ISSN 2047-3338

Blockchain Based Efficient Peer to Peer Authentication Model for Security and Privacy Challenges of Internet of Things (IoT)

Rizwan Ali, M. Junaid Arshad
Department of Computer Science, University of Engineering and Technology, Lahore, Pakistan

***Abstract*-- Nowadays, the Internet of Things (IoT) have very crucial part in the life of our planet and in this system of things, there is a lot of exchange of fully automatic data, so for these objects, there is need to be verified and maintenance of data with verification of authenticity, because these objects are always targeted. There are catches for abuse. Given the nature of the IoT, it's almost impossible to imagine a centralized system for this parable. In this piece of research work, a decentralized system called a zone of trust has been proposed for creating the authenticity of data using blockchain. This is our best safe bet for maintaining data integrity with flexibility sustainability hinges. Each bubble has a manager that gives all its members a ticket which allows objects to use their ticket to prove their identity in the blockchain. This system uses asymmetric encryption algorithms to verify the authenticity of message encryption.**

***Index Terms*—IoT, Blockchain, Security, Privacy, Attacks, Bitcoin, Threats, RSA and Ledger**

I. INTRODUCTION AND PROBLEM STATEMENT

TODAY, with the ever-increasing use of the IoT in life, Issues Including the security of this case need attention. To solve these security issues related to IOT distributed approach is used. The determination of the mentioned proposed model is to plan a decentralized system for authentication of objects on the IoT. At present, the IoT is involved with all aspects of our livings. According to recent studies in the year 2020 more than fifty billion devices will be linked to the Internet, so cities are moderately replacing their houses or places of residence. Equipped with smart appliances like intelligent Televisions, smart central heating control systems. IoT plays a key role in making cities smart and objects with Internet access. It reduces gas production by CO2 with help of IoT all over the internet, Ham Barry's other functional tools making cities smart, including intelligent waste management, environmental management, smart transportation systems, and it has a smart traffic management system.

The idea of using the IoT is to have a large number of modules present in many services that are interoperable with each other. Any or all physiques of virtue have virtually immense and the other hand can produce content that everyone can access, regardless of their location. On the other hand, the only thing that has been authenticated can use this system security is important. Otherwise, this system is exposed to plenty of security risks such as robbery Information which is the replacement of usurpation information. Therefore, security agents are the most important obstacle to its progress. Many researchers describe the Internet of Things as a system of systems. In some cases, this system should only be used by trusted users. So the requirements are conventional security including authentication, data privacy for all purposes of this system including objects is a key part of important software programs. However, because of the diverseness of resources, electronic equipment, and existent security measures solutions are incompatible with such a system. Apart from this combination of several security technologies are required but this leads to additional costs of the system.

Furthermore, solutions that provide effective security are often centralized, such as public-key infrastructure [1] (PKI) may be the reason for the creation of tremendous flexibility in the surroundings and that has become thousands of users. Finally, the use of this system security builds multi-faceted actions that make parables there are many ways to integrate services into new scenarios. Consequently, provide a complete security solution for Barry is a total disadvantage. The solution should be 1. Easy integration of new devices 2. Also, provide new services. Completely meet the needs of the Internet of Things 3. Devices also do not have the type of architecture used to design it optimally. In the article "Managing the Internet of Things using Blockchain", [2] Security of the IoT is better introduced than any object with a smart contract that Specifies its behavior to be connected to the blockchain, which better permits any object of any mythic object. It also gives. In most previous instances of Internet security, objects are key Are used for cryptography, which does not prevent the presence of mythic objects. Acknowledging the authenticity of the doctrine.

II. BACKGROUND

A. IoT

IoT first introduced in the summer of 1999 by Kevin Ashton but at present, Kerr is working on moving toward the widespread use of this technology. The concept of the Internet is the objects connecting different devices to one another over the Internet. With the help of IoT, applications of various devices can even connect to each other through the Internet talk about interaction. For example, smart refrigerators that are connected to the Internet notify you of the stock expiration date of refrigerated foods.

B. Blockchain

Blockchain is decentralized database that keeps record of transactions permanently and without changes [3]. Blockchain is a circulated record that takes the necessary steps of following exchanges soundness and disentangles the benefits in a hexagonal framework. Blockchain makes its name simple on straw Transaction information in obstructs that are interconnected to frame a chain doing so the number of exchange increments, so does the blockchain. Using peer to peer, a blockchain is completely decentralized. A simplified version of a blockchain is displayed in Fig. 1.

