International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Enhancing IoT Security for Smart Energy Meter using Blockchain

Vasa Vinay, Sendhil Kumar K S

Abstract*: *Internet of Things (IoT) is growing rapidly in recent days and increasing of IoT devices day by day producing vast amount of data, to store this data security is a major challenge in IoT. To avoid these security challenges, blockchain is the perfect solution. With its security by design, immutable nature, transparent nature and encryption methodology blockchain will solve architectural issues of IoT. In these days, the energy meters in our homes are not able send the information to the cloud and man power also needed to update readings every month, and manually errors also taken place some times to avoid these, in the paper a smart energy meter is proposed, that will measure the power consumption and that readings will be stored in to the blockchain to secure the data from the fraudsters and also to make the payment without any third parties like banks, in the blockchain technology amount can be transferred from one to one without any third parties using crypto currencies like bitcoin, ether.., etc. The user will be able to check the bills in the blockchain and do the payments. By using the blockchain technology the user data will be more secure and the IoT security issues also solvable.

Keywords: Blockchain, cryptocurrency, Ether, Internet of Things, Security, Smart Energy Meter.

I. INTRODUCTION

Internet of Things (IoT) is nothing but the physical devices connected with the internet and they are generating vast amount of data on daily basis and this data is stored in the cloud or local servers, cloud is the best solution to store this data than the local servers and the communication purpose also it's better and also to store the vast amount of data. [1] By this we are facing security issues of data and facing cyber-attacks. Traditional security methods are expensive and also attackable. In terms of user privacy they are producing noisy data. So we need new technology that gives more security and privacy [2]. To provide security for this vast amount of data, it a challenge and here comes the security issues into the picture.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Vasa Vinay*, School of Computer Science and Engineering Department, Vellore Institute of Technology, Vellore, India, Email: vasavinay5@gmail.com
Sendhil Kumar K S, School of Computer Science and Engineering Department, Vellore Institute of Technology, Vellore, India, Email: sendhilkumar.ks@vit.ac.in

In IoT [2] every node itself is possible to attack, such as DDOS (Distributed Denial-of-service) attack, applying the more traffic to the one node and try to collapse that node. Another challenge is its centralized server, easy for the attackers and another major challenge is the confidentiality and authentication and data integrity. While exchange the data, the security becomes challengeable [13]. Suppose the sensors are sending the data to the servers, it is difficult to say that we are getting the information from the authenticated sensors only any intruders can be able to send the information.

And the delay in sending the information because of network failure or power failure leads to huge damage to the system [15]. Electricity meters nothing but energy meters are measuring the power consumption based on the voltage and the current to show that in kilowatt hours, some energy meters have the led light, based on the number of times light glows , power readings will be taken, normally three thousand six hundred times is equal to one unit[14]

Blockchain is emerging technology in terms of security, with its immutable nature it will provide high security for IoT. Initially it is used for Transaction purpose only [2]. The privacy of the user data is main concern, by the blockchain we can surely say that the data is secured. By using the cryptocurrency (e.g. Bitcoin) we can achieve these transactions smoothly [16], we don't need any central authority (banks) for the transaction in the blockchain. BC have some properties (a) In the Blockchain network no need to know each other for the transaction process, (b) there are no deciders like banks we can freely do the transactions, (c) here trust is based on their cryptographic algorithms, if the transaction is processed that will be unstoppable [10]. Blockchain is categorized into two types based on its functioning permissioned and permission less, In the permissioned Blockchain based on the consensus algorithm, limits the users who can be able to do validations and who can create smart transactions and in the permission less Blockchain any one can do these operations [11].

In the Blockchain there are some concepts are there first one is peer to peer network in this central authority will be avoided only nodes can communicate with each other[18] , second is open access and distributed ledger in this everyone in the network will be able to see the ledger to validate the records and third is mining here who can be able to add the block to the Blockchain we can call it as miner, to add the blocks to the chain, miner has to solve the mathematical calculations called PoW then only miner will be able to add the blocks to Blockchain [12]. Here that every block consists of

- Data: that sender and receiver information of a transaction.
- Hash: every block will have the hash value of its own and unique (SHA-256).
- Previous hash: that every block has he hash value of its previous block.[20]

A. Consensus

In this algorithm base the new blocks will be added, the leader will add the blocks, basically leader will be selecting based on the voting and he responsible for validating [12].

