Framework For Securing Automatic Meter ReadingUsing Blockchain Technology

Esraa Dbabseh* Radwan Tahboub†

Abstract

The Automatic Meter Reader (AMR) for energy consumption is one of the most important issues in smart cities, as meters and electricity companies suffer from insecurity. The Internet of Things (IoT) can be used to achieve effective and reliable AMR in real time. Blockchain is a very advanced technology and technology that can be used to secure transactions such as meter readings and meter control. It is based on the idea of sequencing data blocks in a secure and distributed manner. Ensures the security of the blockchain representing the data in each block (reading the meter for example). The block is created and verified by many devices distributed on a network. Blockchain can be implemented in various ways and environments such as the Ethereum platform. In this paper, we will present a new automated meter reading platform using blockchain technology to meet the complete security requirements of AMR systems. When DoS attack was launched, requests did not affect the data itself, but the response speed of the blockchain network to incoming transactions from the servers was reduced very slightly. In addition, the results show that Blockchain could provide a promising technology that can participate in securing network meters.

Keywords

AMR, Blockchain, Ethereum, IoT, Smart Contract .

*College of Graduate Studies and Sc. Res. Palestine Polytechnic University. Email: 131076@ppu.edu.ps

†Departement of CE, College of Information Technology and Computer Eng.Palestine Polytechnic University. Email: radwant@ppu.edu

1 Introduction

The development of technology and the existence of the Internet play a vital role in all areas of life. One of the most important of these applications and technologies is the Automatic Meter Reading Technology(AMR). The automatic meter reading is intended for remoting, monitoring and controlling of the local energy meters. This technology enables regular meter reading without visiting every home. The reading can be achieved with a micro-controller that continuously monitors and records the meter reading in the databases [5]. The data is transmitted by using the internet to achieve efficient and reliable AMR in real time. The automatic meter reading will be the consumer friend, because it takes care of all the problems that a consumer could potentially present and fully in control of the power board. Automated metering uses online applications, these apps mostly deal with databases that must be protected which they often contain sensitive data . Database serves a large number of users. Attention needs to be focused on many attacks, whether single or group. Therefore, the applications should provide security and don't allow unauthorized persons to access and read this data without knowing its details; Otherwise, the data loses its meaning and value [8]. There has been a lot of results aimed at sending data over the Internet of Things and storing it in the cloud and other solutions. But these solutions are still central and there is a third party controlling them[3]. One of the technologies that has appeared recently is blockchain technology that has changed a lot of applications, because it has a lot of features that makes it stands out from the rest. The most important of these features is that it is distributed and decentralized. The idea of the blockchain is a network that contains a large number of users who sends transactions to each other. These transactions must be validated and all values verified before entering the blockchain. Data and transactions

are accepted and added if it's validity is proved by so-called miners. Validate these transactions by solving mathematical equations that are present within each transaction. Thus, makes this technology powerful and distinct from others [14].

