Word Count: 5650

Plagiarism Percentage 8%

Matches

1 **World Wide Web Match**
View Link

2 **World Wide Web Match**
View Link

3 **World Wide Web Match**
View Link

4 **World Wide Web Match**
View Link

5 **World Wide Web Match**
View Link

6 **World Wide Web Match**
View Link

7 **World Wide Web Match**
View Link

8 **World Wide Web Match**
View Link

9 **World Wide Web Match**
View Link

10 **World Wide Web Match**
View Link

11 **World Wide Web Match**

View Link

12 **World Wide Web Match**
View Link

13 **World Wide Web Match**
View Link

14 **World Wide Web Match**
View Link

15 **World Wide Web Match**
View Link

16 **World Wide Web Match**
View Link

17 **World Wide Web Match**
View Link

18 **World Wide Web Match**
View Link

19 **World Wide Web Match**
View Link

20 **World Wide Web Match**
View Link

21 **World Wide Web Match**
View Link

22 **World Wide Web Match**
View Link

23 **World Wide Web Match**
View Link

Suspected Content

Blockchain based Security Model for IoT Kruthik J T Ramakrishnan K PES1201701509 PES1201701906 PES University PES University jt.kruthik@gmail.com k.ramakrishnan10@gmail.com Abstract—The

Internet of Things has emerged as an area of incredible potential and growth, 2

complemented by the advent of smart devices with increased computational power. However, these complex systems have large attack surfaces making them susceptible to various security attacks. Most common among these are data forgery and identity theft. Further, once the IoT is compromised, the smart devices may be controlled remotely by the attacker and used as botnets in Distributed Denial of Service attacks. The size and scale of the complex system results in technical challenges in management, synchronization and security.

In this paper, we propose and implement a blockchain model to secure the 3

IoT system. Using Ethereum, we developed a private blockchain model, verified its functionality in a simulated IoT environment and analysed the performance of the model. Further, we developed a web based interface to the IoT system to

demonstrate the working of the blockchain. Keywords—Internet of Things, network security, 1

Blockchain, Ethereum, Hashing, web interface INTRODUCTION The world took a major leap when different computers were connected for the first time in 1965 marking the birth of the Internet. The interconnection of computers and networks lead to faster development in the modern world. Then

in 1999, the term Internet of Things was coined by Kevin Ashton as an interconnection of 12

objects in the real world. Currently, the Internet 4

of Things has grown into a key technology which enables faster interaction

with the real world. Similar to the internet, IoT 4

has also

seen an exponential growth in recent years. 4

This growth is complemented by the development of smart devices. The increase in power of computing systems these days have enabled machines to learn and find patterns from the data. This has led to further

improvement on the data processing and decision making capabilities of the devices and hence in improvement of IoT as a whole. Smart device is an electronic device capable of collecting data via sensors and communicating with one another with minimal human interaction. These devices can take action on the environment based on this data. The data they collect from the environment is also shared among other smart devices using a peer-to-peer network. Data collected is of prime importance. The data processing may be done at the device itself for example in case of emergencies or real time response, or may be moved to the cloud. Further this data is crucial for training, testing, developing and maintaining the AI and ML models. The smart devices are a part of a peer-to-peer to network since a lot of simultaneous communication is needed, which is not feasible in a client server network. A peer to peer network means that each device may be able to communicate with other devices in the network and there is no fixed client and server. In most IoT systems involving an end user, an interface is provided. Since few IoT systems use the internet, a web based interface is convenient. Also, the interface must be able to monitor the devices in the network and notify the user in case of device crash, emergency, or security breach etc. IoT systems use the network connection extensively for their processing. This means that existing security threats in the internet can affect the systems. Some of these security breaches in IoT are relatively new. They show the need for securing the network and hence its devices from security attacks. The infamous “Mirai” IoT bot-net attack is a Distributed Denial of Service attack carried out using IoT devices that run on ARC processors. The malware Mirai infects the IoT devices, by exploiting the default username and passwords, turning them into remotely controlled bots. This network of bots (botnet) was used to carry out a DDoS attack. By November 2016 the Mirai malware had infected over 6 million IoT devices. These devices were then used to bring down a cybersecurity blog. Since there are many devices, it is a challenge to find the attacker. Apart from DDoS attacks, IoT is also

vulnerable to man in the middle attacks. The attacker

secretly relays or alters the messages in the communication. These attacks could lead to severe problems such as identity theft and ransomware. Attacks like these bring down the users' trust on the system and hinder the growth of IoT. These attacks demonstrate the need for a strong and convincing solution for IoT security. In 2008, Satoshi Nakamoto invented bitcoin. This cryptocurrency has a distributed architecture, and runs on a p2p network. Blockchain is a new technology introduced as the public ledger to track and validate the transactions done using bitcoin. It works using cryptographic hashing. Nowadays, there is a lot of research on extending Blockchain for other applications as well, such as in the supply chain and smart contracts. Further the growth of blockchain has brought more attention to its development. Ethereum is one such platform that helps in developing new blockchain systems using Solidity programming language.

