

Secured Internet of things (IoT) Model using Blockchain

ABDUL MUNEEM KHAN¹, FUAD HOSSAIN ONI¹, JABED OMAR¹,
MD. ABDULLAH AL NOMAN¹, MD. BORHAN UZ JAMIL¹, DR. MUHAMMAD IQBAL HOSSAIN¹

Software Engineering, Department of Computer Science and Engineering, Brac University, Bangladesh
E-MAIL: {abdul.muneem.khan, fuad.hossain.oni, jabed.omar, md.abdullah.al.noman, md.borhan.uz.jamil}@g.bracu.ac.bd,
iqbal.hossain@bracu.ac.bd

Abstract:

Anything which is connected to the internet is prone to threats. The internet has a saying that, "There are two types of hacked devices. One which is hacked, and the other one is which does not know that it is hacked". Security and privacy of valuable data have been a major issue over decades. Researches based on IoT device security is going around for quite a good time in this era and still has many scopes to build a more secure, data, and privacy protected IoT system. As beneficial as internet-connected devices are, they create some significant challenges. While we assume that these devices are protected with the same security level as the typical network server, it is not the case. IoT devices present some major security concerns, which we will talk about in broad. Blockchains can be a solution for securing IoT devices. Blockchain is a cryptographically secured, distributed ledger technology that allows for secure data transfer between parties. Blockchain is surely one of the promising and revolutionary technologies of this era because it reduces risk, stamps out fraud, and brings transparency in a scalable way for many uses.

Keywords:

IoT; Blockchain; Ethereum; Security; IoT Security; Mining; Proof of Work; Smart Contract; Cryptography; Hash Functions, SHA256

I. Introduction

The world is getting smaller and smaller in terms of connectivity. Thanks to the internet, everything is now connected. From the smartwatch in our hands to the fridge in our home, everything can be controlled by the internet now. The Internet of Things can be connected to the internet and can communicate with other internet-connected devices. As the internet of things can communicate with each other, sensitive data might be easily breached via a miscommunication or other means. IoT security is a much-underrated topic, which is becoming very important day by day. Blockchain is a digital ledger technology that

ensures integrity and can be used in various fields. Blockchain uses a linked list like data structure but uses cryptocurrency and many other techniques to keep chain data secure. Blockchain is the most transparent and immutable or unchangeable way to store data to date.

Nothing is done until we can feel the actual need for it. From our months of research, we have found out that though IoT will take over the world, there are some obstacles. Almost in all the papers, security was a major concern where protecting privacy has become an alarming issue. Moreover, in different layers of any system, we have got that the network layer is most under threat. As everything is connected to the internet, so it has become really easy to invade it, which is a major security concern. Preventing these kinds of invasions became our major motivation for what we started to think of something that could stop such threats. After researching and comparing for a while, we found out that blockchain is the most convincing way to do that. In the future decades, blockchain will surely play a major role to secure IoT based applications. Therefore, securing the IoT devices, protecting user's privacy, and preventing invaders from controlling the device are our major motivations behind using blockchain to secure IoT based systems.

After the invention of IoT, its rapid growth of using clearly says how the world is being dependent on it day by day. For the increasing rate of IoT now, security has become the most concern issue for us. Millions of data are generated on the world by these devices in each second and stored in a centralized server for simplicity. In contrast, this method can be vulnerable because of IoT connectivity with many devices. Insecure home thermostats, hacked baby monitors, Hackable medical devices, hacked autonomous cars, etc. are examples of real-life problems that we can face if IoT data gets breached. [7] We have discussed blockchain technology is the most secure technology till now. Still, we could not find any proper system where blockchain is

implemented in IoT and made IoT more secured. We want to develop a model where blockchain can be used in IoT devices and make IoT data fully secured so that we don't have to suffer like the problems stated above.