2 Background

This chapter provides a background and an introduction to the automatic meter reading and its importance, after which an overview of the blockchain and its implementation methods will be presented, and then an overview of the ethereum smart contracts.
AMR technology allows the automatic collection of consumption and diagnostic data from meter. This can lead to decrease labor costs and more accurate billing. Basically, the meters are equipped with sensors that register the meter automatically. These sensors then transfer the data electronically. The data is then transferred to a central database for billing and analysis, which reduces the chance of input errors. These meters help in accessing accurate and up-to-date data from meters and closely monitor and control energy costs. These meters also help solve many problems, especially in reaching remote areas that are difficult to reach periodically [6].
Cryptographic technologies are based on the science of cryptography, which protects sensitive information that cryptographic techniques use to restrict behavior instead of using trusted third parties. Blockchain is a series of continuous data records called blocks that are linked together and secured with cryptography. Based on a peer-to-peer topology, the blockchain is a distributed ledger technology that allows data to be stored globally on thousands of servers while allowing anyone on the network to view anyone else's entries in nearly real time. This makes it difficult for a single user to control with the network. A blockchain begins when the user sends transaction to other user and transactions are enabled, although they can be tracked, but are anonymous. Public keys are cryptographically generated addresses stored in the blockchain. The amazing feature of blockchain is that public keys are never associated with a real-world identity. The blockchain is a decentralized network that contains a shared, unchanging authority ledger, which means that the information inside the authority leader is open and available to all. The blockchain network is transparent and this feature makes its reliable [9]. This technology, is an easy way to pass information in a completely secure way. The block is created and verified by thousands of devices distributed on the network. It is added to the previous group of chains and stored across the network. If someone wants to forge a single transaction, they are forced to change the entire previous chain and this is almost impossible. So the data is not changeable and the database is managed using a peer-to-peer network. Ethereum is a decentralized computing platform. It generates a cryptocurrency token known as Ether. Ethereum was released in 2015 and is open source software for major chains used in cryptocurrencies and ether. It enables the creation and operation of smart contracts and distributed applications (DApps) without any interruption, fraud, control or interference from a third party. Ethereum helps developers create and deploy distributed applications, not only because it is a platform but also a complete Turing programming language. There are two types of accounts: the first type is externally owned accounts that are controlled by private keys, and the second type is the contract account that is controlled by its contract code. Miners use this algorithm to verify the validity of a transaction before adding it to the chain of blockchain[11].

3 Literature Review

There are many different new technologies used to read meters, the most important one is that which uses Internet technology. AMR can be classified into wired and wireless systems, depending on the medium used to transmit the readings. Both systems have advantages and disadvantages. Measuring power over the wire is an expensive system because it requires a change in the infrastructure compared to wireless units. WIFI is more suitable for this type of application because WIFI has become one of the common facilities everywhere [1]. Here we will talk about different techniques and methods described by the authors. Wessam Mesbah, Senior Member [7] Authors discuss a new way to secure meter reading against tampering or malfunction to discover and correct customer attacks that aimed to change smart meter readings. The idea of linear error-correcting block codes was used, which was used in a system of Communications to detect and correct errors in data transmission. It was suggested to use codes with some modifications in order to detect false readings in some meters that measure electrical energy. Xingyuan Fan, Chun Zhou, Ying Sun, Jinyang Du and Ying Zhao

[4] Authors proposed designing a new generation of meter-based meter reading system through Narrow Band Internet of Things (NB-IoT) technology. The direct connection between the power meter and the main station system was achieved. The intermediate equipment measurement station was deleted and the complexity of the current intensive copy platform structure was reduced. The central management and real-time monitoring capacity of the power meter was improved, and the group coverage rate was improved effectively. Also the number of connections to one base station can be increased easily. The smart meter connects directly to the NB-IoT network via a remote connection unit that supports the standard NB-IoT connection. Pranav Singhal, Sakshi Upadhyay, Sheenam and Annurudh Pratap Upadhyay [10] Authors proposed the smart power meter uses IoT technology to monitor and manage energy. The system was designed to resort in a local server and database when the internet connection was resumed. In this research, a digital power meter consisting of blinking LED signal was used. It is coupled with a controller using Optocoupler. This microcontroller reads data and sends it to the IoT platform using the WiFi unit. Sequentially transmits data to the IoT platform for display where power meter readings can be accessed globally. The reading of energy consumed is displayed on the platform website. Energy consumption reports are generated daily and can be monitored around the clock at any time.

4 Blockchain Based AMR Framework Design

The proposed model aims to create a hybrid model consisting of a cluster of servers with a blockchain, in order to maintain electricity meters and read data, as well as many of the features available. This improves the safety of multiple attacks and also monitors and controls meters. The proposed system has two main components. The first is a network of smart meters distributed in the regions of customers. It consists of a control panel through which data is read and displayed on the LCD screen. The second component is the blockchain network, the data coming from the meters will be used as input to the blockchain network, whether for examination, control, or preservation. This app is used to store meter reading for all users. These components will be used to prevent multiple security attacks. Figure 1 shows an overview of the frame structure. As shown in the figure, any server must participate in the blockchain network in order to preserve the network and its data as well as obtain the benefits of using this framework. Each group of meters belongs to a specific server. The use of blockchain within the proposed framework is to preserve data and prevent multiple attacks.