In this paper we propose and implement a IoT security model using blockchain.

This paper is divided into 7 main parts. We start with a literature review to understand the current progress in the field of IoT, blockchain and IoT security. In order to demonstrate the model, we build a simple IoT network and simulate the transfer of data through the network. We develop a front-end (end-user application) for enhanced access to the IoT network. This simulation of the IoT system and the workflow is illustrated in the as a sub-section under the proposed system. Moving on, we discuss the basics of a blockchain and how to implement one. We describe the architecture of the model and the various components of the system and conclude with the future scope of the project. LITERATURE SURVEY A

complete understanding of the working of an IoT system is crucial to identify the attack surface of the system. Mrs.Soumyalatha and Ms.Shruti [1] provide an introduction to IoT systems and architecture. The IoT system provides the smart objects under it to connect

to the internet and communicate with each other with minimum human 7

interaction. In their paper, Soumyalatha, Shruti [1] discuss IoT and its architecture. Further they elucidate its relationship with the Wireless Sensor Networks (WSN). Through this paper, many applications of IoT are explained in brief along with the current tools, advantages, disadvantages and challenges of IoT.

This paper also proposes an idea for using IoT in the domain of Indian 7

architecture. There are different kinds of security attacks possible on an IoT system. In order to secure the system, it is important to know the existing security measures. Also knowledge of various ways an attack can occur helps in finding the attack surface of the system. Once the attack surface is identified, then a security model can be developed. Minhaj and Khaled [2]

present and survey the security issues for IoT by reviewing and 2

categorizing them. They

tabulate and map the security problems with the existing solutions. 2

They discuss how blockchain

can be a key enabler to solve many security problems. 2

They identify

open research problems and challenges for IoT security. A 2

Blockchain model consists of various components with independent functionality. To implement a blockchain model, it is crucial to know the internals of a blockchain, how it works, and how it can be used in other systems as well. Christy Varghese [3] gives a basic introduction to IoT technology and its architecture through the paper. This paper also proposes building IoT systems using blockchain platforms. Also a system is implemented using the Ethereum platform for IoT. The benefits of such a system are enlisted and discussed in brief. Ziyan Wang, Xinghua Dong, et al. [4]

focuses on the research of model construction and performance evaluation. 1

The theoretical and data support is surveyed through literature.

An IoT security model is established based on blockchain and IPFS (InterPlanetary File system). 1

The security risks and system performance is analysed for the exposed system. Then

the average latency and throughput of 1

the system is analysed. These analysis and tests

demonstrate the effectiveness of the blockchain based security model. 1

Jayavardhana, Rajkumar et. al. [5]

presents a Cloud centric vision for worldwide implementation of 16

IoT. Various existing IoT tools such as RFID are discussed here. Further the internal working of IoT in a cloud based system is explained. The cloud implementation is done

using Aneka. It is based on the interaction between public and private 5

clouds. The paper concludes its

IoT vision by expanding on the need for convergence of WSN, the Internet and distributed computing directed at the technological research community. Sathish and 5

Dhiren [6] introduces IoT. They explain its capabilities to connect real world objects into a unified system. It discusses the serious concerns raised regarding personal information. The concern in IoT security pertaining to device and individual privacy is also discussed. They conclude the survey by summarizing the privacy concerns and security threats of IoT. Atzori, Iera, et. al. [7] addresses IoT and the integration of several technologies and communication solutions. It explains how IoT is a system built from several other domains such as telecommunications, electronics, informatics and social science. This survey reviews the visions of IoT paradigms and its enabling technologies. The paper also discusses the major issues faced by the research community in detail. Nakamoto [8] introduces crypto currency and means to enable transactions in a peer to peer network. This paper aims at enabling transactions among peers without a centralised system. This paper

proposes a solution to the double spending problem using a peer to peer network. 11

