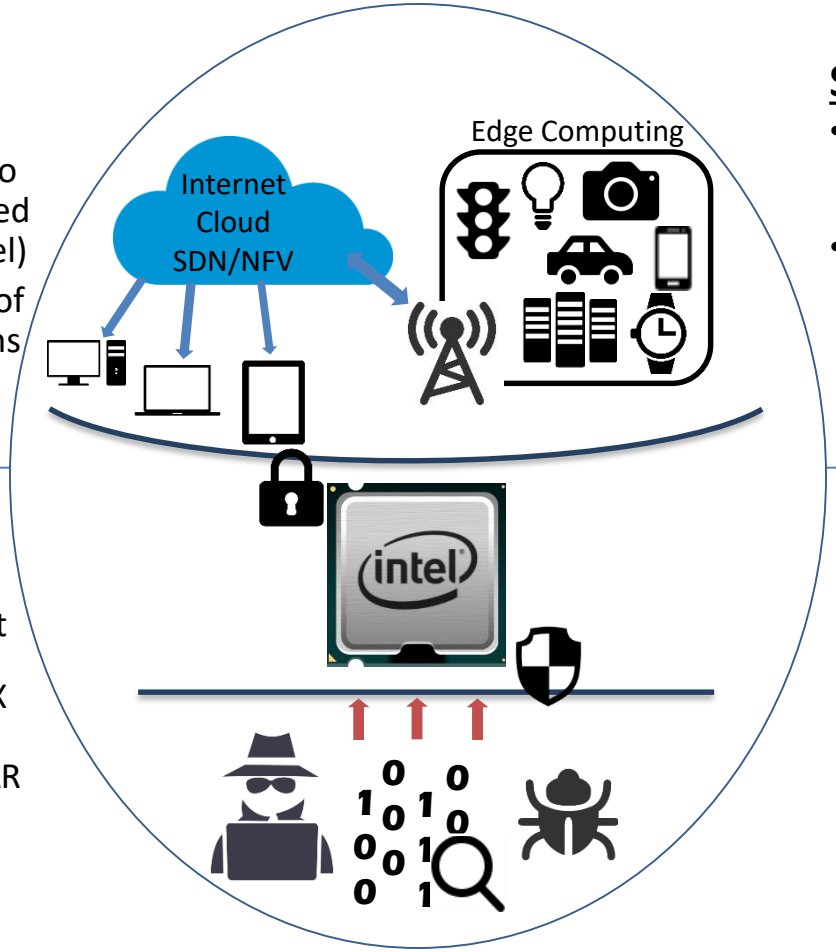
Secure Design of SGX Enclaves

Optionally, one university or project logo may go in this space. Delete this box!

Challenge:

- Intel SGX is vulnerable to attacks from an untrusted kernel (e.g., side channel)
- Intel SGX lacks support of self-defense mechanisms (e.g., ASLR)



Scientific Impact:

- Practical design of enclaves against known security threats
- Open source tools allows communities to easily use, evaluate, and extend

Solution:

- T-SGX
  Protect enclaves against page-fault side-channel attack by using Intel TSX
- SGX-Shield
  Enable fine-grained ASLR for enclaves

Broader Impact:

- Facilitate the adoption of SGX especially on cloud environment
- Enable rich SGX applications with stronger security guarantees
- Draw more attention from community to use SGX solve security problems

Project info (number, institution, contacts,...)