>>>>The paper does not provide comparable results with existing literature. These results would provide a more comprehensive understanding of the strengths and weaknesses of the proposed approach.

Solution::::

Accuracy = [0.9964548494983277, 0.9606020066889632, 0.939933110367893, 0.9389297658862876, 0.9332441471571906, 0.9037458193979934, 0.8147157190635451, 0.8110367892976589, 0.8018060200668896, 0.7763879598662208, 0.7476923076923077, 0.7138461538461538, 0.6842809364548496, 0.6709030100334448, 0.6577257525083612, 0.5874247491638795, 0.5807357859531772, 0.5721070234113712]

Precision = [0.9948263854342851, 0.9444601870218192, 0.9224057917208094, 0.9212014461852229, 0.9140754369825207, 0.8790401133445497, 0.7889226342710998, 0.7855153203342619, 0.7798902235303476, 0.766813627254509, 0.7480484307790346, 0.730020903682264, 0.7119120244019906, 0.7053354890864996, 0.6983185768824628, 0.6690488794776778, 0.6644052863436123, 0.6574049803407601]

Recall = [0.9999, 0.9999, 0.9938, 0.9937, 0.9936, 0.9927, 0.9871, 0.987, 0.9804, 0.9566, 0.9391, 0.908, 0.8869, 0.8725, 0.8597, 0.7583, 0.7541, 0.7524]

F1 Score = [0.9973567403122039, 0.9973567403122039, 0.9713897119541459, 0.9567728891884085, 0.9560783181796315, 0.9521801629132727, 0.9324191048701451, 0.876954513148543, 0.8748061156658542, 0.8687253555447256, 0.8512569521690767, 0.8327569389021903, 0.8093412960156877, 0.7898299047110161, 0.7800625838176128, 0.7706512482631886, 0.7108840348739102, 0.7064168618266979]

For Window size 2-20

Comparison with: Performance Evaluation …. And Taking a Peek …. (Week 7)

>>>> Fig 3 offers visuals on the proposed approach. Very little of figure 3 is explained in the texts of the paper. Unfortunately, it’s hard to understand the approach by simply looking at Fig 3. For example, how do you detect a benign call and filter it from? Is it a signature-based approach, i.e., you only check a list of system call sequences and if a sequence does not match those in the list it is a malicious call? If so, how do you ensure the robustness and completeness of those signatures? None of these are addressed.

Solution::::

Redesign the whole figure. Explain each box more simply.

>>>> The paper does not clearly bring out what are the main scientific contributions of the paper. The seems to be a fair amount of engineering involved. But what is the novelty - it is unclear.

>>>> The evaluation of the proposed approach is missing too many details. For example, how different thresholds (e.g., the upper and lower bounds) are measured? Are they defined on the same data for training and evaluation? How are the training and evaluation data obtained? How precision and recall are measured? Is precision when the approach identifies that a container has a security issue? If so, the precision is either 0 or 100%? The same question for Recall.