It discusses various technologies such as hashing, proof of work, and immutable records. This paper explains the working of a blockchain and how it is used in the cryptocurrency bitcoin. Seyoung, Sangrae et. al. propose the use of blockchain

to build an IoT system. It discusses the management of keys using RSA public key 9

cryptosystems. This paper uses Ethereum

to store the public keys and run the 9

smart contracts. They used Ethereum for its advantage of fine grained management of IoT devices. This paper also includes a proof of concept using few IoT devices. It ends with a future scope of building a fully scale IoT system using blockchain. PROPOSED SYSTEM Blockchain is a ledger used to track and manage transactions in a network. It is maintained by a community of decentralized peer-to-peer networks. This means that the data is not stored in a central server, but is written to a ledger. Also the nodes of the network connect to each other in the peer-to-peer networks unlike the traditional

client-server architecture where multiple clients connect to a single server. 15

Further, a decentralised system in general enables easier management of the transactions and quick decision making.

Every node in the blockchain network has a copy of the ledger. This 6

ensures transparency in the system, since each node can access the data without releasing on a particular node, but the entire network. Blockchain ensures that any transaction in the network is immutable. This guarantees that the data stored in the network is not modified at a later point in time, thereby preventing data tampering. However, the data to be written must be verified before insertion. A blockchain can be viewed logically as a collection of 3 major components: 1. Data: The transaction that needs to be stored in the chain. This data is generally hashed to store into a fixed length field. Most common hashing used is the SHA256 hashing which ensures output size is 256 bits or 32 bytes. 2. Previous information in the network: The existing information in the chain is stored as a hash of the data. The previous hash is used to track changes in the chain. 3. Nonce(number only used once): This is a random number generated by each node in the network. This number is used to generate required hash values when appending the block to blockchain and prevent replay attacks. Working of a blockchain When a transaction is initiated in the network, a new block is created with the transaction details hashed into the data field. To ensure that the transaction is valid, the transaction must be digitally signed by the user or node. This is done using public private key pairs generated by the user for the first-ever transaction. The data is signed using the private key

of the user. This private key must not be shared. The transaction signed with the private key must be broadcast along with the public key. The public key is used to validate the source as well as the transaction. Once the transaction is validated and accepted, the transaction can be added to the block. This append must be done by every other member in the blockchain holding a copy of the block. A block can accommodate a certain amount of transactions in it. Once the limit is reached, the block must be attached to the blockchain. This process of adding a block to the blockchain is accomplished after solving a cryptographic puzzle of generating a smaller hash value than the previous hash. The process of adding the block to the blockchain is called mining and the nodes that do this are called miners. While solving the puzzle, a lot of hash values need to be generated making this process computationally expensive. Every block maintains

> a link to the previous block in the blockchain. This is **21**

how the chain is maintained among the blocks and it is achieved

> by storing the hash value of the previous block in the current block. **3**

A hash is generated using a function called the hash function. The most commonly used hash function is SHA256. A hash is generated by applying the hash function on the data, in this case the entire block. SHA256 hash function generates a 256 bit value for the input. Since the probability of a collision in the hash is negligible, it is safe to assume that different inputs will always generate different hash values. Further a single input will always generate the same hash value. A unique property of the hash value is

> that it is not possible to generate the input string using its hash value. This ensures that the **13**

data is secure and can not be deciphered from its hash value. This can be viewed as a method of storing the information of the input. So by tracking the

> hash of the previous block, its **6**

information is passed on to the

> current block. The hash of the current block **6**

will incorporate its own information as well the information of the previous blocks. The hash value generated by the miner must satisfy some requirements in order to append the block to blockchain. The first requirement is that the hash generated

> must be lower than the target hash. The value of the **20**

target hash changes based on the difficulty of mining such hash values. The second requirement is that the hash generated must start with a specific number of leading zeros which is set by the blockchain. Since the data and previous hash can not be altered when adding to the blockchain, the only way to generate different hash values is by concatenating a new number called nonce. This number helps to satisfy the second requirement. So each miner has to generate nonces, compute the resulting hash value and repeat until the hash generated is less than the target hash. The nonce value is random and is best found using trial and error. Once the feasible nonce is found, the miner can append the block to the blockchain. This method is called

proof of work. The proof of work mechanism makes the 4

blockchain more secure. It deters security

attacks like denial of service and 4

spam since some computation must be performed by the sender. Blockchain's advantages over a client server model. The distributed nature and the proof of work mechanism implemented in blockchain provides certain important advantages over the traditional client server model: 1. No single authority: The blockchain is available to all in the network. The blocks can be added by any miner. This means that no single authority can take control over the blockchain network and the blockchain itself. This transparency of the network brings in consensus in the decision taken. 2. Consensus Algorithm: Blockchain uses