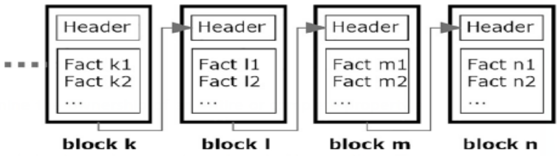


Fig 1: The block data of blockchain

C. Asymmetric encryption

There are two important cryptographic algorithms in the cryptographic debate: symmetric and asymmetric. The asymmetric encryption procedure uses two changed keys and there is a mathematical relationship between them. Which holds these keys as the private key and we know the public key that makes a pair of keys together. The working process includes message encryption and decryption. Here message is encrypted with a public key and encoded message is decrypted with a private key, and keys are transferred through secure communication. The algorithm working is shown in Fig. 2.

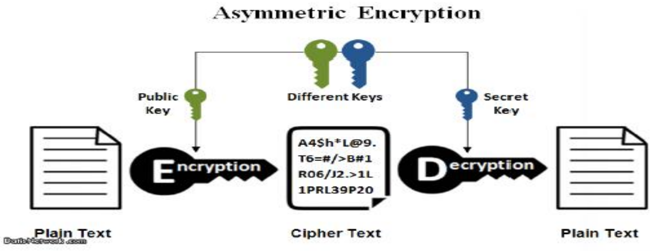


Fig. 2: Asymmetric Encryption

D. Bitcoin

Bitcoin is first and most popular application that runs on top of blockchain. Bitcoin is a cyptocurrency and digital payment system depends on public blockchain [4]. Bitcoin uses proof of work consensus mechanism for blocks validation process. In bitcoin each block is divided in two parts. First part is called header which includes timestamp, hash of its transaction data and hash of previous block. In verification process, receiver node verify the transaction as well as its proof of work (POW). In bitcoin, the operation of blocks updates occur after every 10 minutes.

E. Ethereum

Ethereum is public blockchain platform which provides digital currency caller ether (ETH). In ethereum, blocks have ability to store records and smart contracts. Contract is basically a transaction protocol. By using smart contracts in ethereum decentralization network is achieved. All the nodes of system run this contract on an operating system called ethereum virtual machine (EVM). Here validation process takes only 14 seconds due to small size of block while bitcoin takes 10 minutes. Ethereum uses GHOST protocol for consensus mechanism and reward is given to miners. In this process, a miner that validates the block, receives 5-Eth and also receives gas. Ethereum uses proof of work mechanism for validation process.

F. Hyperledger Fabric

Hyperledger does not provide cyptocurrency unlike biotin and ethereum. It is open source blockchain which is created by Linux and IBM. In this platform nature of information decides that the transaction can be public or confidential. Hyperledger uses PBFT as a consensus mechanism [5]. PBFT is used in decentralized networks in which some degree of fault can tolerated for normal execution of system operations [6]. In Hyperledger, smart contracts are applied called context chain codes.

III. REQUIREMENTS FOR SECURITY

An IoT plot must satisfy various security necessities so as to guarantee the supportability and strength of the scheme. Hence, this particular segment, we depict the fundamental security objectives, and we acquaint the benchmark required by assessing the suitableness of confirmation plans for verifying IoT usage scenarios.

- Integrity
- Availability
- Scalability
- Nonrepudiation
- Identification
- Collective authentication

A. Model of Threat

This part of the work gives an overview of our proposed threat-related model.

B. Model for network

The general reason for an authentication conspire is to enable various hubs to impart in a reliable manner over a known confided in organize. In our proposed research work, we study a system that claims a lot of real-world appliances offering and utilizing distinctive IoT benefits in a brought together or dispersed engineering. The system work comprises of just sending parcels and doesn't give any security assurance, for example, trustworthiness or authentication. Therefore, a vindictive client can peruse, change, drop or infuse arrange messages.

C. Model for attacker

Our proposed research work mentioned that, we accept that an aggressor or pernicious client has all-out power over the pre-owned system i.e., client can specifically be able to sniff the messages, drop the messages, replay the messages, reorder the messages, infuse the messages, delay the messages, and change messages discretionarily with unimportant postponement. Be that as it may, we don't think about physical assaults on gadgets, where the aggressor can recover a few the entirety of the item's insider facts, for example, Priv. keys. We accept that articles are secured versus forcible assaults so there it subsist various techniques to shield them from such assaults by making this data discernible just by the gadget itself [7].

