Date: 29-09-2023

Dear Editors,

At the outset, on behalf of all the authors, I thank the reviewers for their valuable comments and suggestions on the manuscript.

The manuscript's content is revised to meet the reviewers' concerns regarding the statistical analysis of the proposed approach and some remarks in the references. You'll find responses to the reviewers' comments on the following pages.

We believe that the manuscript is now suitable for publication in PeerJ Computer Science.

Sudhanshu Shekhar Bisoi.

Dr. Sudhanshu Sekhar Bisoyi

Assistant Professor
Department of Computer Science and Information Technology
Institute of Technical Education and Research
Siksha 'O' Anusandhan (Deemed to be) University
Jagamara, Bhubaneswar-751030, Odisha, India
sudhanshu.bisoyi@gmail.com
(On behalf of all authors.)

Reviewer 1 (Anonymous)

Basic reporting
All of my earlier comments have been successfully addressed by the authors.

Experimental design
All of my earlier comments have been successfully addressed by the authors.

Validity of the findings
All of my earlier comments have been successfully addressed by the authors.

Additional comments
All of my earlier comments have been successfully addressed by the authors.

I am recommending the paper to be accepted.

Reviewer 2 (Anonymous)

Basic reporting
This paper present a study of a multiclass classification problem utilizing an imbalanced data set, and the characteristics used to examine the categorization of each form of malware are the API sequences from various malware classes. To combine the output of various 1D-CNN classifiers trained using the One-vs-rest principle, a 1D-CNN based ensembled architecture is presented. For training and testing purposes, the data set Mal-API-2019 is used.

The Word2Vec embedding technique with the Skip-gram model is used in the proposed ensembled 1D-CNN architecture to look into the semantic relationships between APIs in API sequences. A few 1D-CNN classifiers are trained on the data set utilizing the One-vs-rest notion for classifying the various classes of malware. A suggested ensembling method combines each of these results to explore efficiency improvement.

This architecture has three phases and conducts training and testing using data set. The dataset is vectorized in the first phase, independent 1D-CNN models are trained as One-vs-rest classifiers in the second phase, and in the final phase, an ensembled model using the ModifiedSoftVoting algorithm is created to address the multiclass malware classification problem.

Experimental design
Good design

Validity of the findings
Good results

Additional comments
Remarks:
Most of the remarks of the first review have been taken into account by the authors.
However, there are still ignored remarks in the references section such as:

9. Please consistently use the page numbering in the references section, in some cases you use: 208-233 in others you use pages 137-149

Response: The references are rewritten following the directions the esteemed reviewer gave.

Reviewer 3 (Anonymous)
Basic reporting
Several issues I identified have been addressed. However, the problem is still not motivated within the landscape of larger cybersecurity. Specifically in Kavak et al. (Simulation for cybersecurity: state of the art and future directions) the problem the authors are addressing is identified as a future direction research of cybersecurity would better establish the need for the research.

Response: We have referred to the article by Kavak et al. to establish the need for research. This is reflected in lines 145–147 of our article to ensure motivation within the larger cybersecurity landscape.

Experimental design
These issues have been sufficiently addressed.

Validity of the findings
Several issues I identified have been addressed. However, the problem of conducting tests for statistical significance of the superior performance of the ensemble model compared to alternatives has not been performed established. This would demonstrate that the ensemble approach's superior performance is likely to generalize to different benchmarks as opposed to it just being noise in the evaluation data leading to ensemble approach being evaluated as more effective.

Response: Lines 283-294 add further content and results to the article to highlight the ensemble model's improved performance. The ensemble model's statistical significance in comparison to a base model is confirmed by McNemar's test.