Leveraging Blockchain for IoT Access Management

Ujjwal Nadhani Russell Tapia Dr. Gaby G. Dagher Praneeth Babu Marella

BOISE STATE UNIVERSITY

Blockchain REU 2022

Introduction

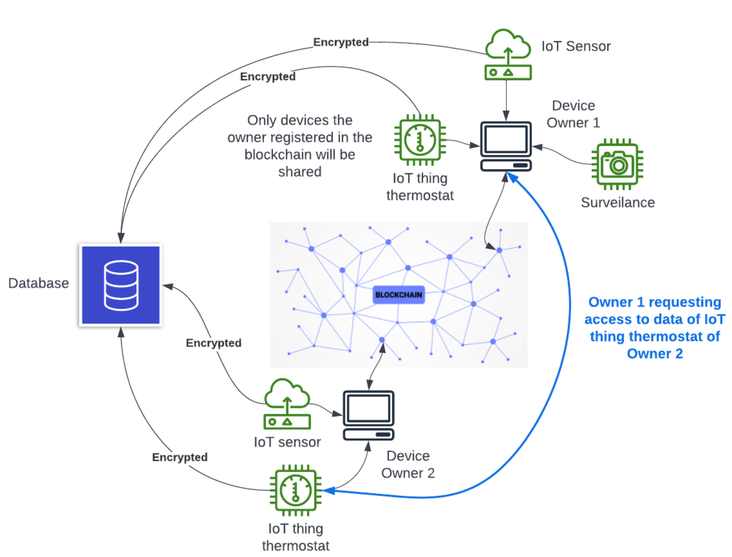

Figure 1. Blockchain based IoT Access Management.

Abstract

In 2022 on average there are about 16 Internet-of-Things(IoT) devices per household. Since these IoT devices have the capability of connecting to the internet, there is also opportunity of collecting data using these IoT devices. **Assuming some of these data are insensitive and the owner is willing to share them,** there is an opportunity to gather more data than what one owner is capable of gathering on his/her own. One example of this is pretend each house in a city have a soil moisture sensor. If there is a way to gather all the data that each soil moisture sensor in the city have collected. Then you have a picture of the water content in the soil in the whole city, instead of just one small area where your soil moisture sensor is. On the other hand you can do the alternative, buy enough soil moisture sensor to cover the whole city (assuming you are trying to get the water content of the soil in the whole city).

Using blockchain for access management of shared IoT devices, we can have a transparent record of who have utilized access of specific IoT devices. With the reputation based system the users are incentivesed to share their data as much as possible. Sharing valid data and participating in data validation awards device owners with more reputation. The higher the device owner's reputation the more device data he/she can access. By encrypting device data in the database the systems guarantee that data has not been tampered with. To compensate for the limitations of IoT devices, IoT devices will only handle encryption of the data they have collected and have an off-chain database that stores all the encrypted data.

Background

1. **Blockchain**, the most popular application of blockchain is in cryptocurrency like Bitcoin or Ethereum. In its simplest explanation, blockchain really is a digital record of transactions that is kept in a network of computers. The traditional way of keeping records(data) is to keep it in one database, normally a server, making data or assets centralised. In blockchain, since data are stored in a network of computers, blockchain is considered **decentralised** or **distributed**. This property of blockchain makes data **transparent** to everyone in the network. Along with transparency, blockchain is also hard to change, **immutable**.
2. **IoT devices**. Devices that have internet connectivity capability.
3. **Permissionless Blockchain**. There are two types authorization to make a transaction in the blockchain. Permissioned requires predetermined authorised entity to make a transaction in the blockchain. Permissionless allows anyone that is in the blockchain to make a transaction. In our system we are using permissionIless authorization.
4. **Nodes**. Computers in the blockchain network. In this case they are the device owners.
5. **Requestor**. Device owners that are requesting access to IoT device in the network that is not their own.
6. **Smart contract**. A programming algorithm that executes when invoked.
7. **Off-chain Database**. The database that will be storing the encrypted data of all the IoT devices.

Contribution

- Introduced a **Blockchain-based IoT Access Management** to automate access to shared IoT device data.
- Introduced a secure **permissionless reputation based authentication** to streamline access to shared IoT devices.
- Altogether the system is a **lightweight solution** for a secure and transparent device or data sharing network.

Solution

Our system is streamlined data sharing network with minimal data owner interaction. To remove the owner from having to manually give access to the data the requestor is requesting, the system uses blockchain technology. The system uses smart contract to instantiate the transaction for accessing the data that is being requested by the requestor. To gain access to the data of a specific IoT device in the blockchain network the requestor creates a request.

The following are the steps when a request is made.

1. **Verify**
   - The system verify that the device exist in the network.
   - The system verify that the requestors reputation $\geq$ device reputation requirement.
2. **Validators**. The system will collect node volunteers to be validators.
3. **Validation of data**. Validators download classifier and new data set to.
   - Verifies the correctness of the classifier.
   - Run data set on classifier.
4. **Consensus**. Validators agreed and sign a transaction and propagate in the network the data key.
5. **Accept**. Nodes in the network will accept the transaction if $(1 - \alpha)$ signatures from IoT approved validators. α being the probability that the node is malicious.
6. **Decrypt**. Requestor decrypts data key and use it to decrypt requested data set.

Solution cont.

Reputation calculation = normalised to a score of 100

Spending

- For every data shared the owner can request three data.

Award

- Sharing data gives 40 reputation scores.
- Validation gives 20 reputation scores.

Penalty

- Malicious activity will deduct 40 reputation scores.
- Inactivity will deduct 10 reputation scores.

Test

Using basic **hyper distribution formula**

$$h(x; N, n, k) = [{}_kC_x][{}_{N-k}C_{n-x}]/[{}_NC_n]$$

$$h(3; 1000, 20, 150) = [{}_{150}C_3][{}_{850}C_{17}]/[{}_{1000}C_{20}]$$

$$h(3; 1000, 20, 150) = 24\%$$

- N = 1000; number of nodes in the network.
- k = 150; number of bad actors in the network. We are assuming that there will be 15% of malicious actors in the network, which is excessive.
- n = 20; number of selected validators.
- x = 3; number of bad actors per selected validators. We are assuming that there will be 15% of bad validators, which is excessive.

Conclusion

As the diversity of IoT devices expands, IoT devices not only allow automation of some processes but also allow for the ability to collect data for those processes. Combining IoT and blockchain technology there is a possibility where we can trade data (just the ones we want to share) with other IoT device owners giving us the ability to gain more data samples than we can normally have on our own. To be able to share data collected by our IoT devices, we have to give access of our IoT device to other IoT device owners. For a transparent, secure and ultimately self-correcting shared access to IoT devices we use blockchain technology in our system, creating a network of device owners that are willing to share their collected data. Making sure that participants are acting correctly by using a reputation based authority. Using basic hypergeometric distribution formula assuming that there are 15% of bad actors in the network after the system have picked validators there is a 24% chance of getting 15% of the validators are malicious.

In conclusion, using blockchain there is a possibility of collectively maximizing the benefit and use of IoT devices if owners are willing to share them with one another