Report on

**BLOCKCHAIN BASED SYBIL-SECURED SIMULATOR FOR IOT ENVIRONMENT**

(minor project)

Submitted by

Akhilesh Dodla (1606062)

Sai Chandra K (1606094)

Deeraj Reddy K (1606097)



**A report submitted in partial fulfilment for the degree of Bachelor of Technology in Computer Science & Engineering.**

Under the guidance of

**Dr. Ditipriya Sinha**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

NATIONAL INSTITUTE OF TECHNOLOGY PATNA

JUL-DEC, 2019.

**राष्ट्रीय प्रौद्योगिकी संस्थान पटना**

**NATIONAL INSTITUTE OF TECHNOLOGY PATNA**

**(An Institute of National Importance under MHRD, Govt. of India)**

**ASHOK RAJ PATH, PATNA – 800005 (BIHAR)**

# **CERTIFICATE**

This to certify that the project entitled “Blockchain based sybil-secured simulator for IoT environment” submitted by Akhilesh Dodla (1606062), Sai Chandra K (1606094) and Deeraj Reddy K (1606097) in partial fulfilment of the requirements for the award of Bachelor of Technology degree in Computer Science and Engineering at the National Institute of Technology Patna is an authenticate work carried out by them under my supervision and guidance.

To the best of my knowledge, the matter embodied in the project has not been submitted to any other university/institute for the award of any degree or diploma.

## 

## ……………………

## **Dr. Ditipriya Sinha**

## **(Supervisor)**

……………………

**Dr. Jyoti Prakash Singh**

**(Head of Department, CSE)**

Date: ………………….

Place: …………………

## **DECLARATION**

We students of 7th semester hereby declare this project entitled “Blockchain based sybil-secured simulator for IoT environment” has been carried out by us in the department of Computer Science and Engineering of National Institute of Technology Patna under the guidance of Dr. Ditipriya Sinha, Department of Computer Science and Engineering, NIT Patna. No part of this work has been submitted to any other institute nor copied from any journals or articles or project reports.

**Akhilesh Dodla -1606062**

**Sai Chandra K -1606094**

**Deeraj Reddy K -1606097**

Date: ………………….

Place: …………………

# **ACKNOWLEDGEMENT**

We would like to take this opportunity to thank all our sources of aspiration during the course of this project.

First and foremost, we are grateful to Dr. Ditipriya Sinha ma’am, who gave an opportunity to work on a research-based project “Blockchain based sybil-secured simulator for IoT environment” and for her continuous support during the project and for her patience, motivation and immense knowledge. She helped us come up with project topic and guided us over almost a semester of development. And during the most difficult time when writing this report, she gave us the moral support and the freedom to move on.

We are really grateful to Dr. Jyoti Prakash Singh (H.O.D., Dept. of Computer Science and Engineering, NIT Patna) who provided us with a helping hand by allowing us to undergo this interesting learning experience and has always been a source of inspiration for us.

We therefore take the benefit to offer our thanks to every one of the general populations who straight forwardly or by implication associated with the execution of this work, without whom this project would not have been a triumph.

Then we would like to thank our project team member for their kind cooperation, help and never-ending support.

We are also thankful to NIT Patna for providing us technical skills and facilities which proved to be very useful for our project.

**Akhilesh Dodla -1606062**

**Sai Chandra K -1606094**

**Deeraj Reddy K -1606097**

**CONTENT**

List of figures.……………………………………………………………………………………

1. Introduction……………………………………………………………………………………
2. Problem Statement ……………………………………………………………………………
3. Implementation ……………………………………………………………………………….

3.1 Device setup phase ………………………………………………………………………

3.2 Dual identity validation……………………………………………………………………

3.3 Secure data transmission…………………………………………………………………..

3.4 Encoding mechanisms…………………………………………………………………….

1. Results…………………………………………………………………………………………
2. Related Work………………………………………………………………………………….
3. Conclusion…………………………………………………………………………………….

Reference…………………………………………………………………………………………

**List of Figures**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.no** | | **Name** | **Page no.** |
| **1.** | | Structure of blockchain | 7 |
| **2.** | 2.1 | After several valid transactions | 12 |
| 2.2(a) | An outside device which is not in the network | 12 |
| 2.2(b) | Acknowledgment for untrusted transaction | 12 |

1. **INTRODUCTION**

**1.0 Internet of Things (IoT):**

The **Internet of Things** (**IoT**) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

It consists of devices that generate, process, and exchange vast amounts of security and safety critical data as well as privacy-sensitive information, and hence are appealing targets of various cyber-attacks. Many new networkable devices, which constitute the IoT, are low energy and lightweight. These devices must devote most of their available energy and computation to executing core application functionality, making the task of affordably supporting security and privacy quite challenging.