B. POW (Proof of work)

To add a new block we have also calculate the mathematical problem, the problem is very difficult problem to solve, suppose the intruder can be able to change one block but he has to do the same work for every block because of every block contains the hash of previous block, so it is computationally infeasible[12].

C. Smart-contract

Is nothing but set of rules or the program on the blocks that has to follow the users to do the transactions, Smart contracts are immutable and distributed so it's not possible to tamper. Ethereum is best platform to create smart contracts and they are having their own language called solidity to create the smart contracts [12].

II. RELATED WORK

D Lestari, et al. [3] proposed an Energy monitoring systemis gives the energy consumption data to the user, it is important to provide the electric usage to the user. By this we can reduce the power consumption and by the rapid development of the IoT devices it is possible to monitor the power consumption. They proposed an architecture to monitor the energy consumption. To find the real readings of the energy consumption, they attached the sensors in each corner of the electrical circuit. And the readings is collected and processed and shown in the web apps and they achieved 95% accuracy.
BK Baraman, et al. [4] proposed a cost effective system for monitoring and controlling the power consumption using IoT based smart energy meter. Wi-Fi module is used here to collect the consumption of the power readings from the proposed energy meter and sending to cloud, from the cloud consumer is able to fetch the record and also analyze the data how much energy consumed by this consumer can control energy consumption.
DE Kouicem, et al. [5] proposed that Internet of things are growing rapidly and the main challenge in this is to provide security and problem in the current client-server model is synchronization. They proposed Blockchain for the security and mainly ethereum platform is chosen by its smart contract providing security in better way and the proposed system forms a decentralized network and show cases the transparency security and data integrity.
S Huh, et al. [6] proposed that the IoT is known to every one now a days and it plays major role in smart cities, energy monitoring and transportation. Due increasing the number of IoT devices, the data producing from IoT devices also increasing by this we need one secure system to store the data and using for future purpose. With the blockchain and its nature of security and resistant to many attacks like DDOS and also it is fault-tolerant by this we can able to create a system for secure way of data storing and transaction.
HK Patel, et al. [7] proposed a system that adding some feature to the existing meters and building a new system, with the using GSM shield, LDR sensor, RTC and Relay. The LDR sensor is used sense the energy used and to send the signals to microcontroller, the RTC for time, the Relay will stop the supply whenever user wants and GSM module is used to send a sms to the user, by this they say that this will be energy and economy efficient system.
MH Yaghmaee, et al. [8] Proposed a system and that is also implemented in the Mashhad city, the SCT current sensor is used to measure the power consumption and it is stored on a centralized server and from that user will be able to monitor and controlling the electrical appliances.
JK Mishra, et al. [9] proposed a system that is used TCS 3200 light sensor, by this they can measure the energy consumption. This is placed on old meters and it calculate how many times light is blinking which on the meter and finding the energy consumption and sending this data to the cloud for the consumer purpose, the consumer can be able see the data in the cloud.

III. INTEGRATING SMART ENERGY METER WITH BLOCKCHAIN ARCHITECTURE

- Firstly we will get the input from the smart energy meter as how much power is consumed.
- The architecture of the smart energy meter is shown in the Fig. 2, here current sensor ACS712 will find the amount of power is consumed and Arduino will collect the information from the current sensor.
  - Then the data will be shown in the lcd screen.
  -

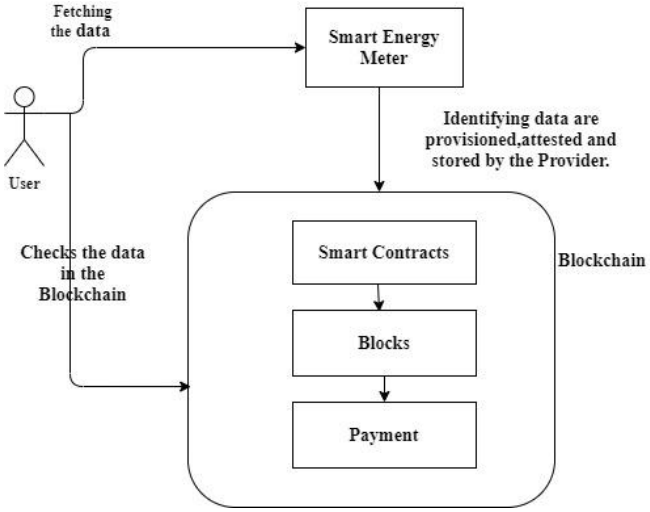

Fig. 1. Smart Energy Meter with Blockchain

- The data will send to the smart contracts (program), from the smart contract the data will be loaded into the blocks based on the proof of work , it is a mathematical problem to solve this problem we need more computational power, so who can solve the problem they will add the blocks to the blockchain.