Blockchain technology is currently one of the best technologies we have to keep our data secured and maintain privacy. To get or manipulate the stored data from a blockchain, a hacker would have to control and manipulate the data stored on every user's computer in the blockchain network or make a 51% attack. [9] There could be hundreds or thousands of computers, with each one saving a copy of a portion of blockchain data or all of the data. So, the hacker has to simultaneously bring down an entire network to take control of a blockchain, Blockchain would continue running to verify and record all the data on the network. The possibility of taking down a whole chain decreases along with the number of users on a network. This complex configuration gives blockchain technology the ability to be known as the most secure form of storing and sharing information online maintaining confidentiality and integrity. The IoT sector is one of the most fast-growing sectors in the IT industry, generating huge data. A centralized IoT system usually has a server or a cloud where the data are saved and fetched from. In a decentralized system, there is no need for a centralized server as they are already inter-connected. Data generated from these IoT devices can be hazardous in the wrong person's hand. Still, securing IoT data is an important thing we often forget. We propose a model that merges blockchain technology with IoT devices to ensure user data safety and prevent stealing or compromising data.

II. Literature Review

According to a research paper [1], IoT is typically structured into 3 basic Layers. And they are the Application layer, Network layer, and Physical layer. The physical layer can face Node Tampering, RF interface, Node jamming, Malicious node injection, Physical damage, Social engineering, Sleep deprivation attack, etc. The network layer is hampered by Traffic analysis attacks, RFID spoofing, RFID cloning, Sinkhole attack, Man in the middle attack, DOS, DDOS, Sybil attack, etc. And in the application layer, there are several attacks like viruses and worms, Spywares, Adware, Malware, Trojan horse, DOS, etc. They also stated some layer-wise mitigations to be safe from those threats. The secure boot of IoT devices, Device authentication using low power techniques, ensuring data confidentiality, and maintaining data anonymity can safeguard us in the physical layer or IoT devices. For the network layer, securing communication between the devices, implementing routing security,

and securing user data on the device is mentioned in the paper to counter-attack incoming threats. Lastly, data security, ACLs, Firewalls, and protective software like antivirus or anti-adware can prevent threats in the application layer. Finally, regardless of any layer, there are some suggestions to counter-attack threats in all layers which are, finding new threats, applying updates and patches, providing improvements, upgrading systems, using IDS (Intrusion Detection System) in the device, Securing IoT physical premises, monitoring devices, Trust management, etc.

In another research paper, [4] Sensor-based threats in IoT devices can be categorized into four broad categories based on the purpose and nature of the threats: Information Leakage, Transmitting Malicious Sensor Patterns or Commands, False Sensor Data Injection, and Denial-of-Service. Information leakage can be divided into few parts such as Keystroke Inference using Light Sensors, Motion Sensors, Audio Sensors, Video Sensors, Magnetic Sensors, Task Inference using Magnetic Sensors, Power Analysis, Location Inference, and Eavesdropping. Transmitting of Malicious Sensor Patterns or Commands can occur via Light Sensors, Magnetic Sensors, Audio Sensors. It also explained some existing security mechanisms to prevent sensor-based threats like Enhancing Existing Sensor Management Systems and Protecting Sensed Data. They provided some excellent future scope of their research, which included Study of Expected Functionality to Identify Threats, Control Sharing of Data among Sensors, Protect Sensor Data when at Rest, Prevent Leakage of Secret Data, Protect Integrity of Sensor Operations, and Adoption of Intrusion Mechanisms to Detect Attacks.

In a study [2], with and without using blockchain an IoT system is supposed to be developed and then make a comparison between two of the systems. MQTT is used as a communication protocol in the IoT system without the blockchain technology. On the other hand, the system developed with blockchain technology has used Ethereum combined with a smart contract. Both the IoT systems are supposed to be analyzed and tested for their safety level by perceiving their safety aspects and simulating attacks. The result was crystal clear as the IoT system designed with blockchain technology has a higher level of security than the IoT system designed without the blockchain technology. In recent years, the development of IoT technology has increased at a huge rate but has gone along with security problems. The insecurity of communication that happens between IoT devices is one of the common security issues that arise. In this particular research, the design and building up of the IoT system have been conducted with and without using blockchain technology to check and compare the results of the test and experiments.