D. Attacks

An attacker can have different objectives, for example, sending incorrect data so as to misdirect the framework's choices or the refusal of the framework's administrations. Therefore, it can lead to various assaults:

- Sybil attack:
- Deception attack:
- Substitution of message attack:
- Attacks related to denial:
- A replay of message attack:

An overview is displayed in Table I.

Table I: Proposed model assessment benchmark

Assessment benchmark	Included or not
Mutual authentication	Yes
Integrity of data	Yes
Message removal	No
Scalability	Yes
Message substitution	Yes
Confidentiality	No
Sybil attack	Yes
Spoofing attack	Yes
Nonrepudiation	Yes
Message replay	Yes
Integrity of messages	Yes
DoS/DDoS administration	Yes

IV. RELATED WORK

Internet of things (IoT) is gaining special attention especially in case low power loss network (LLNs) which has constrained resources because of high speed internet and smart devices. IOT systems represents a network in which devices called “things are connected through a dedicated or open network” and sensors are attached to these IOT devices. Different researchers have done work on the integration of blockchain into IoT biological systems. Be that as it may, not many works were keen on how blockchain meets the security needs related to help in IoT. In the mentioned segment, we overview practically every one of the works that expect to acknowledge such coordination and show the uncommonness of works that understand the reconciliation so as to address security issues.

S. Huh et al. [2] propose a way to deal with coordinate blockchain to IoT. Their methodology depends on con-calculating each article by a devoted smart contract that defines its activities. Be that as it may, authors' research work is in earlier stages till the time of this writing. Similarly [8] gives an idea of blockchains and agreements can be included in IoT.

Blockchains decentralized approach encourages integration of IoT to overcome security problems. Tandon [9] has done a deliberate investigation of the different difficulties associated with IoT separately and furthermore the points of interest and difficulties of coordinating it with the blockchain framework. Catchphrases—Blockchain, IoT, challenges, security, joining. In their research work [10] the primary motivation behind this examination is attempting to expand trust among farming store network gatherings to ensure the nourishment quality, wellbeing and supportability from an inventory chain the executives point of view, and the key problem is utilizing a distributed innovation which isn't reliant on the belief of a focal position or association for the entire production network. In referred research work [11] authors suggested a fresh Service-Oriented Architecture (SOA) considering a blockchain of semantic nature for enlistment, revelation, decision, and portion. Such undertakings are actualized as sharp understandings, allowing spread implementation and believe. The authors of this research work [12] give a blockchain-based design for IoT.

For secure IOT systems [13], physical interface should be secured. Deprived human security, software entree and tools used for analysis and repairing may be compromised by insecure physical interface and results in malfunctioning of systems. In their research [14] work, authors propose NormaChain, a blockchain-based standardized self-ruling exchange settlement framework for E-business in IOT platform. By structuring an exceptional three-layer sharing blockchain organize, they can essentially build exchange proficiency and framework adaptability. Table II summarizes the surveyed work.

Table II: Concise of Existing Work

Methodology	Identifiable	Type for blockchain	Application
R. A. Memon (2019)	No	Public	Yes
C. Liu, (2019)	Yes	Private	No
Dorr. et al. (2017, 2018)	Yes	Private	Mock-Up
Xui et al. (2018)	No	Unspecified	No
Hu et al. (2017)	No	Public	Yes
Rizwan Ali (2020)	Yes	Both	Yes

V. PROPOSED METHODOLOGY

In the previous section, we looked at the overall structure of the IoT and the blockchain Internet, defining trust zones to provide security for the objects in the IoT system. We have used an open blockchain because of heterogeneous use cases so that new node can be entered and scalability issues can be resolved. That is the main reason that why private blockchain in not considered here. Upon using a private blockchain, it makes our technique available for only predefined customers and new customers will not entertained, due to scalability and flexibility issues arises. If the main blockchain verifies first Sender «A» then the system approves the message exchange. Now the second sender e.g., «B» is able to peruse this specific message. In this whole process, we portray the entire lifespan of and object in IoT biological system which executes the trust zone proposed approach. Now at third step model is designed and train for IoT and blockchain standards. After validation proposed system is evaluated on a given blockchain and IoT network with the ECC algorithm.