- Then the user will be able to get the data from the blockchain and he can able do the payment with the Ether. Ether is a crypto currency nothing but digital money.

IV. SMART ENERGY METER

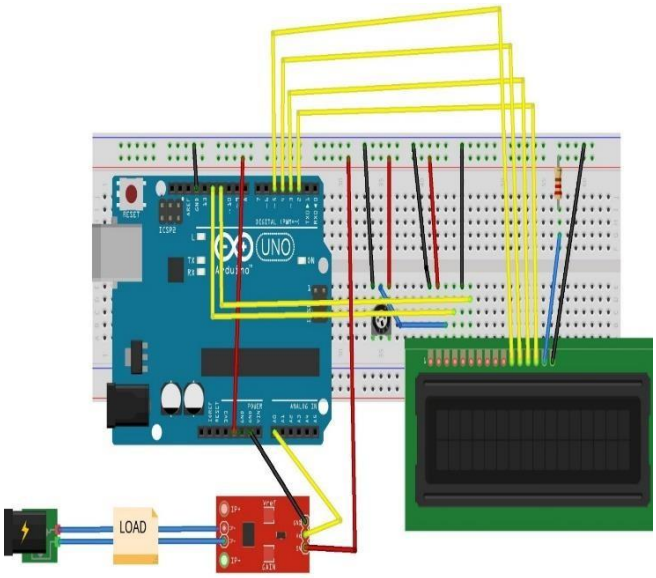

Fig. 2. Smart Energy Meter Circuit Diagram

A. Hardware Used

- Arduino UNO
- LCD 16X2
- ACS712 Sensor
- 10k ohm Potentiometer
- 220 ohm Resistor
- Jumper wires
- Bread Board
- Electric plug
- Bulb(as load)

B. Arduino Uno

Arduino Uno is a board based on the ATmega324p microcontroller, the code can be deployed in the Arduino and run the program without using an outside hardware programmer. Arduino has digital and analog input and output pins for get connected with microcontroller and various IoT devices.

C. LCD 16X2

The LCD 16x2 is having 16 character on each line and 2 such lines are there. And it is having data pins, output pin, anode and cathode pins and one ground and one voltage pin. And it is having register select pin, in the register, it is having two registers command register and data register. For initializing and clearing screen, command register and to store the data, data register is used. And one enable pin, one read/write pin.

D. ACS712 Sensor

ACS712 IC is used to measure the current by using Hall Effect and its starting voltage is 5V. It will measure both AC and DC current. And it is very easy to contact with any microcontroller, from the microcontroller you can read the vales produced by the sensor [17].

E. 10k ohm Potentiometer and Resistor

Potentiometer is one type of resistor only and it having three terminal, two are fixed ends and one variable end. It is used as a variable resistor. It is used for adjust the resistance instead fixed resistance, in the paper it used for adjusting the LCD brightness and it can be used in the audio devices also to reduce the volume.

Resistor is used to reduce current flow or to reduce voltage levels in the circuit in case any high voltages are there. Resistor avoid the circuit damage.

V. RESULT AND DISCUSSION

Fig. 3. Smart Energy Meter

The above Fig. 3 shows the smart energy meter setup, which shows the power consumption by the load (electric bulb on the left) on the lcd(on right) is 1.09 kilo watts, thousand kilo watts is equal to one unit and the price is updated according to the standards of the concerned authority.