Like the previous paper, Ethereum is used as the field of a blockchain network in the IoT system. Along with the Ethereum to store and retrieve necessary information from the blockchain network, smart contracts are used as well. Calculating and checking all the results of various tests can prove that the IoT system developed using blockchain technology can prevent security threats that are seemed in communication between IoT devices as it has a higher level of safety measures than the IoT system developed without using blockchain technology. So by using blockchain technology in IoT systems data integrity can be well guaranteed. This can be observed and verified from testing of attack simulations and monetization of avalanche effects accomplished where the application of blockchain technology has better security in the IoT system.

IoT technology is mostly used for a smart home system, but there is some obstacle regarding the security issue of data. One of the information that should be secure is the entryway/door lock information access. This information should not be defenseless against duplicating and hacking because an entryway/door is sincerely identified with the security of the property holder. Door lock access information can be utilized to discover who and when somebody is in or out of the house. Hence, we can expand home security if something doubtful occurs. One paper, [6] proposed a door lock system that will be secured by the Ethereum blockchain. Moreover, some other researchers mentioned the same kind of framework. For ensuring who will enter or exit from the house the proposed door lock system used a webcam to do face recognition. Webcam catches the face before it. At that point, the webcam will perceive the face, if it is enrolled. On the off chance that the face is as of now enlisted as the proprietor of access rights, the situation will check whether the webcam is enrolled on the blockchain network or not. The paper also clarifies transaction handling, which is using smart contracts to set methods made by the property holders. On the private blockchain, a miner is pre-selected to keep up the blockchain network. All the transaction data of the door lock system will be stored in a private blockchain. The proposed framework design comprises of nodes (webcam and mortgage holder), a miner, and a private blockchain, which is Ethereum blockchain, alongside the smart contract. The paper also shows the experimental results which were performed on the system, and there was some significant success as well.

The authors of a paper [5] were seemed to take benefit of the distributed quality of blockchains to set up a huge IoT control system and they prioritized smart contract-based tokens to implement a better access control mechanism. Keeping that

under consideration they constructed a blockchain-based system that permits users to run and control IoT devices arranged in “groups” (e.g., turn on the lights of a smart city). This system is constructed using the Ethereum blockchain, takes the limitations under consideration and capabilities of the IoT devices, and also the required items of the blockchain technology. They built a blockchain-based IoT design-oriented system on presently available technologies and defined its users and their internal communication where they build, implement, and verify an event-oriented IoT management solution dependent on Ethereum smart contracts.

III. Proposed Model

In most of the IoT network, the devices which need to be connected to that device are known to us. For example, if we have a smart air conditioner, it will be connected to our thermostat to sense the temperature and control the air conditioner depending on that data; or if we have a smart water motor system in the reserve tank, the motor will be connected to some depth sensor in our water tank which will send a signal to turn the motor on or off. Our model will be a blockchain-based IoT model, there will not be any centralized server in it. Every device will be running a private and local blockchain instance which is by definition not accessible outside of the network and possibly the most secure system till now in terms of immutability. Each device will be called nodes. So, each device will have a unique Ethereum address. Also, Every IoT devices should be inter-connected by a peer to peer connection manually. We will store the Ethereum addresses of those devices on a smart contract, which we know that our node or device needs to be connected with to function, in the blockchain instance. In our system, devices or nodes which are not enlisted in our smart contract shall not be communicated by the nodes on our blockchain. This will ensure security from malicious attacks or commands to IoT devices. Features of our model are the following:

- 1) Only the Ethereum account owner on the device shall be able to add or delete a device to the blockchain network. We shall call the owner, 'Home miner'. In other words, only our home miner shall be able to add or delete nodes in the chain; thus, only the home miner can decide whether that particular node can communicate with another particular node or not.
- 2) We will use a local private Ethereum blockchain for implementing our system. Ethereum system has to be installed on all of the IoT devices which want to use this secured model.

