COLLEGE OF ENGINEERING
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

CPE496/498 Capstone Design Course

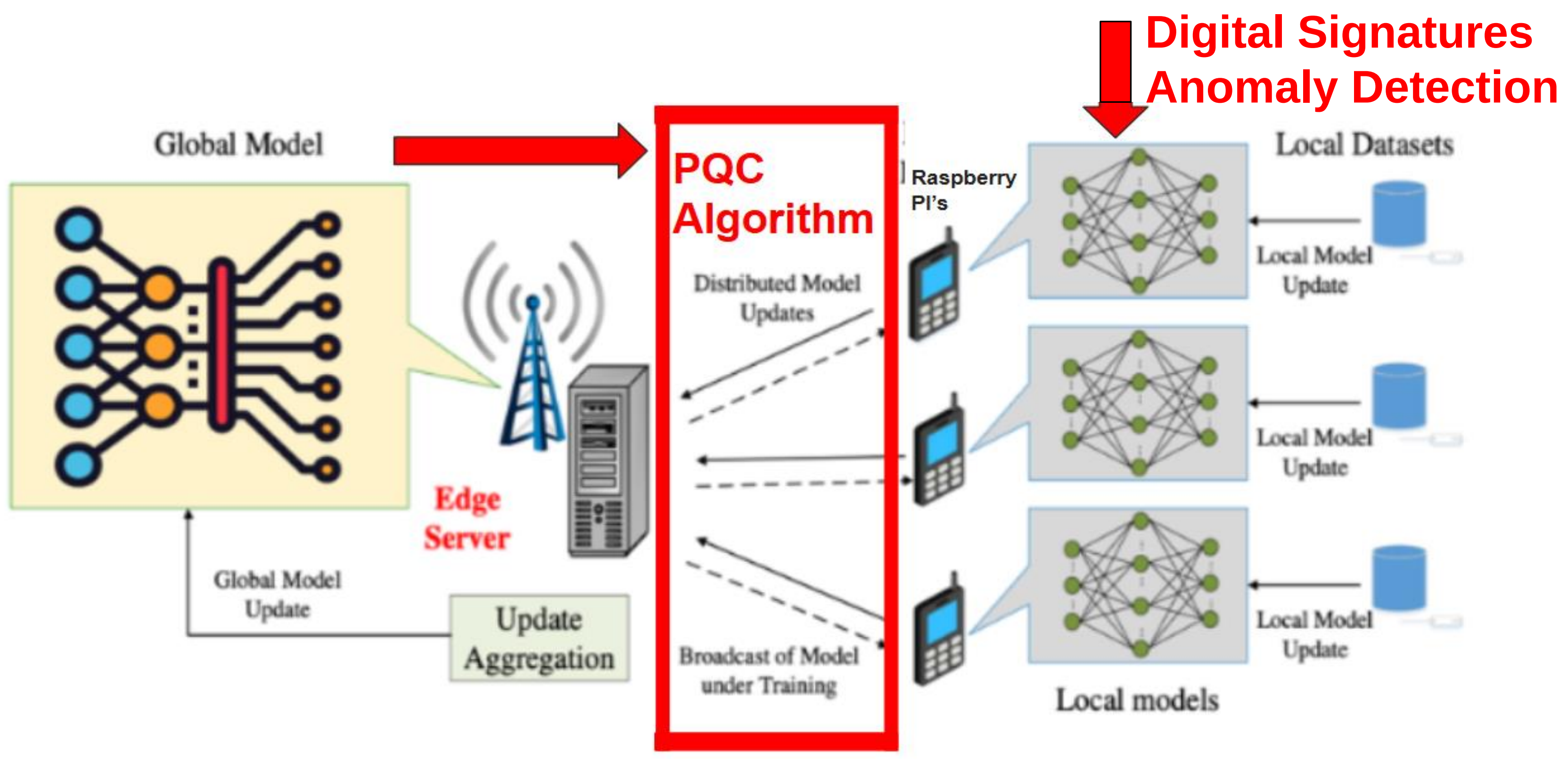
Security for Federated Learning System (SFLS)

Garrett Heston, Michael Agnew, Heath Hudson - ECE department, Dr. Nguyen - ECE department,

Overview of Project

Federated learning is the distribution of machine learning to smaller nodes to increase efficiency and scalability. By transferring models instead of raw data, this drastically improves privacy.

We enhance this privacy by encrypting model distribution (model updates) with post quantum cryptography (PQC).