**Applications:**

**Smart Home**: IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media and security systems. Long-term benefits could include energy savings by automatically ensuring lights and electronics are turned off. A smart home or automated home could be based on a platform or hubs that control smart devices and appliances. For instance, using Apple's Home Kit, manufacturers can have their home products and accessories controlled by an application in iOS devices such as the iPhone and the Apple Watch. This could be a dedicated app or iOS native applications such as Siri.

**Medical and healthcare:**The Internet of Medical Things (IoMT), (also called the Internet of health things), is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring. The IoMT has been referenced as "*Smart Healthcare*", as the technology for creating a digitised healthcare system, connecting available medical resources and healthcare services. IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialised implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids.

**1.1 Blockchain:**

A **blockchain**, originally **block chain**, was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications, and blockchains that are readable by the public are widely used by cryptocurrencies.

A blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

**Structure of blockchain:**

By design it is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp and transaction data (generally represented as a Merkle tree). The following figure represents a general structure of blockchain.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Previous Hash |  | Previous Hash |  | Previous Hash |
| Timestamp | Timestamp |  | Timestamp |
| Transactions  (Merkle root) | Transactions  (Merkle root) |  | Transactions  (Merkle root) |
| Nonce | Nonce |  | Nonce |
| Block hash | Block hash |  | Block hash |

**Fig 1. Structure of blockchain**

1. **PROBLEM STATEMENT**

Since these IoT devices exchange vast amount of data among themselves over the internet, they should be in a secured environment such that attackers shouldn’t be able to attack the network. Traditional security methods tend to be expensive for IoT in terms of energy consumption and processing overhead. Moreover, many of the state-of-the art security frameworks are highly centralized and are thus not necessarily well-suited for IoT due to the difficulty of scale, many-to-one nature of the traffic, and single point of failure. To protect user privacy, existing methods often either reveal noisy data or incomplete data, which may potentially hinder some IoT applications from offering personalised services. Consequently, IoT demands a lightweight, scalable, and distributed security and privacy safeguard.

So, to provide the above-mentioned necessities, we have used the blockchain technology for the IoT network to establish a well secured, ease of use methodology to overcome any sybil attacks.

1. **IMPLEMENTATION**

Proposed solution depicts a Blockchain-based Sybil secured IoT framework to address the first two listed research challenges and an alternative consensus algorithm “Proof-of-Confidence” to address the other listed research challenges.

There are 3 stages to completely enable the mentioned IoT framework:

**1.Device setup phase**

**2.Dual identity validation**

**3. Secure data transmission**

**3.1 Device setup phase:**

In this section, we describe the process of adding devices and policy header to the local BC. To add a device to the smart home, the miner generates a genesis transaction by sharing a key with the device. The shared key between the miner and the device is stored in the genesis transaction. As for defining policy header, the home owner generates its own policies according to our proposed policy structure and adds the policy header to the first block.

First, we give the number of devices so that it creates a public/private key pair for the devices. Later each device is made to do a genesis transaction with the central HUB.

Thus, every valid device which is added to the network should do a genesis transaction so that later in the data transmission phase its identity gets verified. The Identity of a device is created only when it makes a genesis transaction with the hub.

**3.2 Dual identity validation:**

As mentioned above, once the ID is created it can do further data transmissions within the network. The ID is created using the following attributes:

1. Block Number
2. Block Hash
3. Difficulty target
4. Node ID
5. Public key
6. **Block Number:**

In the initial device setup phase, as mentioned each device makes a genesis transaction with the network hub (device 0).

Each transaction in the setup phase creates a new block and adds it to the blockchain network. The Block Number is said to be ***i*** if it is reasonable to create the ***ith*** block in the blockchain.

1. **Block Hash:**

The block hash attribute of the device is the hash of that corresponding block which is created while doing the genesis transaction.

1. **Difficulty target:**

The difficulty is a number that regulates how long it takes for miners to add new blocks of transactions to the blockchain. Generally, this difficulty value updates every 2 weeks to ensure that it takes 10 minutes (on average) to add a new block to the blockchain. But in our project, we have set a constant difficulty target of 3.

1. **Node ID:**

Node ID is defined as a unique string that is generated using HMAC algorithm which takes Block hash and Transaction Index as the inputs.

**HMAC**: In cryptography, an HMAC (key-Hashed Message Authentic Code) is a specific type of message authentication code involving a cryptographic hash function and a secret cryptographic key. It may be used to simultaneously verify both the data integrity and the authenticity of a message, as with any MAC.

1. **Public Key:**

This is the public of the device which is created in the initial setup phase.

* 1. **Secure data transmission**

This is the final stage where the network is ready to transmit data from one to another. A transaction (data which is being transferred) is considered to be valid only if the ID of the sender and the receiver is verified, and then a valid signature of the sender is authenticated.