- 3) 3 types of requests can be done by the home miner in our system. Add a device, delete a device, and the other is to check connectivity. As the name suggests, add or delete is requested to add or delete a new device on the network, which is only valid if our home miner requests.
- 4) Regardless of which request a device sends, it has to send a valid Ethereum account address to add or delete or check connectivity as well as any random message with the request. The message and the Ethereum address of the requester generates a signature that is encrypted, and our system gets the signature and the hashed message as soon as the requester sends the message. Now our smart contract shall decrypt the signature and will get the Ethereum address of the sender.
- 5) Our system already knows the Ethereum address of our home miner. If any other node sends add or delete requests rather than our home miner, the system will not allow the request and submit a transaction containing the possible intrusion. If our home miner sends the request, then that address shall be checked for validity to add or delete and will simply be added or deleted from the network, and a transaction containing the address and information regarding the device shall be stored in the blockchain.
- 6) Check connectivity request is made when our home miner tries to check if another device is connected to our network or not. In other words, when an IoT device wants to know whether it will communicate to another IoT device holding the provided Ethereum address or not, it sends a connectivity check request. For this particular request, the smart contract first checks the requester's account address. If the address is matched with our home miner, that means the request is valid and our home miner wants to know if the address it sent should be communicated with or not. Then our smart contract checks if the requested address is enlisted in our list or not and sends the result true or false thereby. But if the sender is not our miner, that means someone from outside is trying to access our system, then the system will count this as an intrusion and take the provided steps.
- 7) The verification of the home miner is done using Elliptic-curve cryptography. It is a widely known algorithm to verify digital signatures [10]. Elliptic-curve cryptography (ECC) is public-key cryptography which is based on the algebraic structure of elliptic curves over finite fields. This method verifies the signature of a sender by using the public key. The signature can only be generated using the sender's private key.

Our model shall be a combination of IoT and Blockchain,

which shall provide more secure communication between IoT devices. We have proposed and implemented the Blockchain part but this blockchain-based model needs to be implemented on the network layer or add a blockchain layer after the network layer of IoT architecture to provide security. It can be implemented in such a way that if an IoT device requests to communicate with another IoT device, the 2nd device shall check connectivity before actually communicating with the first device. If the first device is permitted to communicate or in other words, the address of that device exists on the connected device list, only then the second device will communicate with the first device.

A flow chart defining the basic functionality of our proposed model is given in figure 1-3 below:

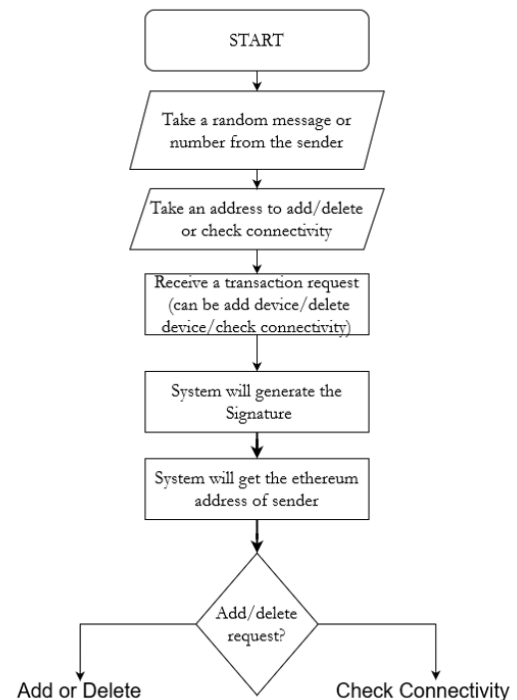


FIGURE 1. Flowchart for Blockchain-based IoT model

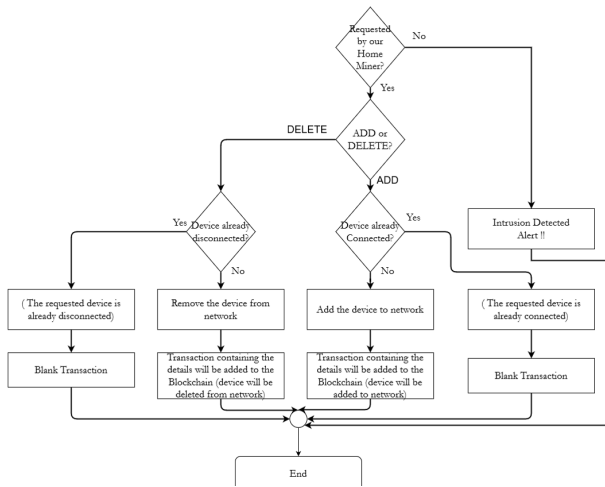


FIGURE 2. Flowchart for Adding or Deleting devices in Blockchain-based IoT model

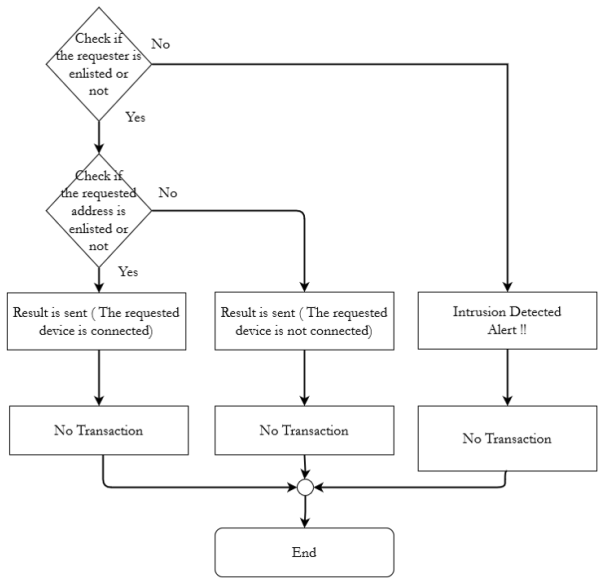


FIGURE 3. Flowchart for Checking Connectivity in Blockchain-based IoT model

The sequence diagram for our model is given below:

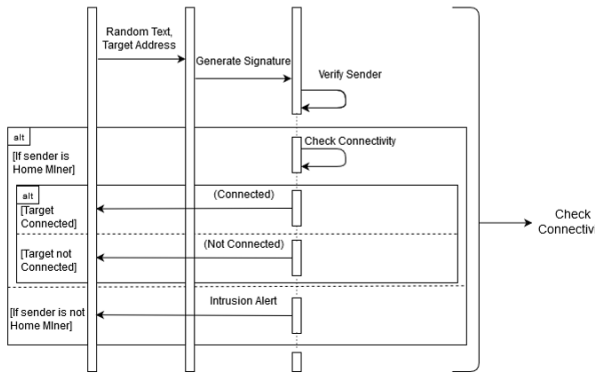
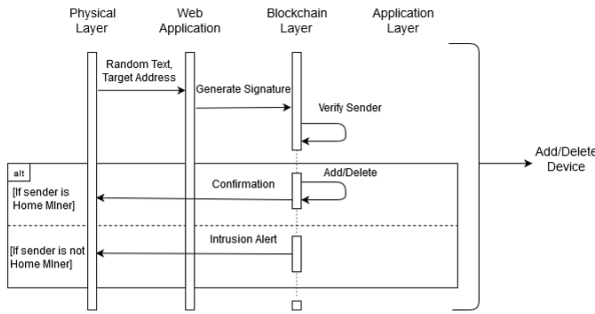


FIGURE 4. Sequence diagram for three types of request in Blockchain-based IoT model