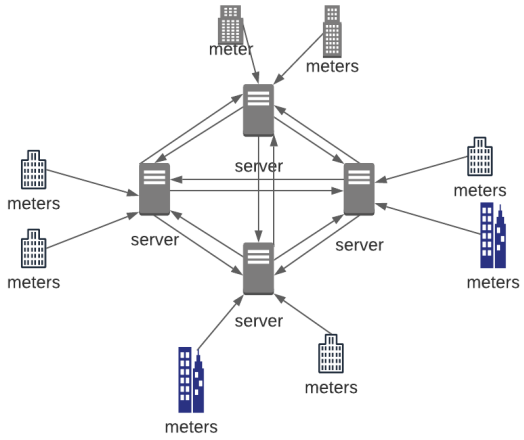

FIGURE 1: General Architecture of the Proposed Framework

The server is part of a blockchain network. One of the server's tasks is to send the received data from the meters and save it to the blockchain network. Each server stores the data in the blockchain network through transactions. In a smart contract, the addresses of servers that are allowed to read and write in the blockchain network are defined. Since the server is part of the blockchain network, each server has a unique address in the blockchain network. If the address is one of the allowed to write on the blockchain network so the data will be received from the server and stored. To increase safety of the received data from the meter to the server, it will write the data after making sure that the current reading value for this meter is greater than or equal to the previous value, in order to ensure the correctness of the upcoming data.

A smart contract defines the rules between different organizations in executable code. Applications call a smart contract to create the transactions that are recorded in the ledger. Using the blockchain network, we can turn these contracts into actionable software. Smart contracts are applications that are published in the authority book and executed independently as part of the validation of transactions. Once the contract is created, the address and balance are also created for it. Smart contract is written in several languages, but

the language used to write nodes is solidity, which is the JavaScript language developed for writing smart contract. Figure 2 shows, the smart contract that was used in the proposed work is a deal within the Ethereum blockchain. In this decade, addresses of users able to write into the blockchain network were identified. For example, in our reseach the server is part of the blockchain that receive data from the meters. the servers are the blockchain network users who can send the data to the smart contract and which has to save the data.

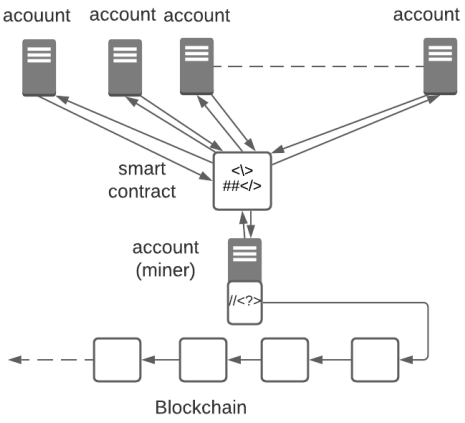

FIGURE 2: Smart Contracts Architecture

5 Proposed Framework for Blockchain Based AMR

In our proposed work, meter reading was secured between server nodes in the blockchain network. when an attacker attempts to write to a blockchain network, the address of the server that sent the data to the network will be verified from the addresses allowed to write to the blockchain network. Likewise, if the attacker was able to know a valid address, he wouldn't also be able to write, because he does not have the private key of the server on which the transaction is signed. So this network will be resistant to this attack [12].

Since the blockchain systems are independent and do not depend on any technology, the availability in the meter network using blockchains will be ensured. For the denial of service attack to succeed, requests are sent to one node because the system is central. As the blockchain is a decentralized system linked to multiple nodes, a denial of service attack needs access to the different nodes at the same time to damage the network. This prevents denial of service attacks through the decentralization of the network[13].

replay attack resends a previously sent message. And the data that are sent is correct, but duplicate. In a blockchain network when the attacker tries to send a previous reading saved in the blockchain network, this technology prevents this attack because every transaction (i.e. reading a meter) has an infrequent timestamp is used. It is placed so that a distinction is made between the original (first) transaction and that no repeat transaction is accepted after it. [2].