a peer to peer network and complex mechanisms such as 3

proof of work and consensus algorithm. These components ensure that each node in the network participates in the decision being taken and that the decision is not always favourable to a particular node in the network. 3. Immutability: The data once written in the blockchain can not be easily modified or removed at a later time. This mechanism ensures that only valid blocks are added to the blockchain and encourages more trust among the users of the system. 4. Validation: Any user in the network can verify the data written to the public blockchain using the right tools. This ensures that blocks in the network are valid. Blockchain for IoT It is noticeable that IoT and blockchain both work on peer to peer networks. Now IoT is

vulnerable to attacks such as data forgery and identity theft. If blockchain is 19

incorporated within an IoT system, the security of the IoT systems can be improved. Also this model may be easier to develop since both technologies work on peer to peer networks. The users of the IoT system can be assured of data safety since blockchain prevents updates in the data. Unlike the existing client server model where the server or client could be targeted to attacks, the decentralised model of blockchain does not suffer from such vulnerabilities. However, this also means that each node must be protected equally well. In most cases, the blockchain being used will be a private blockchain, for instance in smart homes. This will reduce the chances of a remote attack from outside the network, since only devices in the same

network will be able to access the blockchain. Even in case of a compromise, the data can not be altered since no single authority can control the chain. Further any activity of the attacker can be found and tracked. Blockchain only provides support for operations such as read and write. It prevents any updates or deletes on the data stored in the network. These mechanisms can help in improving the security of IoT systems using the advantages provided by blockchain. In order to use blockchain for IoT, it is necessary to track the parameters that need to be stored in the blockchain. Since the data flows from one device to another within the peer to peer network, few parameters that can be tracked include transaction id, timestamp, data being communicated, device id and device name. These parameters can help in tracking the compromised devices and the history of transactions from or to the system, thereby helping in identifying the attacker. Ethereum Ethereum is an open source public blockchain platform which was first proposed by Vatalik Buterin in 2013 and introduced in 2015. Ethereum also has a cryptocurrency called Ether which is the second largest cryptocurrency in the world after bitcoin. Ethereum has spanned further in the blockchain domain. It also provides a distributed computing platform unlike bitcoin. This platform enables users to build distributed applications (dapps). A major component of these dapps include blockchain. These apps use blockchain as the background in their working model. Since Ethereum is open source, it also allows development and testing of the dapps and blockchain models built. The access to the private is provided using programming languages such as solidity, serpent, etc. These languages are similar to python, and are supported with a rich documentation and active community. The platform allows compilation, execution and simulation of the blockchain. The public blockchain in Ethereum is open to the internet. Once registered, miners can contribute to the network by computing the nonce of a block before it is added to the chain. This task requires high amounts of computational power and time. The miners are awarded for the same using the ether. Ethereum also allows users who generate the transactions to set an extra amount in cryptocurrency that is transferred to add the transaction to the blockchain. This extra incentive can attract more miners. Ethereum can be thought of as a transaction-state machine, which means that when a transaction is executed on the system it changes its state and stores the same. Ethereum provides Smart contracts. These are immutable rules or protocols which cannot be changed. These rules provide the interface to access the blockchain and must be followed by the users. Smart Contract The smart contracts are digital contracts which enforce and control the access to the blockchain being built. These rules are similar to protocols and must be followed in the transactions and access. Ethereum provides immutable smart contracts which can not be changed once compiled and deployed on the blockchain. A Smart contract can be understood as a contract set between two parties in a deal. The contract would be a list of specifications, conditions and terms. Both the parties of the transactions will proceed only when the contract is valid. When the contract specifications or conditions are met, the contract holds true and is said to be valid. Necessary actions are taken only when the contract is valid. Generally this action would be a transaction among the parties. In case the deals are not abiding to the rules of the contract, the transaction can be penalized or considered invalid and dropped, and no further action is taken. Similarly a smart contract is a set of rules written which are applied on the blockchain when a developer calls it. A user needs to communicate with the blockchain using smart contracts, be it reading data from the blockchain or writing data to the blockchain. Ethereum allows developers to create unlimited smart contracts. The advantage of a smart contract is the elimination of a middle man or a mediator for the transactions to be executed: transactions are executed only if the rules of the contract are met. The smart contract works automatically. Developers can leverage this feature and eliminate middlemen and mediators and ensure a transparent transaction between the two parties. This can improve the trust in the system and hence elevate the user experience. IMPLEMENTATION MODULE Scenario For this project, we have chosen three raspberry pis to mimic the actions of a camera, HVAC system and voice assistant(Alexa). Each raspberry pi will act as nodes of the peer to peer network and will use the Ethereum platform to access the blockchain. Storing data

on the blockchain is an expensive voyage to carry out because blockchain is best suited for transactions and can't store large amounts of raw data. Instead we store the