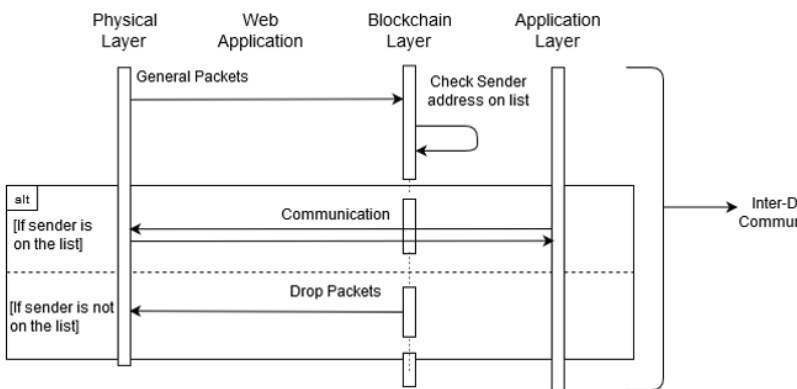


FIGURE 5. Sequence diagram for Inter-device Communication in Blockchain-based IoT model

IV. Experimental Progress

A. Experimental Configuration

For the implementation of our model, we used a machine that has a processor of core i3 6th generation. This particular processor has 2 cores and 4 threads built into it. Our processor has a clock speed of a maximum of 2.3 GHz and has 3 MB cache memory. We used Ubuntu 20.04 LTS for implementation experiments. Also, our machine had 4 GigaBytes of DDR3 1600 MHz of physical memory or RAM installed.

B. Experimental Implementation of the Model

We can deploy a private blockchain on our local computer by creating a genesis block first. Then we can initialize and start our very own private blockchain. We could deploy our smart contract on our private blockchain and proceed further, but we used a Truffle framework named Ganache for easy processing. Ganache is a personal blockchain developed by Truffle which can be used easily to deploy or develop dApps. After starting, Ganache gives us 10 Ethereum accounts, each loaded with 100 ethers running on a private blockchain.

As we have our blockchain running on Ganache, we need to deploy a smart contract to our blockchain. For that, we used the Remix IDE. We wrote our solidity code on the Remix IDE, compiled it, and then collected the ABI. Then we deployed the smart contract on our ganache blockchain. After deployment, we got a deployment address for our smart contract. The deployment address is needed to send the virtual ethers to the smart contract for the needed transaction.

We also designed a web application to communicate with our blockchain via smart contract. Figure 6 shows the initialization of the system. It is a simple representation of our planned IoT-Blockchain model. We can think of this page as a user interface of our proposed system. Our device has a unique Ethereum address and if any account without that address requests to manipulate data on our blockchain, it will be ignored. After adding a device address on our system and then if we request a connectivity check with a random message and that target address, we just added, we get output like figure 7 which ensures us that our addition of device addresses is working. Then suppose we want to delete a particular device from our network, we request to delete it and we can again ensure that the particular device/Ethereum address is

not on our trusted device list by checking the connectivity check.