A. Initial Phase

In each zone, an object is designed as a zone manager that holds a pair of private/public keys and any device can be a manager. The manager makes a private/open key pair for every adherent. This speaks to the general population key of the adherent, a marked structure that is the zone supervisor's mark with the ECC[15]computerized signature calculation utilizing a private key.

B. Suggested Model

To accomplish such a framework, we utilize a blockchain in the event that an object ‘A’ wants to communicate with an object ‘B’, at that point the sending node ‘A’ firstly sends some message to the main blockchain. And if the main blockchain verifies the sending node «A» then the whole system approves the message exchange. Now the second sender e.g., «B» is able to peruse this specific message.

C. System Functionalities

In this section, we will examine the different phases of the proposed system. This part of the research work is divided into several sections which we explain one by one in an easy manner. Another thing to be noted is that we present an algorithm which acts as the base for the complete proposed system.

First, we start from first phase or also called Phase (A) where the objects that are connected to the system can be of any type. It may be a medical system for hospitals, smart parking management, Mobile management, or home automation.

In phase (B) the group manager sends the request to form the zone to the blockchain. Transaction the zone making request contains both the manager's name and the zone name. The blockchain first checks that there is no group with that name before and also checks that no one with that name is already a member of another group. The zone making transaction is then stored in the chain.

During the phase (C) People who want to become a member of each zone first ask the manager of that zone then the manager issues them a ticket and manager assigns the ticket with his own private key. In the succeeding phase, the follower joins the bubble after receiving the ticket from the manager. The blockchain first checks for the zone manager's public key to be valid and then checks that the name is not already in a group and its name is unique.

Phase (E) defines a process when a transaction seeker succeeds in adding to a zone (a follower succeeds) in subsequent requests well there is no need to use your ticket for authentication. Phase (F) shows how blockchains can control access to objects and transactions. The last stage depicts a worldwide perspective on the environment. The ensured modules or objects (containing tickets) able to be added to their gatherings whenever needed.

D. Complete Proposed Model Architecture

The overall architecture of the system consists of zone manager segments, trackers in each zone and blockchain, including the number of zones in which each zone contains a number of objects, and the blockchain is constructed containing all bubble information and all objects and this chain is unmanageable. The manager triangulates the zone with a single name and records the zone information in the blockchain. The manager issues tickets for objects that are intended to be added to the node. Followers can only become members of a zone by offering tickets and cannot create a new zone. Followers need authentication using tickets to add to the blockchain to establish transaction owners. When the intelligent contract is developed and already sent to its corresponding blockchain with help of exchange now it’s on miners to approve it and miners must approve it if it is legitimate. On the off chance that the approval is fruitful, at that point, the agreement's proprietor gets a location which refers the contract in the blockchain. This location is open and can be used by any user without any restraints. To abridge, contingent upon the article's sort, the savvy agreement's standards are applied as pursue:

A blockchain-based system includes the following:

- Node(object)
- Transaction
- Blockchain
- Extractor
- Agreement/contract

Each node on this system has a complete copy of the whole blockchain. Complete working of the proposed system shown in Fig. 3.

- *Master/Manager:* can make just one air pocket utilizing an extraordinary gathering identifier, that doesn't belong in the blockchain. The Manager's job is just marking new tickets. In the event that a Master is out of administration, it doesn't upset the working of the air pocket (aside from including new gadgets).
- *The follower:* (1) is related just if its air pocket exists; (2) can't have a place with more than one air pocket; (3) can't make another air pocket; and (4) its first exchange requires a confirmation, utilizing a ticket marked by the gathering's Manager Key which is called private key.