> hash value of the data on the blockchain and the 3

raw data and transaction details regarding the transaction on a secondary cloud storage. Unlike the server client model, where

> there is a single point of failure, Ethereum is a distributed 17

platform, where every node present in the blockchain has the copy of the chain and the transactions involved in it. Consensus algorithm helps execute and store the transactions into the network, making it highly difficult for attackers to tamper with the data, using these characteristics an IoT system is built, which can stand against many attacks like denial of service attacks. Data

> is stored on the blockchain using a Smart contract 14

and every node

> in the blockchain can use the same smart contract 14

to add the hash of the data to the blockchain provided they're members of the network. Data is retrieved from the blockchain and compared with the data stored on the cloud storage, if the hash of the raw data matches the value retrieved from the blockchain then it can be said for sure that the data is not tampered with. This data is later shown to the user on a web interface. Ethereum Model

> Launched in 2015, it is the world's programmable blockchain. Like other blockchains, it has a cryptocurrency called Ether (ETH). Unlike the 8

client server

> model, Ethereum is a distributed computing platform in which 18

data is distributed to all the nodes storing the blockchain, therefore even if one copy of the blockchain is corrupted other copies can be used. Ethereum allows developers

> to build new kinds of applications. These decentralized applications (dapps) gain the advantages of blockchain technology. They 10

are reliable and predictable, It will always run as programmed when uploaded to the Ethereum network. Because Blockchain is decentralized and the data on it cannot be tampered DDoS attacks and forgery attacks can be avoided. In this project we use the Ethereum blockchain platform to hold the sha256 value of the data generated by the IoT devices. Smart Contract Smart contracts are computer programs which dictate the way nodes interact with the blockchain. In this project we have one smart contract using which the participating nodes(camera, hvac, voice assistant) read or write data to the blockchain. The Smart contract implemented mainly has two functions one is to write to a transaction, the function takes as input id and sha256 output of the data as input. The provided id and sha256 output

id becomes crucial in storing data in a blockchain, without the id retrieving this data is highly difficult. The second function is used to read data from blockchain or precisely the transaction data or the sha256 value of the data, the function takes the id as input and then searches the blockchain for the data stored with respect to this id and returns it. Architecture The entire system consists of three raspberry pis which act as IoT devices, the camera stores its video, the hvac system stores sensor data and voice assistant stores the voice commands. Blockchain is used as an authentication and verification platform and not as a data storage platform because storing large data on blockchain is not feasible as the blockchain is held by every node on the chain. When the devices have to store the data, it is first checked with the blockchain if it is a valid node and part of the IoT ecosystem and not a foreign device. Once the authentication is completed the sha256 output of the data is stored in the blockchain with a user defined id via the smart contract. The raw data is written to the cloud storage with the id defined by the user and the transaction hash. This id is highly crucial to retrieve the data stored on the blockchain. When the owner wants to view the output of the devices through the web interface, he/she requests for the data, the respective data is extracted from the database. A request is now sent to the blockchain to retrieve the data pertaining to the id and if present the data is read from the blockchain, the data is in sha256 format. Therefore, the raw data extracted from the database is converted to sha256 value. This value is compared with the data retrieved from the blockchain, if a match occurs the owner can be rest assured that the data was not tampered. Therefore, to sum it up only devices registered to the IoT system can access the blockchain and data tampering can be detected in case of any. Results Through this project we have been able to address some of the major security issues in IoT generated data. Prime among them are those related to protecting the data generated by the IoT devices from tampering and altering or deleting. We also address data confidentiality, data integrity and tamper detection of the database. The data requested by the user is validated before servicing this request. Through the course of the project we found that the major reason for such security breaches is that the network is not secure. Any new node in the network must prove its authenticity before being able to participate in the transactions of the network. We ensure authenticity by allowing only devices with registered ethereum accounts to add or read from the blockchain. We use the blockchain’s distributed ledger to store our transactions, this ledger system makes it hard to alter the data, because to do so a hacker must take control of more than 50% of the network and must alter the hash of all the blocks which is computationally very expensive. Therefore we can ensure that data tampering is prevented. A major shortcoming of a blockchain network is that storing the data is an expensive process. The use of a SHA256 hash function to generate the hash values, which are then stored in the blockchain, is a good workaround to address this. The data present in the blockchain can be viewed by every node in the network, but we encrypt the data using SHA256 algorithm and then store it in the blockchain ensuring confidentiality. When a user requests for data from the database, we retrieve the data and run the SHA256 algorithm over the