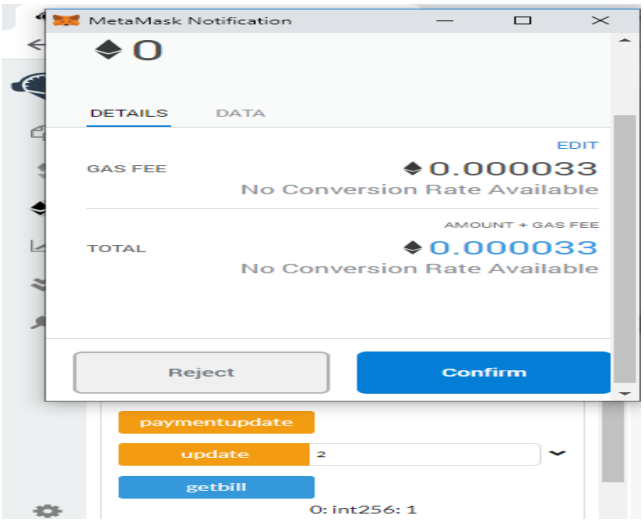

Fig. 4. Providers Smart Contract

- Those power readings we are storing in the blockchain as shown in the below diagram for every update metamask will ask you for some gas fee.
- Gas fee nothing but cost per the transaction in the network.
- In the Fig. 4, the provider side smart contract is shown and updating the bill is also shown and you can see every information about the blocks in etherscan.

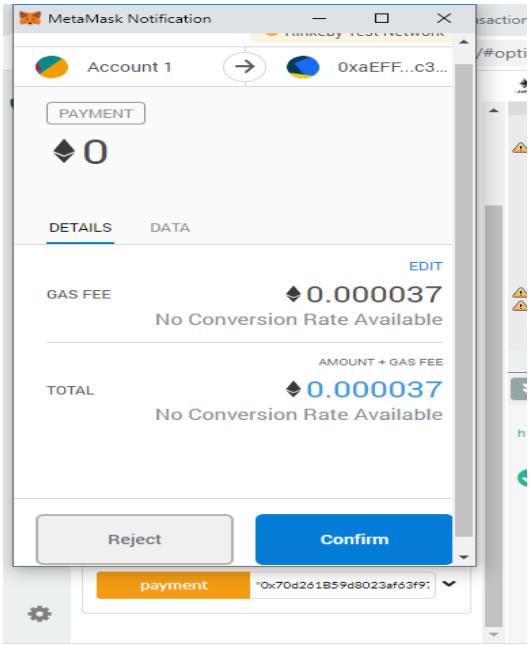

Fig. 5. Payment from Customer

The Fig. 5 represents the customer smart contract, here how much the bill amount is finding through the functions in the smart contract and the payment is done through payment function by providing the address of the bill provider.

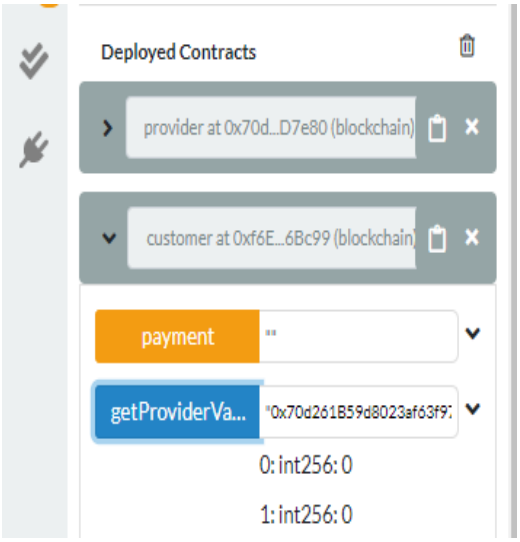

Fig. 6. Payment Checking

- Then you can check the bill, if the payment is done or not is shown in the Fig. 6.

Table- I: Energy Consumption Readings by the Load

Time (hours)	Readings (Watthours)
0.05	0.11
0.1	2.78
0.15	5.99
0.2	9.1
0.25	12.13
0.3	14.95
0.35	17.78
0.4	20.69
0.45	23.19
0.5	25.75
0.55	28.29
1	30.84
1.05	33.54

In the above Table- I, the readings of the energy consumed by load for every five minutes is shown and the readings are in watthours, we used here the 15watt(night lamp) bulb is used as load to generate these values, it consumed approximately 34 watts for one hour. 1 unit is equal to 1000 watthours so according to that we can measure the bill.

VI. CONCLUSION AND FUTURE WORK

In this paper we proposed a smart energy meter to provide more security of the user's data integrating with the blockchain technology. The energy meter will be able to find the energy consumed by the load and then it will upload the data into the blocks, by this overhead of the updating the readings from every house is reduced and man power also reduced and it is also cost effective because of we are using very less cost microcontrollers and sensors. As discussed in the paper, securing the data with the blockchain is achieved successfully, and also getting the power readings from the proposed energy meter and storing the values in to the blockchain done well. And the future work to improve our work is to upload the energy meter readings automatically, then it is very useful and also we can say that security is well established.