6 Implementation of The Framework

This section explains the practical approach and the implementation of the blockchain network on the prototypes used. Also, it demonstrates the effectiveness of the proposed framework and discuss response time and Latency on Transaction. Latency is the time taken to transmit a packet over the network. The main concerns of this research are writing on the blockchain network and reading from that network when needed. Whenever an attempt is made to implement writing or to make a connection to a blockchain network to read through specific addresses that are permitted to interact with this network, which are specified in the smart contract. Then these readings are sent after checking the addresses and comparing the current data with the previous one for this meter, the decision is to establish a connection to execute this transaction depends on the result returned from the ethereum blockchain. At the start of the trials, the ethereum blockchain Private Network was configured. Then the proposed contracts are also published in that blockchain. Since this work is based on ethereum smart contracts, a new experiment is underway to evaluate the response time for reading the proposed smart contract. Table 6.1 shows the response time for writing smart contract data. The results showed that the speed of response time was relatively acceptable in the experiment. On the other hand, in a true application server environment, the hardware specifications will be much better than the device used in our experience. This will positively enhance the response time.

TABLE 1: Response Writing Data to The Proposed Smart Contract.

of transaction	time(sec)
1	.27
100	19.5
200	41.07
300	61.98
400	82.72
500	90.5

Figure 3 and 4 illustrates measures of response time and latency for meter writing readings into a blockchain network. These results were for a simple sample of readings from the meters and typed on the blockchain network.

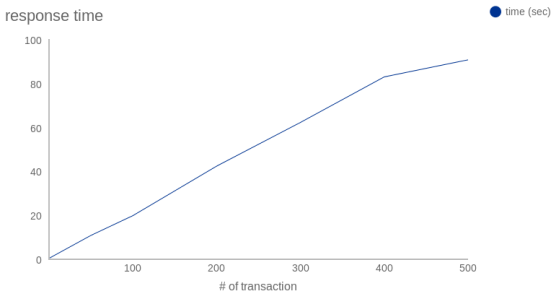

FIGURE 3: Transaction Response Time.

6.1 DDoS Experiment Results.

In our experiment, we studied the effect of the DoS attacks on the performance of servers connected with smart meters. The experiment was conducted by launching DoS attacks on servers, and then studied their strength against such attacks by analyzing their response time and their ability to communicate with the counting smart server while under attack. Packet generation tools can be used to build traffic or attack packets. For example, LOIC was used here. This tool performs a DoS attack by sending too many random data in the form of UDP, TCP or HTTP to the blockchain network to be dropped. The large numbers of packets are created per second and sent to servers. Figure 5 and 6 illustrate the effect of DDoS on transactions on a blockchain network, and the results of the experiments have also clearly shown that DDoS attacks had little effect on network performance. The responses from these servers to requests were very slow as these requests did not affect the data itself but rather the speed of the blockchain network's response to the transactions received from the servers is decreased. Also, this delay in response time was not significant and had no effects on the blockchain network. The response times were less than 0.4 ms before the DoS attacks. when testing DoS response times, they increased normally.

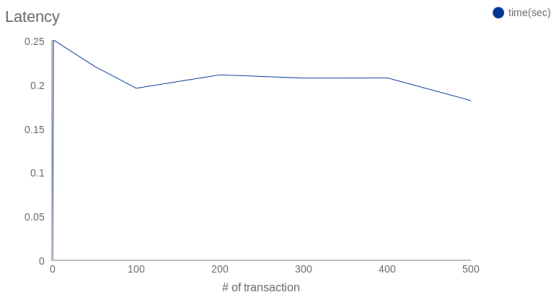

FIGURE 4: Transaction Latency

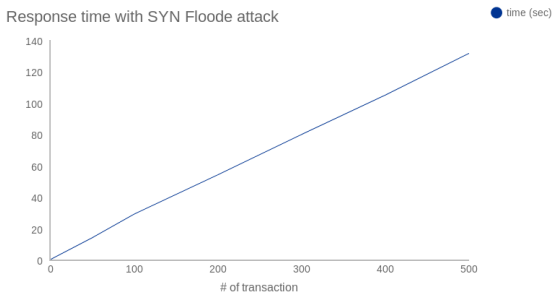

FIGURE 5: Transaction response time with DDoS Attack.

