Private Memoirs of IoT Devices: Safeguarding User Privacy in the IoT Era

Dhruva Sogal, Keyang Yu, Dr. Dong Chen,
Colorado School of Mines Department of Computer Science

Abstract

The use of Internet-of-Things (IoT) devices in U.S. homes is becoming increasingly popular. These "smart" devices, however, come with a a security and privacy risk: network traffic data collected from IoT devices is frequently sent to servers or data centers where machine learning (ML)-based data analysis is performed, moving personal data out of the control and possession of the consumer. The solution we propose to this problem is to build a new framework that can perform ML analysis locally, on the IoT devices themselves eliminating the need for personal data to be shared. We build a prototype using Raspberry Pi, which can simulate a range of hardware resource limited IoT devices, and validate the feasibility of our new framework using a set of benchmarking metrics. We plan to further evaluate our new framework using more IoT devices and services.

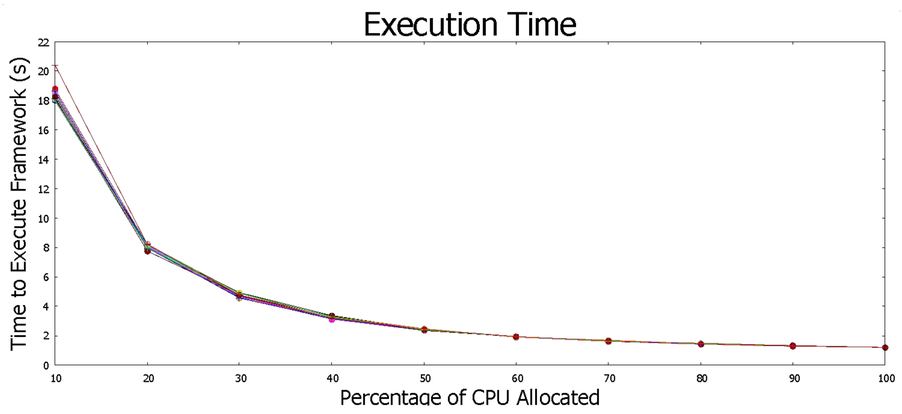
Methodologies

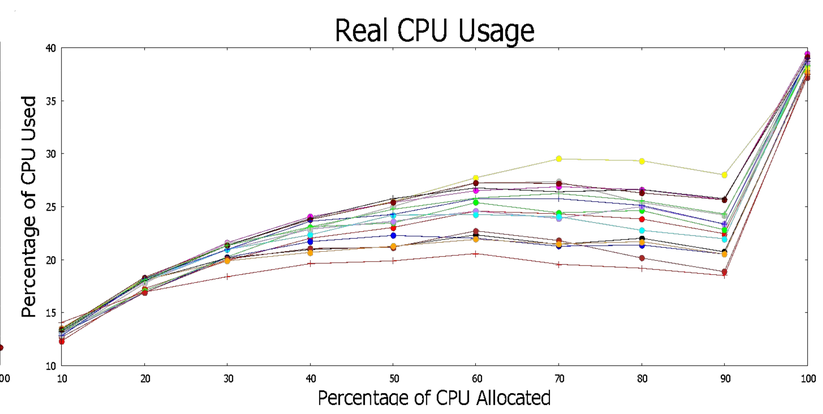
- Utilize BASH scripting to automatically and repeatedly run TinyML Framework[1] at various RAM and CPU Benchmarks
- Collect data at 10 CPU benchmarks at each of 16 different RAM benchmarks
- Turn of Swapping to ensure adherence to RAM benchmarks
- Log execution time, temperature, and actual CPU usage for analysis
- Use weighted sum optimization to find acceptable bounds on CPU allocation

References

[1] *Quickstart for Linux-based devices with Python*. TensorFlow. Accessed: 08/2023. [Online]. Available: https://www.tensorflow.org/lite/guide/python#install_tensorflow_lite_for_python

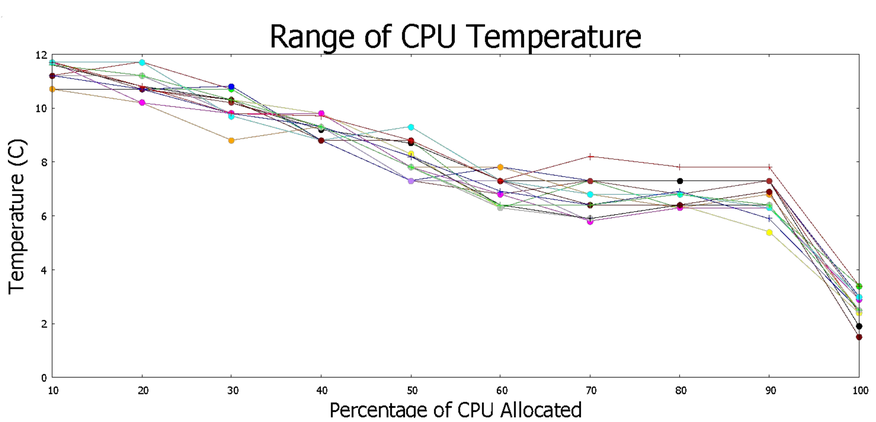
Results

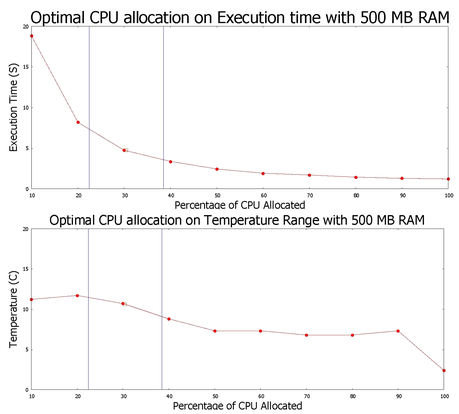


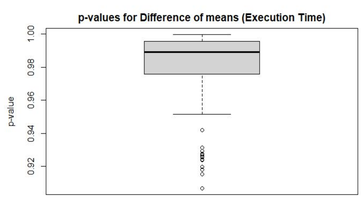


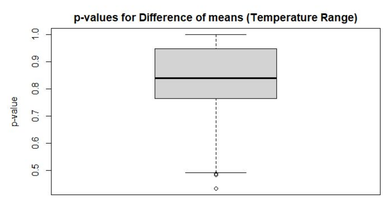
*CPU usage measurement precision = ±15.335

Using weighted sum optimizations for execution time, CPU usage, temperature range of [0.9,0.1,0.1] and [0.99, 0.05, 0.05]
Optimal CPU allocation range:
[22.42, 38.5]









Alternate Hypothesis: Means are not equal

Conclusion

- Framework can be executed at no significant loss using only 500 MB of RAM
- Acceptable execution time is achievable using only ~30% of CPU usage

Next Steps

- Build working system on consumer IoT devices
- Source and benchmark more frameworks