Problem Statement and Goals

Cloud-based IoT applications collect potentially sensitive information. This poses a massive threat to user’s privacy. Migrate application logic from cloud to edge device with trusted computing capabilities.

Approach

- Migrated speech recognition application from cloud to Intel SGX-capable edge device
- Partitioned codebase into trusted and non-trusted components
- Secure execution of trusted components takes place inside cryptographically signed enclaves
- Remote attestation provides external code verifiability to cloud service provider

Results

- A 10 second long audio file takes 6 seconds for transcription with SGX as compared to 3.5 seconds without SGX due to context switch in and out of enclaves.
- But we save one round trip time to the cloud as compared to the legacy cloud application.

Future Work

- Explore automatic code partitioning tools like Glamdring.
- Check for remote verifiability of untrusted components using software-based attestation tools like Pioneer.
- Compare performance of manual code partitioning using Intel SGX SDK with other tools like Graphene library OS and SCOME Docker containers that allow easy migration of legacy applications into SGX environment.

Acknowledgments

- Project advisor: Dr. Patrick Tague
- Project team members: Xincheng Wang, Nishchala Tangirala