CSE499A Senior Design Project I **Group 02**	
Name	Kazi Safin Arafat
ID	2211778642
Section	15
Class	04
Type	Project Update
Faculty	Md. Mohammad Shifat-E-Rabbi

After going through research papers on ML based IDS, there is always a common occurrence of models being big size and computationally intensive. Thus, making them incompatible for IoT devices where hardware power is very limited often running on Raspberry Pi, ESP32, STM32.

Like a paper from S. Pande and A. Khamparia [1] proposed a DNN model that identifies malicious network traffic with high accuracy which used LRP and Lime for model interpretability. But it is only deployable on heavy processing powered hardware ie unsuitable for IoT.

Then another paper from A. E. Muhammad et al. [2] introduced a framework where LIME is embedded into IDS pipeline for interpretability. Which helps Security analysts to understand why a traffic is flagged, reducing false positives. Still, the paper didn't address the compatibility with IoT devices. Also, it is not optimized for real-time performance.

All in all, most of the papers doesn't focus on low powered devices and often opting a cloud-based NIDS which often add overhead to the response time for the Device. So, the gap remains. Our prospective solution is to create efficient model design and post training optimization. TinyML models like TinyCNN, EdgeTPU and the likes possible can create very light weight model. Then there is model optimization like pruning, quantization, distillation and many more.

For our dataset it has to be smaller with less features and strictly traffic has to be from IoT device as we not using it for dedicated NIDS. Some datasets are

NSL-KDD [3] with 125k(approx.) records, 41 features, only problem is that it has outdated attacks

UNSW-NB15 [4] size 2.5M, 49 records. Quite big but we will trim it according to our need.

TON_IoT [5] contains records for specific type of IoT and contains variety of attack factors to train

And this concludes my weekly update of week 04.

References:

[1] S. Pande and A. Khamparia, “Explainable deep neural network based analysis on intrusion detection systems,” Computer Science, vol. 24, no. 1, 2023

[2] A. E. Muhammad et al., “L-XAIDS: A LIME-based eXplainable AI framework for intrusion detection systems,” Cluster Computing, 2025.

[3] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "NSL-KDD dataset," 2009. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html

[4] M. Moustafa and J. Slay, "UNSW-NB15 dataset," 2015. [Online]. Available: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/

[5] A. Tonyali, F. Al-Turjman, "TON_IoT dataset for IoT network security," 2020. [Online]. Available: https://www.unsw.adfa.edu.au/ton_iot_dataset/