transaction value of that particular transaction and then match this to the data present in the blockchain using the transaction ID. The user can stay rest assured about the data in the blockchain, but by matching the data present in the database to the data in the blockchain we can detect if the data has been tampered in the database from the time it was stored in the blockchain. Even though the project protects data upto a certain extent, access control is necessary to display the data to the concerned user. A web interface is built to demonstrate the functioning of the IoT system and blockchain. The web interface allows the user to view the live readings from the device network. In case of a camera, the web interface displays the live feed onto the web page. For this purpose flask is used. The web application uses the database and makes requests to the blockchain. In case of sensory devices like HVAC, the history of readings collected is displayed. Sometimes the processed data is preferred over the raw input. For instance the voice assistant converts the voice requests into text for further processing. The web interface allows access to this history as well. Following are the screenshots of the application. FUTURE SCOPE This project currently runs on a public blockchain. It can be restricted to a private blockchain to enforce strict access control. The project can be extended to use a more secure storage mechanism such as a distributed file system. The blockchain model does not handle all the security vulnerabilities of the IoT network, and hence must be incorporated along with the existing models. The future scope of this project lies in the fact that blockchain can maintain a secure accounting of the transactions in a p2p network. It can also help in identifying security breaches in the network and securing against the breach in the future. CONCLUSION IoT technology is increasing at a rapid pace. Its advantages are immense. Securing the data generated by the IoT network is crucial to ensure the growth and development of IoT. Further authentication and authorization must be ensured on the IoT system. Securing the data can establish data privacy and eliminate data forgery and data tampering. These measures will improve the user experience and trust on the IoT system. Blockchain provides this solution with its decentralized and immutable nature. In this project we use these features to address the major issue of data security. Access control is guaranteed by ensuring that only registered devices can access the blockchain. Further a decentralized and immutable nature enforces data availability and security. Data forgery is prevented by the use of SHA256 hashing to encrypt the data before storing it in the blockchain. Data tampering is also avoided using authentication, authorization and verification steps. Other attacks such as man in the middle are avoided by the use of the nonce field in the blockchain. Thus using blockchain for IoT devices provides a good blend between the technologies and can avoid DDoS attacks, forgery attacks. The blockchain is used along with the existing IoT security models guaranteeing enhanced security in the system. ACKNOWLEDGMENT We are grateful to Prof. Sunitha for the help, motivation, guidance and support provided throughout the project. We would like to thank the CSE department and ISFCR research group of PES University for providing us with the necessary facilities for the project. REFERENCES [1] [2] Soumyalatha, Shruti, Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges, 2016/05/01 Minhaj Ahmad Khan and Khaled Salah, "IoT security: Review, blockchain solutions, and open challenges", Future Generation Computer Systems, Volume 82, 2018, Pages 395-411, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.11.022. [3] Christy Varghese, “IoT DEVICE MANAGEMENT USING BLOCKCHAIN”, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 8, Issue 3, March 2019, http://ijsetr.org/wp-content/uploads/2019/03/IJSETR-VOL-8-ISSUE- 3-79-84.pdf [4] Z. Wang, X. Dong, Y. Li, L. Fang and P. Chen, "IoT Security Model and Performance Evaluation: A Blockchain Approach," 2018 International Conference on Network Infrastructure and Digital Content (IC-NIDC), Guiyang, 2018, pp. 260-264 [5] Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic a, Marimuthu Palaniswami, — Internet of Things (IoT): A vision, architectural elements, and future directions”, Future Generation Computer Systems, Elsevier,2013. [6] J. Sathish Kumar, Dhiren R. Patel, —A Survey on Internet of Things: Security and Privacy Issues”, International Journal of Computer Applications (0975 – 8887) Volume 90 – No 11, March 2014 [7]

[8] [9] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer. Networks. 54 (15) (2010) 2787–2805. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. White Paper, 2008 Seyoung Huh, Sangrae Cho, Soohyung Kim, ”Managing IoT Devices using BlockchainPlatform”, 19th International Conference on Advanced Communication Technology (ICACT), pp 464-467, IEEE 2017