Major Results & Design

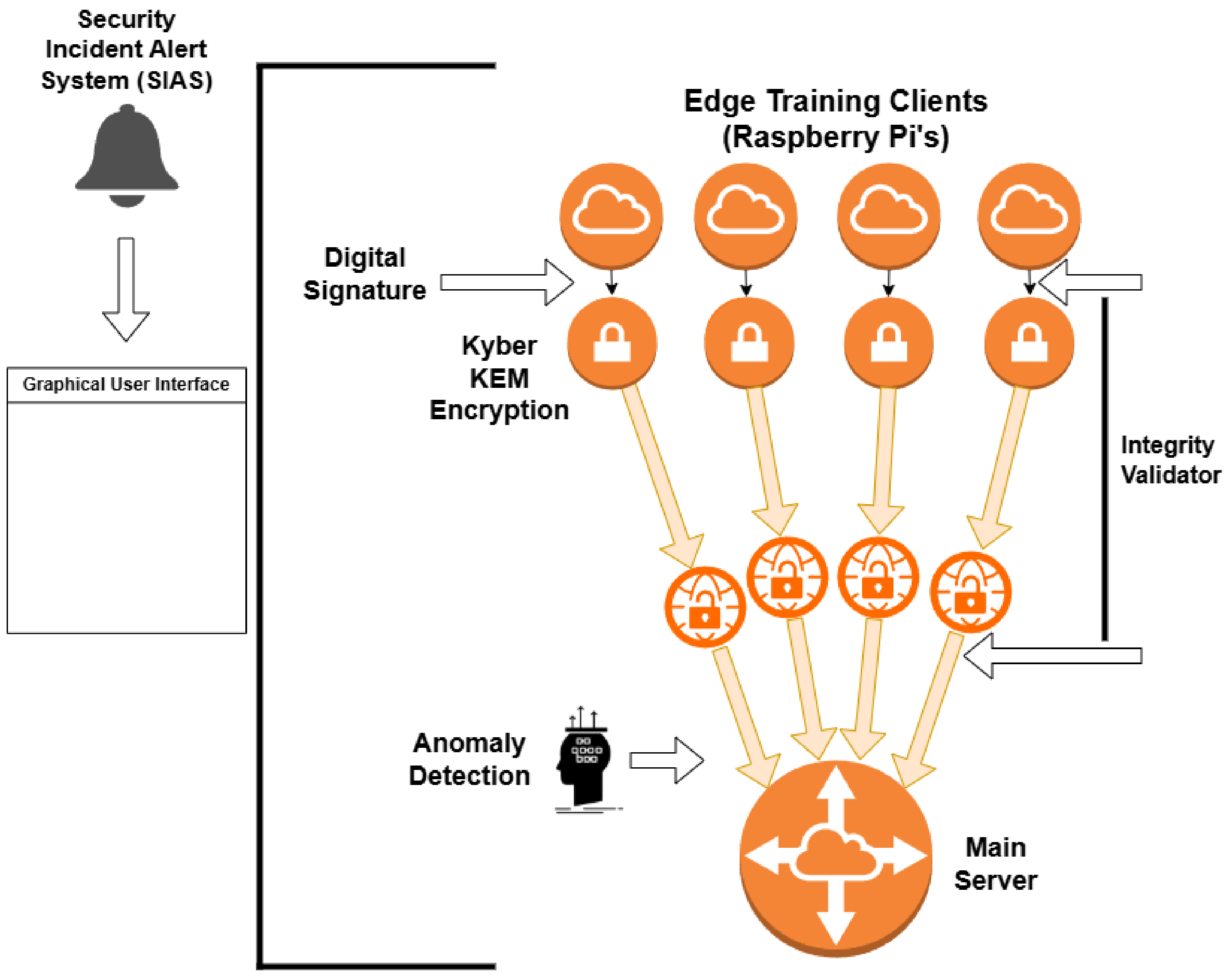
We've fully secured all Raspberry Pi clients: PQC encryption protects model-update transfers; digital signatures authenticate clients; integrity checks ensure update quality; anomaly detection spots poisoned nodes; private SSH key exchange and ephemeral storage safeguard each node; and our Security Incident Alert System (SIAS) notifies admins via a GUI that also serves as the federated-learning control and results dashboard.

Conclusions

We present novel research in the area of federated learning, ensuring security from various threat vectors, providing availability through a graphical user interface, and implementing a future-proof design to protect against quantum attacks. If we had more time or there was a group to take over, we think that blockchain logging would be a good addition to this project.

