Securing IoT data using Blockchain

Jothi Arul Prakash, Nagendra Prasad, Sindhu

IoT

The **Internet of things** (**IoT**) is the network of devices, vehicles, and home appliances that contain electronics, software, actuators, and connectivity which allows these things to connect, interact and exchange data.

Blockchain

Blockchain is a series of blocks that contain data. It is a distributed ledger that is open to everyone, once data gets recorded in the blockchain it becomes very difficult to change it.

Challenges Facing IoT

- Jamming Attacks
- Sleep Deprivation Attacks
- Replay Attacks
- RPL Routing Attacks
- CoAP Security with the Internet
- Middleware Security
- Insecure Software/Firmware

Why Blockchain for IoT Security?

- Peer to Peer transactions
- Keep track of each transactions
- Avoid Intermediates
- Rewriting of history is nearly impossible.
- Decentralized nature

Aspects of Security

- Confidentiality
  - Cryptographic keys
  - Ledger keeps track of devices in chain
  - The Devices entering the chain must be authenticated

- Integrity
  - Decentralized distribution of Data
  - Transactions are irreversible
  - Attempt to data change in one block is impossible

- Availability
  - Each block have access to ledger
  - Local ledger can saved by each block
    - Improves rapid verification

Data and User Authentication

- Use of unique public key, GUID and smart contracts

Secure Communication

Challenges in Blockchain

- Consensus Mechanism can allow attackers to host a blockchain
- Cryptographic keys with limited randomness can be exploited