

Blockchain for IoT Security and Privacy: The Case Study of a Smart Home

Group 6 - Lukas Merli, Serdar Öztürk, Katja Root

Introduction

Internet of Things (IoT) consists of devices that deal with vast amounts of security- and safety-critical data as well as privacy-sensitive information, and hence are appealing targets of various cyber attack

- IoT demands a security and privacy safeguard, which is lightweight, scalable, and distributed
- The Blockchain technology that underpins a Bitcoin system, has the potential to overcome these challenges - the previous approach was exemplified in a smart home setting and consists of three main tiers: cloud storage, overlay, and smart home. - Here: outline the various core components and functions of the smart home tier

Core Components of Smart Home

- Transactions = communications between local devices or overlay nodes
 - Different Types: store transaction(to store data), access transaction (to access the cloud storage), monitor transaction (to periodically monitoring a device information), genesis transaction (to adding a new device to the smart home) and remove transaction (to remove a device)
 - All of these transactions use a shared key to secure the communication
 - All transactions to or from the smart home are stored in a local private BlockChain
- Local Blockchains
 - In each smart home, there is a local private BlockChain that keeps track of transactions and has a policy header to enforce users' policy for incoming and outgoing transactions
 - Each block in the local BlockChain contains two headers: block header and policy header
 - The block header has the hash of the previous block to keep the BlockChain immutable
 - The policy header is used for authorizing devices and enforcing owner's control policy over his home
 - Besides the headers, each block contains a number of transactions with different parameters

Core Components of Smart Home

- Home Miner
 - Smart home miner is a device that centrally processes incoming and outgoing transactions to and from the smart home
 - Similar to existing central security devices, the miner authenticates, authorizes, and audits transactions.
 - The miner collects all transactions into a block and appends the full block to the BlockChain
- Local Storage
 - Local storage is a storing device e.g. backup drive that is used by devices to store data locally
 - This storage can be integrated with the miner or it can be a separate device

The BC-Based Smart Home

In This part we have three important points

- Initialization
 - describe the process of adding devices and policy header to the local BC
- Transaction Handling
 - smart devices may communicate directly with each other or with entities external to the smart home
- Shared overlay
 - if more than one home à than separate miners and storage

Security Analysis

1. Security Requirements Analysis

- a. Confidentiality (only authorized user is able to read the message)
- b. Integrity (message is received without any change)
- c. Availability (service or data is available when needed)
- d. User control
- e. Authorization

Requirement	Employed Safeguard
Confidentiality	Achieved using symmetric encryption.
Integrity	Hashing is employed to achieve integrity.
Availability	Achieved by limiting acceptable transactions by devices and the miner.
User control	Achieved by logging transactions in local BC.
Authorization	Achieved by using a policy header and shared keys.

Performance Evaluation

1. Simulated flow patterns

- a. Periodic (Devices send their data to the cloud periodically e.g thermostat)
- b. Query-based (Device sends data on-demand equivalent to storing data to the cloud by home owner)

2. Evaluated Metrics

- a. Packet overhead (length of the transmitted packets)
- b. Time overhead (processing time for each transaction from miner to requester)
- c. Energy consumption (energy consumed by the miner for handling transactions)

Evaluation Packet overhead

Packet Flow	Base (Bytes)	BC-based (Bytes)
From devices to the miner	5	16
From the miner to the cloud	5	36
From the cloud to the miner	5	16

Using encryption and hashing increases the packets payload size compared to Base Methode

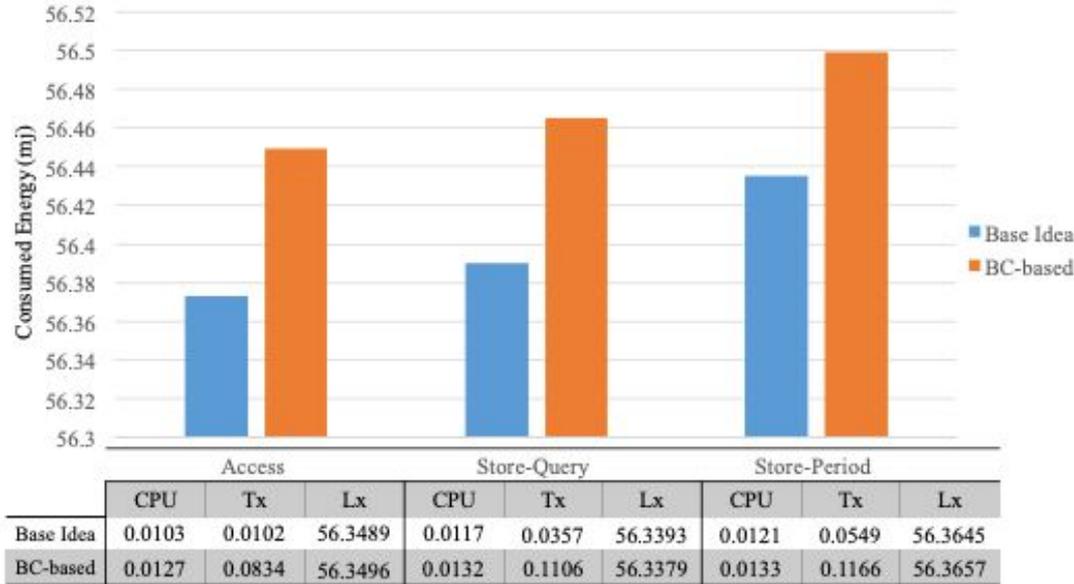
Evaluation Time overhead



Fig. 3. Evaluation of time overhead.

The BC-based design consumes more time to process packets compared to the base method which can be attributed to the additional encryption and hashing operations.

Evaluation Energy consumption



Due to the encrypting and hashing operations the BC-Based consumes more energy, but in summary, the low overheads introduced by our BC-based method significantly outweigh given the significant security and privacy benefits on offer.