Requirements

- SFLS must protect model updates and communications with PQC encryption in a federated machine learning system.
- SFLS must be distributed across raspberry PIs that act as machine learning clients.
- SFLS must incorporate security measures such as anomaly detection and digital signatures to detect compromised client nodes
- Create and analyze threat model for system



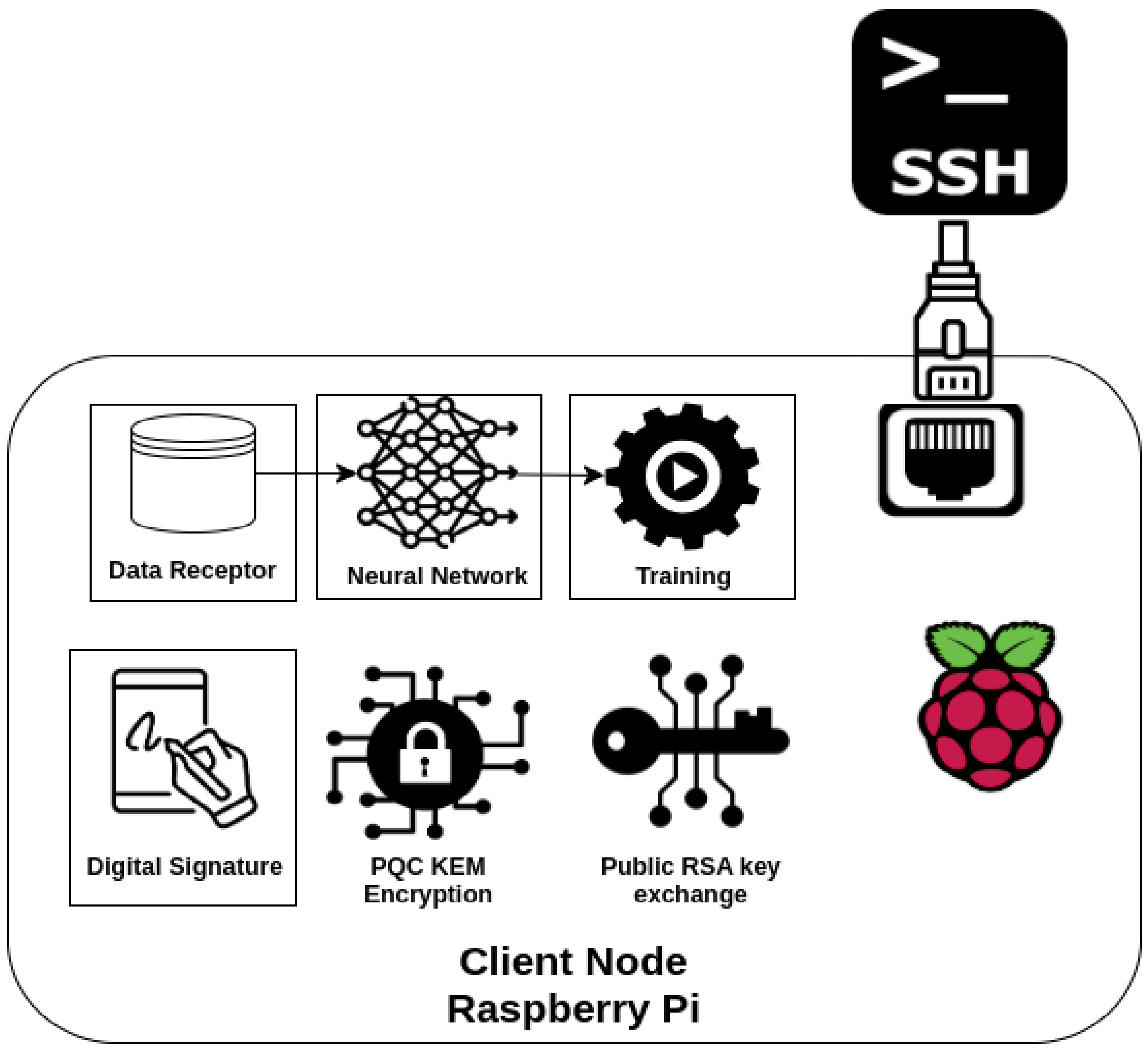


Illustration of Raspberry Pi client system and software design

Acknowledgements and References

Thanks to our sponsor Dr. Nguyen for his provisions. He has provided many facilities including his computer laboratory and 2 raspberry Pis. The ECE department also provided 2 Raspberry Pis.