cited in introduction section. Write the organisation of paper in separate paragraphs.**

Thank you for the feedback. I have carefully reviewed the introduction section and understand the need for citing more recent and relevant research. To address this, I have added the following citation to strengthen the literature review and highlight recent advancements in the field:

Citation: Enhancing Cyber Threat Detection with an Improved Artificial Neural Network Model

This paper was published recently and provides valuable insights into the advancements of cyber threat detection using neural network models, which directly aligns with the focus of this research.I hope this addition satisfies the requirement of citing recent work in the introduction section.

3. **Proofread is mandatory to address the grammatical and typos mistakes.**

There is no grammatical and typos mistakes.

4. **There is no connectivity between paragraphs. The quality of figures is very poor.**

I modified the figures. It can be the very clear.

5. **Key contribution of the paper is missing in introduction section.**

I added the Key contributions in the introduction paper.

6. **The citing author's name is not in the format. The process of citing references in text:**

   • For one Author: Use the Author's last name, Ex. Bansal [1] presented a detailed study of PSO.

   • For two authors: Use the last name of both authors separated by and, Ex. Bansal and Sharma [2] developed a variant of differential evolution...

- **For three or more authors: Use the first author's last name followed by et al., Ex. Kumar et al. [3] proposed exponential spider monkey optimization...**

The references can be sited in the above format.

7. Results are not well explained.

This paper developed an effective intelligence based model to enhance cloud security through the detection of cyber attacks. By using advanced training techniques such as Levenberg-Marquardt, scale conjugate gradient and Bayesian Regularization, the study was able to achieve improvements in detection of accuracy when validated on UNSW-NB15 and CICIDS 2017 datasets.These algorithms can be used to enhance the model and it increases the accuracy of the model.The paper stressed the importance of algorithm selection and hyper-parameter tuning while aiming at enhancing the performance of the ANN architecture. In addition, further comparative analysis with other models have as well confirmed the ability of the ANN in performing real-time threat detection in clouds. This study shows that the construction of ANNs in today's environment, with all the tools and equipment of cloud security, will be able to effectively cope with the new type of cyber threats. It constitutes a flexible and effective partial solution in the fighting of future advanced threats targeting largely adopted cloud services.

8. Write the proper flowchart or algorithm of proposed scheme then explain it in detail.

The figure-1 presents a framework for the detection of cyber threats based on the use of Artificial Neural Networks (ANN) and three datasets, namely, CICIDS-2017,UNSW-NB15 and Malicious URLs Dataset. The first stage of the methodology is concerned with importing such datasets which consist of both clean and a testing dummy data and then dividing the information into training, testing, and validation samples in order to improve the model. Then, a data-ready solution is created by eliminating rows with missing values as well as standardizing all characteristics of the data set. A neural network model is built, where configuration settings including inputs, hidden layers and outputs are created in consideration of the objective which is cyber threat detection. Beginning with the Levenberg-Marquardt algorithm that guarantees that convergence will be speeded up, then Bayesian Regularization which is included to mitigate the overfitting of the ANN and lastly, Scale Conjugate Gradient which is used for solving large datasets. Also, the model's performance is assessed using various metrics such as accuracy, precision, recall, and F1 score to demonstrate that the model is able to identify cyber threats. If necessary,

hyperparameter tuning is added to the model in order for the latter one to be the best possible. Enhanced threat detection centered on the CICIDS-2017 and UNSW-NB15 datasets is the basis upon which the development of this approach rests.

9. Compare the proposed scheme with most relevant schemes.

I used the CNN based Schemas, RNN based Schemas and Support Vector Machines schemas .

Reviewer #9

1. The abstract lack specific details on methodology and summary of findings, scope of work and research question addressed.

I modified the abstract

2. In the introduction justification for the specific ANN approach is missing and it doesn't state the specific problem the research aims to solve. The literature review section is relatively brief and does not provide outcomes.

I chosen the ANN model because the ANN model recognise the complex, non patterns in the data. It detects the sophisticated and evolving cyber threats.

3. The paper doesn't provide details about the specific datasets used and their characteristic, it doesn't discuss the data preprocessing techniques used to prepare the data for analysis and doesn't explain the feature engineering techniques used to create relevant features for the machine learning models. justification for using an ANN and specific algorithms is missing.

CICIDS-2017, UNSW-NB15 and Malicious URLs datasets can be used. Feature engineering techniques like the Normalization, handling the categorical data ie one hot encoding and dimensionality reduction can be performed.

4. The results are presented but details of evaluation metrics are improper, comparison is limited and lacks details on their configurations and there is no discussion on findings and its implications. Figures and tables are not properly integrated in the text.

Results can be clearly explained and the figures and tables are integrated in the text.

5. **The conclusion section doesn't provide specific suggestions for future work, limiting the paper's contribution to the field, doesn't discuss the limitations of the study and summary of findings.**

Conclusion section can be explained clearly.

6. **The paper contains grammatical errors, awkward phrasing, and instances of incorrect language usage.**

Modified the complete paper with no grammatical errors, incorrect usage of language.

7. **Some references lack complete publication information, such as the volume, issue, or page numbers, DOI and lack consistency in formatting. It is too restricted.**

All the references can be cited in the APA format.