UNIVERSITY OF TURKU
Department of Future Technologies

ANUM NAWAZ: Secure IoT Devices using Ethereum Platform
Embedded Electronics
Master of Science in Technology Thesis, 65 p.
May 2018

---

Existing technologies plays a vital role in mitigating the IoT security risks. Our existing client server models are exactly the same we were using during the 80s and 70s. Vulnerabilities enforce us to look for some novel approach which can handle the explosive growth of data in Internet of things. At this stage, industry of IoT is running without any standards of software/hardware and awaiting for the big breakthrough in the existing network infrastructure. Nakamoto released the first version of bitcoin in 2009, which breeds the decentralized technology. Transparent and distributed structure of blockchain, shed new light on the evolution of IoT system. Existing hurdles which IoT industry is facing can be clear by developing new infrastructure on this distributed platform.

In this thesis, we present a novel approach to validate the integrity of data and communication of things by using Ethereum platform. This distributive ledger based platform provides transparency, trust and accountability in the world of IoT. Our research is divided into two main parts.

In the first part, we proposed a new model for the security of IoT device. We also discuss about the existing structures. Our designed model provides data Integrity, Gave control of data to its rightful owner, Improve AI through user data, Achieves authenticated communication b/w things, Immutability & Availability. We also achieve success in removing some major drawbacks of blockchain technology in IoT, we avoid the high consumption of electricity by choosing algorithm Proof of stake (PoS) as it doesn't require devices to do complex calculations, and we avoid the issue of large storage space by using the Light Ethereum client protocol (LEC/1) as it only requires the devices to save the hashes of all transactions instead of whole transaction. We used child key derivation function (ckd) to derive child public/private keys. To save data in an encrypted manner we use public key encryption.

In the second part, we implement our purposed model to check the validity of our purposed model. We create private Blockchain, Develop and deploy smart contracts, Develop front-end/back-end application interfaces by using MySQL database and Go Server. We use Raspberry pi as End Devices (miner node) and solidity simulator to check the simulations of smart contracts. The technology is very young and changing very speedily; to avoid disruptive surprises or missed opportunities we need to look forward very carefully.

Keywords: Ethereum, distributed technology, Ethereum into IoT, Blockchain for IoT, secure IoT devices, Personal ownership of data.