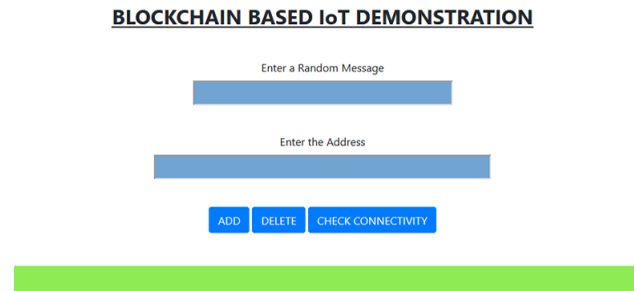


FIGURE 6. Initialization of the System

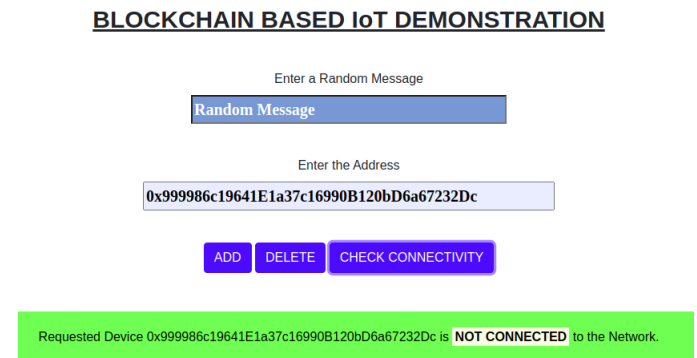


FIGURE 7. Checking Connectivity

C. Experimental Testing of the Model

Our network is a local private Ethereum network. By definition, it is designed such as it cannot be accessed from outside the network. For testing purposes, we changed a digit of the smart contract address on the web application. Then we tried requesting check connectivity and got the output of possible intrusion as shown in figure 8. This message leaves us to the decision that if any digit in the setup of the model is wrong, can be detected and the instruction after that can be provided as needed. Then as an intruder, we tried to manipulate blockchain data shown in figure 9. It is shown that the data is manipulated from the intruder's view but after connecting properly again, that is when we connected to the proper smart contract address again, we could see in figure 10 that the data was not changed and though we tried to delete a device as an intruder, the device was not deleted from the network.

BLOCKCHAIN BASED IoT DEMONSTRATION

Enter a Random Message
RR

Enter the Address
0x999986c19641E1a37c16990B120bD6a67232Dc

ADD DELETE CHECK CONNECTIVITY

Requester is NOT CONNECTED to the Network,
IT IS A BREACH !!

FIGURE 8. Intrusion Detection

BLOCKCHAIN BASED IoT DEMONSTRATION

Enter a Random Message
RR

Enter the Address
0x999986c19641E1a37c16990B120bD6a67232Dc

ADD DELETE CHECK CONNECTIVITY

The Device: 0x999986c19641E1a37c16990B120bD6a67232Dc has been DELETED from the Network.

FIGURE 9. Intruders view to a request

BLOCKCHAIN BASED IoT DEMONSTRATION

Enter a Random Message
RR

Enter the Address
0x999986c19641E1a37c16990B120bD6a67232Dc

ADD DELETE CHECK CONNECTIVITY

Requested Device 0x999986c19641E1a37c16990B120bD6a67232Dc is CONNECTED to the Network.

FIGURE 10. Home Miner's view of a request

V. Result Analysis

A. Speed

The bitcoin blockchain can generate transactions in a 10-minute interval [3]. Ethereum on the other hand can generate up to 20 transactions per second. In our proposed model, 20 inputs per second is more than enough for what we need. We only need to think about the speed if we need to enroll more than 20 devices per second. As we have to taken the Ethereum address inputs by human interaction, it is practically very rare

to get up to 20 inputs in a second. So, our system will not face this challenge.

Moreover, there is a term called 'mempool'. Mempool is the holding area of a node's transaction. For example, if a node is mining a block and a valid transaction request comes, the new request shall be placed in mempool. When the node is done with mining the block, then the transaction will be processed. In another word, the longer it takes to mine a block, the higher of chances that transactions will fall in mempool. And the speed of mining a block depends on the difficulty level of a blockchain. In our proposed system and the implementation, the transaction process time was not very long. As ours is a private blockchain, the difficulty level can be set to low so that it can function properly in the high-end devices as well as in the low computational powered devices.

B. Storage

Storage is one of the major bottlenecks that blockchain face. Current size of the Ethereum blockchain is around 1.498 GB [8] and it is getting larger day by day as more blocks get added to the chain. On our proposed IoT-Blockchain model, we only save a list of Ethereum addresses as a string. From the nature of our model, it should not have a huge number of blocks and that concludes us to a decision that storage should not be an issue for our model.

C. Cost

Our proposed model uses a private local blockchain, which is free of cost. If we somehow manage to run blockchain on IoT devices in near future, the implementation cost of this model will be Zero. Our model only needs a local private blockchain running 24/7 and our deployed smart contract on the blockchain to run properly. Ethers of a local blockchain are virtual ethers and it will not cost a single cent to the device owner.