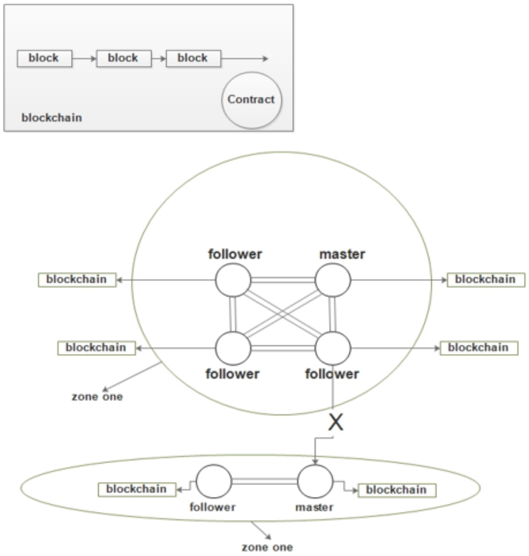


Fig. 3: Overall proposed system architecture

- *The Both Entities:* (1) the item symbol must be special, (2) the article's open location and the pair of the key must be one of a kind; (3) messages must be traded between hubs having a place with a similar air pocket. (4) Every one of the exchanges must be marked and confirmed. Our methodology depends on an open blockchain, which brings huge points of interest:
- *Blockchains* are exceptionally strong decentralized frameworks, which causes our way to deal with acquiring those highlights;
- *Referred to open blockchains*, for example, Bitcoin and Ethereum are extremely vigorous against misrepresentation and adjustment, in this way, put away data about trustful hubs are solid;
- *Open blockchains* are self-governing in guaranteeing their own working (approval of squares, accord, and so forth.)

VI. RESULTS AND DISCUSSIONS

As portrayed over, the intensity of our proposed methodology depends on its reasonableness to most IoT situations, all inside guaranteeing a simple mix of new gadgets, administrations, and use cases. In this segment, we assess our methodology in regard to its execution time, vitality utilization just as the budgetary expense of some utilization cases.

A. Use case scenarios

All the usage cases discussed in this stage of our proposed approach are related to currency and cost-effectiveness.

Shrewd house: is a house outfitted through extraordinary composed hook up to engage occupants to distantly mechanism or suite a great deal of motorized home -based electronic contraptions.

Controlling of waste: This one is an expanding issue in urban areas especially in the metropolitan's cities. Major and realized issues in the dump automobile course [16]. A smart processing plant is described by a self-sorted out the multi-operator framework that helped with enormous information based criticism and coordination [17].

Intelligent street radar: an intelligent road radar can be controlled without human intervention and are installed on remote locations.

B. Scheme for Proposed Approach Evaluation

So as to assess the clock and might utilization of proposed methodology, we utilized two objects called nodes or end nodes: 2 different laptops 1 from Samsung and others for HP. Both systems use Linux Ubuntu as an operating system. HP laptop use Linux Ubuntu 18.04 as the main operating system and Samsung uses Linux Ubuntu 16.04 in a virtual machine on top of the Windows 8 operating system. One workstation was structured as a Manager or also called master and the opposite end-hubs as a worker or also called a follower. Table III depicts its highlights. The end node applications are created utilizing python language.

Table III: Experimentation setup features

Node	CPU arch.	CPU mode	CPU speed	RAM	OS
HP Laptop	X64	64 Bit	2370 MHz	4 GB	Ubuntu 18.04
Samsung Laptop	X64	64 Bit	2300 MHz	2 GB	Ubuntu 16.04(VM)

As depicted in the previous section, we utilized ETH as the blockchain. Our approach is based on built up the intelligent agreement which guarantees proposed methodology working utilizing language used for intelligent agreements called solidity. For the connections between end-devices and the blockchain, this approach developed a python API that encodes information from Ethereum. These associations are acknowledged utilizing JSON 10 RPC. In fact, our proposed approach utilized testrpc[18], which speaks to an Ethereum instrument to test and advancement determinations and this thing imitates cooperation to the technology of blockchain and this one does not include the overhead of in-execution genuine ETH device hub. The exhibited outcomes concern 100 experimentation where we estimated:

- The time required to develop a request for the purpose of the association,
- Clock time required to develop a data content message,
- Usage of power of CPU in developing of an association re-quest,
- Usage of power of CPU in developing of a data content message,
- Usage of power of NIC in the development of sending and receiving the responses,
- Usage of power of NIC in the development of sending and receiving a data content message.

In our proposed approach, we are just inspired by Follower utilization. Without a doubt, the Master needs just a single exchange to make the zone pocket. This exchange is equivalent to for a worker or also for a follower to relate for themselves, however in the absence of a ticket. Hence, it has a little sizing that prompts little correspondence reimbursement. When the secure zone is formed besides ticket generation process, the manager can also act as a follower node and can send or receive messages like other nodes.

C. *Results after Evaluation*

In this part, we have evaluated all security requirements of our proposed methodology by using a step by step approach.

