Evaluation of parameter changes on DL models

Mentor's Name: -- **Dr. Binod Kumar**

Authors: -- Abhishek Jilowa (B20CS001), Aman Mithoriya (B20CS004), Gojiya Piyush D(B20CS015) and Harsh Sharma (B20CS017).

Abstract: -

There are now practical uses for neural networks outside of theoretical equations. Understanding neural networks' dependability under less-than-ideal computing circumstances is necessary for its application in real-world settings. The execution of neural network programmes can be impacted by environmental and cyber hazards, but little is known about how resilient neural networks are to attack. The robustness of convolutional neural networks (CNNs) and multilayer perceptron neural networks (MLPs) against weight mistakes is examined in this study. The emphasis is on errors of the Single Event Upset (SEU) type, such as discrete bit flips in memory. To determine whether there is a relationship between neural network architecture and robustness to weight mistakes, the classification accuracy of the networks is assessed both before and after bit flips. According to the experimental findings, MLP networks are often far more resistant to weight mistakes than CNNs. For MLPs, larger networks with more layers outperform smaller, shallower networks in terms of robustness, and for CNNs, larger networks outperform smaller networks in terms of robustness.

Introduction: -

The use of neural networks is expanding beyond academic research and into industry. One of the first kinds of neural networks were multilayer perceptrons (MLPs), but as the field developed, many other architectures emerged, such as convolutional (CNN) and recurrent (RNN) neural networks.

The science of computer vision has seen a revolution thanks to neural networks, and these technologies are swiftly expanding to other disciplines like robotics and natural language processing. This work investigates the robustness of MLPs and CNNs to faults in their weights during training. The Cifar10 dataset is used to train the networks initially. Their Cifar10 accuracy

is noted, and weight errors are then used. The networks' weight mistakes are distributed at random. To determine whether there is a relationship between network size and resilience, several sizes of MLPs and CNNs are evaluated. In order to determine which architecture is fundamentally more resistant to weight mistakes than the other, the performance of the MLPs and CNNs is compared.

Design Problem Formulation: -

We must explore the methodology of parameter changes in accuracy of DL models .We must also explore the robustness of MLPs and CNNs to errors in their weights after training .
The performance of the MLPs and CNNs is compared to see if one architecture is inherently more robust to weight errors than the other .Another area that should be explored with the networks is determining which layers are most sensitive .

Possible Methods to solve the problem: -

1. Observe accuracy changes in neural networks when weights are changed by Single Event Upset (such as bit flip) .
2. Observe accuracy changes in neural networks when weights are changed by adding impurities.
3. Observe accuracy changes in neural networks when weights are changed by multiplying with impurities.

Methodology adopted for the project: -

We changed the weights of different neural networks by using different methods. The weights of a particular layer are changed multiple times and then average accuracy loss across all the weight changes in that layer is calculated. For each layer we calculate the accuracy loss that occurs due to change in weights and observe the layers that result in minimum loss.

Result: -

Following table shows the accuracy loss across MLP and several variants of CNN. It can be observed that MLP is more robust than variants of CNN. We also observed that generally weight change in last layers results in low accuracy drop.

S.No.	Model	Avg. Accuracy Loss
1	MLP	0.404610936
2	CNN(6 conv+3maxpool)	0.791110917
3	MobileNet	0.801500711
4	AlexNet	1.243002465

Conclusion: -

- From the results obtained by doing several experiments we can say that accuracy loss in MLP is less than CNNs .
- So we can say that MLP is more robust than CNN .
- Also we can say that last layers of the model show minimum loss in accuracy .