REFERENCES

1. Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT integration: A systematic survey. Sensors, 18(8), 2575.
2. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.
3. Lestari, D., Wahyono, I. D., & Fadlika, I. (2017, November). IoT based Electrical Energy Consumption Monitoring System Prototype: Case study in G4 Building Universitas Negeri Malang. In 2017 International Conference on Sustainable Information Engineering and Technology (SIET) (pp. 342-347). IEEE.
4. Barman, B. K., Yadav, S. N., Kumar, S., & Gope, S. (2018, June). IOT Based Smart Energy Meter for Efficient Energy Utilization in Smart Grid. In 2018 2nd International Conference on Power, Energy and Environment: Towards Smart Technology (ICEPE) (pp. 1-5). IEEE.
5. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. Computer Networks, 141, 199-221.C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

6. Huh, S., Cho, S., & Kim, S. (2017, February). Managing IoT devices using blockchain platform. In 2017 19th international conference on advanced communication technology (ICACT) (pp. 464-467). IEEE.
7. Patel, H. K., Mody, T., & Goyal, A. (2019, April). Arduino Based Smart Energy Meter using GSM. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1-6). IEEE.
8. Yaghmaee, M. H., & Hejazi, H. (2018, August). Design and Implementation of an Internet of Things Based Smart Energy Metering. In 2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE) (pp. 191-194). IEEE.
9. Mishra, J. K., Goyal, S., Tikkiwal, V. A., & Kumar, A. (2018, December). An IoT Based Smart Energy Management System. In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-3). IEEE.
10. Jiang, Y., Wang, C., Wang, Y., & Gao, L. (2019). A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management. Sensors, 19(9), 2042.
11. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411.
12. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems.
13. Arif, A., Al-Hussain, M., Al-Mutairi, N., Al-Ammar, E., Khan, Y., & Malik, N. (2013, March). Experimental study and design of smart energy meter for the smart grid. In 2013 International Renewable and Sustainable Energy Conference (IRSEC) (pp. 515-520). IEEE.
14. Rahman, M. M., Islam, M. O., & Salakin, M. S. (2015, May). Arduino and GSM based smart energy meter for advanced metering and billing system. In 2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT) (pp. 1-6). IEEE.
15. Sharma, P. K., Chen, M. Y., & Park, J. H. (2017). A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access, 6, 115-124.
16. Conoscenti, M., Vetro, A., & De Martin, J. C. (2016, November). Blockchain for the Internet of Things: A systematic literature review. In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) (pp. 1-6). IEEE.
17. Depuru, S. S. S. R., Wang, L., Devabhaktuni, V., & Gudi, N. (2011, March). Smart meters for power grid—Challenges, issues, advantages and status. In 2011 IEEE/PES Power Systems Conference and Exposition (pp. 1-7). IEEE.
18. Prapasawad, C., Pornprasitpol, K., & Pora, W. (2012, December). Development of an automatic meter reading system based on ZigBee PRO Smart Energy Profile IEEE 802.15. 4 standard. In 2012 IEEE International Conference on Electron Devices and Solid State Circuit (EDSSC) (pp. 1-3). IEEE.
19. Sun, Q., Li, H., Ma, Z., Wang, C., Campillo, J., Zhang, Q., ... & Guo, J. (2015). A comprehensive review of smart energy meters in intelligent energy networks. IEEE Internet of Things Journal, 3(4), 464-479.
20. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184-1195.

AUTHORS PROFILE

Vasa Vinay, pursuing M.Tech in the field of Computer Science and Engineering from Vellore Institute of Technology, Vellore and B.Tech in the field of Computer Science and Engineering from Narasaraopeta Engineering College, Narasaraopeta. His major research interests includes IoT, Blockchain, Database and Android Applications.

KS. Sendhil Kumar works as an Associate Professor in School of Computer Science and Engineering at VIT, Vellore. He received his PhD in Computer science and Engineering from VIT, Vellore, ME (CSE) from Anna University and BE (CSE) from University of Madras. He has twelve years of experience in teaching and research. His research interests includes cloud computing, IoT and big data.