If the ID is not verified or the signature is not authentic, the transaction is said to be invalid and discarded immediately.

Furthermore, a block has a limitation of number of transactions to be held. In our project, we have set the limit to **6** i.e. a block is created for every 6 **valid** transactions.

* 1. **Encoding mechanisms**

**Merkle Root:**

In cryptography and computer science, a hash tree or Merkle tree is a tree in which every leaf node is labelled with the hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes.

**PKCS1\_v1\_5 verification:**

In cryptography, **PKCS #1** is the first of a family of standards called Public-Key Cryptography Standards (PKCS), published by RSA Laboratories. It provides the basic definitions of and recommendations for implementing the RSA algorithm for public-key cryptography. It defines the mathematical properties of public and private keys, primitive operations for encryption and signatures and various secure cryptographic schemes.

**AES:**

The **Advanced Encryption Standard** (**AES**), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AES is a subset of the Rijndael block cipherdeveloped by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposalto NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.

1. **RESULTS**

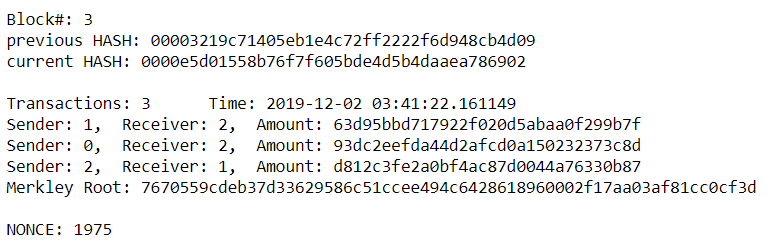


Fig 2.1. After several valid transactions

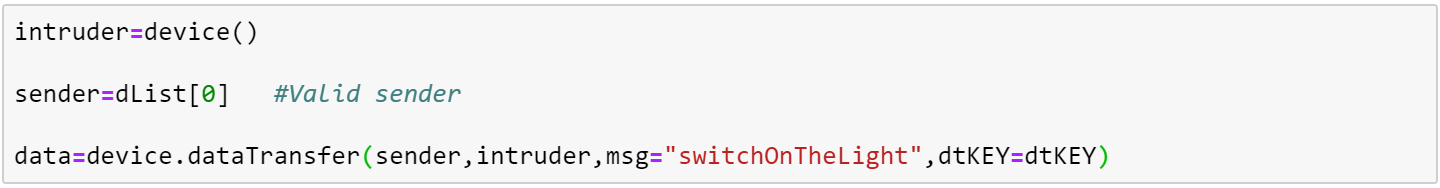


Fig 2.2(a). An outside device which is not in the network

If we try to send any command to a device in the network from a new device, Since the new device did not make genesis transaction with the network HUB, it does not have a valid ID, and hence the transaction is discarded. Shown in below figure.

Fig 2.2(b). Acknowledgment for untrusted transaction

1. **RELATED WORK**

There exist different studies on security and privacy of IoT and smart home. Authors in [4] demonstrated that off-the-shelf IoT devices lack basic security safeguards by hacking into a variety of smart home device including a light bulb, switch and smoke alarm. Authors in [5] argued that the smart homes are vulnerable to attacks conducted by users’ smartphones even if the home gateway controls the exchange of packets to and from the home. Authors in [3] proposed a method with three modules to protect users’ privacy in the smart home. The data collector module collects users’ data from the smart home and sends them to data receiver module that stores data in two different datasets. The result module controls the user’s access to data to protect the privacy. This method ensures that only the true user can access data. Besides, by using two datasets it is guaranteed that linking different data of a user to each other is impossible. However, the method does not provide privacy when the user needs to reveal his data to a service provider.

1. **CONCLUSION**

IoT security is gaining a lot of attention these days from both academia and industry. Existing security solutions are not necessarily suited for IoT due to high energy consumption and processing overhead. We previously proposed a method that addresses these challenges by leveraging the Bitcoin BC, which is an immutable ledger of blocks. The idea was discussed using a smart home as a representative case-study. In this paper, we outlined the various core components of the smart home tier and discussed the various transactions and procedures associated with it. We also presented an all-inclusive analysis regarding its security and privacy.

**REFERENCES**

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in internet of things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015.

[2] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.

[3] A. Chakravorty, T. Wlodarczyk, and C. Rong, “Privacy preserving data analytics for smart homes,” in Security and Privacy Workshops (SPW), 2013 IEEE. IEEE, 2013, pp. 23–27.

[4] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, “An experimental study of security and privacy risks with emerging household appliances,” in Communications and Network Security (CNS), 2014 IEEE Conference on. IEEE, 2014, pp. 79–84.

[5] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, “Smart-phones attacking smart-homes,” in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2016, pp. 195–200.