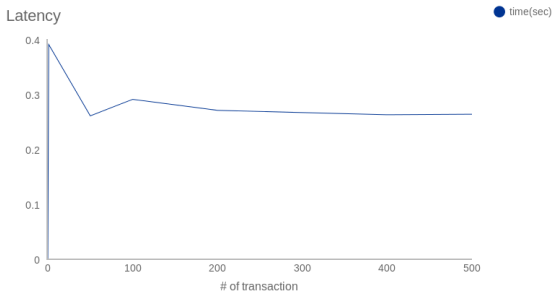

FIGURE 6: Transaction Latency with DDoS Attack.

7 Conclusion

In this research we create a blockchain network that receives data from meters and sends it to servers, and then they send the data to the blockchain network. Besides, we implement every server with an address in the ethereum network. It is through these addresses that data is sent and saved in the blockchain network. Blockchains are chains open to everyone who can read them. Transactions live in mempool before miner puts them in blocks. Generally, no one controls the blockchain so no one can go back to and change the data. As we saw in the results we cannot influence this network through the attacks, mainly because the networks are being paired and there is no need to trust the devices with each other, without a central point of failure. When miners are found, there is no need for central authority to tie one node with another or associate a user with access to another machine. In addition to studying the implementation of the blockchain network in smart meters and studying the effects of this proposal in terms of safety and security.

References

[1] Prachi Bramhe, Akshay Sarode, Vicky Bonde, Rachana Mankar, Ayushi Kesharwani, and Samiksha Dhengale. Automatic electric meter reading using wifi. 2019.

[2] Nutthakorn Chalaemwongwan and Werasak Kurutach. A practical national digital id framework on blockchain (nidbc). In *2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pages 497–500. IEEE, 2018.

[3] Amruta Chore, Prasad Mali, Dinesh Vyanjane, and Vijay Karewar. Iot based smart electricity meter and billing system. *Int Res J Eng Technol (IRJET)*, 5, 2018.

[4] Xingyuan Fan, Chun Zhou, Ying Sun, Jinyang Du, and Ying Zhao. Research on remote meter reading scheme and iot smart energy meter based on nb-iot technology. In *Journal of Physics: Conference Series*, volume 1187, page 022064. IOP Publishing, 2019.

[5] R Govindarajan, S Meikandasivam, and D Vijayakumar. Cloud computing based smart energy monitoring system. *International Journal of Scientific and Technology Research*, 8(10):886–890, 2019.

[6] Wen-xin LEI, Yi-xin JIANG, WEN Hong, Ai-dong XU, MING Zhe, Wen-jing HOU, and Yu-jun YIN. New features of automatic meter reading system: Based on edge computing. *DEStech Transactions on Environment, Energy and Earth Sciences*, (icepe), 2019.

[7] Wessam Mesbah. Securing smart electricity meters against customer attacks. *IEEE Transactions on Smart Grid*, 9(1):101–110, 2016.

[8] Oscar Novo. Blockchain meets iot: An architecture for scalable access management in iot. *IEEE Internet of Things Journal*, 5(2):1184–1195, 2018.

[9] Marc Pilkington. Blockchain technology: principles and applications. In *Research handbook on digital transformations*. Edward Elgar Publishing, 2016.

[10] Birendrakumar Sahani, Tejashree Ravi, Akibjaved Tamboli, and Ranjeet Pisal. Iot based smart energy meter. *International Research Journal of Engineering and Technology (IRJET)*, 4(04):96–102, 2017.

[11] Dejan Vujičić, Dijana Jagodić, and Siniša Ranđić. Blockchain technology, bitcoin, and ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)*, pages 1–6. IEEE, 2018.

[12] Merrill Warkentin and Craig Orgeron. Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, page 102090, 2020.

[13] Rui Zhang, Rui Xue, and Ling Liu. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, 52(3):1–34, 2019.

[14] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. IEEE, 2017.