However, if we want to implement this system where a large number of devices shall be attached or which covers large areas, like a smart city or smart power grid, we might have to make changes to the model. Switching on a public blockchain shall be a good idea then. Public blockchain can be a little costly but still, it will be worth for ensuring security. Or if a smart hospital or library wants to implement this model, they can attach a cloud server to the blockchain and keep the non-sensitive data or books on the cloud so that the blockchain does not hold unnecessary data and stays as light as possible.

VI. Conclusion and Future Works

The goal of this paper was to design a safer and more secured IoT model. Although some drawbacks like design and scalability issues, this model can improve the security of the Internet of Things (IoT) devices dramatically. This model can be a better alternative to the conventional IoT systems of now. As the chain is fully local, the chance to get access to the connected devices list is theoretically impossible. But if somehow it is accessed by someone unknown, it can be detected and it will not let them manipulate the saved data on the blockchain. This describes how this merged IoT and blockchain technology can secure user data and privacy. We described how a data breach can be a potential threat to individuals. We believe that proper implementation of this model can take time but it will provide security and privacy to individuals and keep everyone safe from potential threats.

We must already know by now that the limitation of IoT devices is small memory or processing power. Our system might not need very much power but it should be very difficult to implement it on some devices like a smartwatch or smart bulbs which rarely have a memory greater than some megabytes. Lastly, in the era of automation, we are proposing something manual alike. In our model, we ensured privacy and security by removing automation.

To properly implement our system, an IoT device has to be running blockchain 24/7. But practically, this kind of IoT based system is still not used. In future, if IoT devices have the needed computational energy for running light blockchain then the system can be fully implemented. Right now, all blockchain technologies face some difficulties as it is an emerging technology. Although the resources are mostly open, but the practice of blockchain technology is very rare these days. But as the number of blockchain-based researches grows higher, the technology is getting better day by day.

References

- [1] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," en, in 2015 IEEE Symposium on Computers and Communication (ISCC), 2015, 180–187.
- [2] D. Fakhri and K. Mutijarsa, "Secure iot communication using blockchain technology," in 2018 International Symposium on Electronics and Smart Devices (ISESD), IEEE, 2018, pp. 1–6.
- [3] D. Labrien, "5 pressing issues that slow down blockchain development and adoption," 2018. [Online]. Available: <https://channels.theinnovationenterprise.com/articles/5-pressing-issues-that-slow-down-blockchain-development-and-adoption>.
- [4] A. Sikder, G. Petracca, H. Aksu, and T. Jaeger, "A survey on sensor-based threats to internet-of-things (iot) devices and applications," en, Research-gate.net, 2018, Online Available. [Online]. Available: <https://www.researchgate.net/publication/322975901ASurveyonSensor-basedThreatstoInternet-of-ThingsIoTDevicesandApplications>.
- [5] N. Fotiou, I. Pittaras, V. A. Siris, S. Voulgaris, and G. C. Polyzos, "Secure iot access at scale using blockchains and smart contracts," in 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), IEEE, 2019, pp. 1–6.
- [6] U. Nadiya, M. Rizqyawan, and O. Mahnedra, "Blockchain-based secure data storage for door lock system," en, in 2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICI-TISEE), 2019, 140–144.
- [7] O. Sullivan, "The worst and weirdest IoT hacks of all times," en, Finance-monthly.com, Sep. 5, 2019.
- [8] "Ethereum chain full sync data size," 2020. [Online]. Available: <https://ycharts.com/indicators/ethereumchainfullsyncdatasize>.
- [9] J. Frankenfield, "51% attack," en, Investopedia.com, Aug. 28, 2020, Online Available. [Online]. Available: <https://www.investopedia.com/terms/1/51-attack.asp>.
- [10] M. Zuidhoorn, "The magic of digital signatures on ethereum," 2020. [Online]. Available: <https://medium.com/mycrypto/the-magic-of-digital-signatures-on-ethereum-98fe184dc9c7>.