Evaluation of the proposed security benchmarks

Here, we analyze how our proposed procedure fulfill the security requirements which were targeted at start and security is achieved by using decentralized setup. Furthermore, authentication, integrity and identification are achieved by using signatures:

- *Mutual authentication and messages integrity:* In this part we discuss two things, first, one authentication which is mutual in nature and the second one is the integrity of communication messages utilize by each object of the proposed framework. This is achieved through the process of generating tickets (purpose is for primary exchange) and this is explained as an endorsement comparable. Another advantage is that we used blockchain technology in our proposed approach which provides us a better layer of protection against attacks.
- *Identification:* This generated personality is very much reliable because we can get guaranteed by the sign of manager with the help of a manager special key called the private key.
- *Nonrepudiation:* In our proposed research work every message is signed with the help of a key called the private key. The private key distinctly identifies its creator object in such a way that only just proprietor can utilize it. Hence, it can't preclude the reality from securing marking a message.
- *Scalability:* Our proposed framework depends on an open blockchain, which, thus, depends on a shared system. It is realized that shared systems are probably the best answer to meet versatility everywhere scale[19].
- *Protection against Sybil:* The proposed approach provides very much protection against this type of attack. Here as we know each article must have just a single character and every personality and it has only one pair of the key at a specific time.
- *Avoid Spoofing:* All objects have their own special keys called private keys. So as this is implemented here no one can steal the identity of others and no chance of this type of attack.
- *Protection for substitution of message:* As we know that in this model all messages are signed or marked by a special type of keys called private keys. So to do this type of attack hacker need a legitimate private key. Be that as it may, just believed articles have been given tickets (substantial key-sets) at the introduction stage.
- *Protection against replay:* Here every communication reasoned as exchanges. Every exchange exists here with a timestamp and requirements an accord stage so as to be substantial. Kshetri[20] depicts how the technology of blockchains is hearty against these assaults.
- *Protection for denial of services:* The completely decentralized design of this approach makes it strong besides these types of assaults. To be sure, administrations are copied and appropriated over various system hubs.

Consumption for Clock Time

The segments 2–5 of given Table IV depicts the AVG and SD of the affiliation solicitation and information content planning time period registered more than hundreds of acknowledged investigations. This depicts the AVG and SD of the affiliation solicitation and information content planning time period registered more than hundreds of acknowledged investigations. The normal required clock time to understand an affiliation demand given as 1 and 55 ms in the case of HP. 12 ms for the HP and 0. 044 ms for the Samsung laptop.

Table IV: Time and Energy Consumption

Node type	Assoc time (ms)	Data msg time (ms)	CPU pow assoc (mWatt)	CPU pow data msg (mWatt)	NIC pow assoc (mWatt)	NIC pow data msg (mWatt)
	Av. SD	Av. SD	Av. SD	Av. SD	Av. SD	Av. SD
HP laptop	1.55 0.12	0.03 0.001	8.67 1.98	3.23 0.78	16.08 2.34	12.51 4.49
Samsung Laptop	2.35 0.044	0.80 0.023	12.16 4.06	4.31 1.01	17.14 2.43	16.22 6.11

1) *Consumption for Power*

Table IV depict the traditional and variance of the vitality utilization needed by the central processor thus on acknowledge (1) the affiliation solicitation and (2) to send a data message. Samsung expends 12.2 mW to grasp an affiliation demand whereas simply 8.7 mW is eaten up by the HP digital computer. For the message's causing, Samsung wants 4.3 mW whereas the HP computer wants 3.2 mW.

The 2nd section of Table IV explains about power required to network controller card for network association and for data transfer which depends upon type of network topology and complexity of operation.

Fig. 4 shows results of messages passing on the CPU and to DRAM. In Fig. 3 stages of the message passing process are explained: (1) associate inert stage; (2) Running of loop of 100 messages that sends a wherever hundred ms time difference between every message; and (3) A last the exit stage. These results are obtained by using a software called running average power limit (RAPL), Fig. 4(a) depicts the workstation's outcomes wherever the circle is dead at the twelfth second and Fig. 4(b) portrays the Samsung outcomes wherever the circle is dead at the fifteenth second. Within the 2 cases, one will observe that the result of the circle is very irrelevant. The opposite existing pinnacles square measure known with the operating framework action.

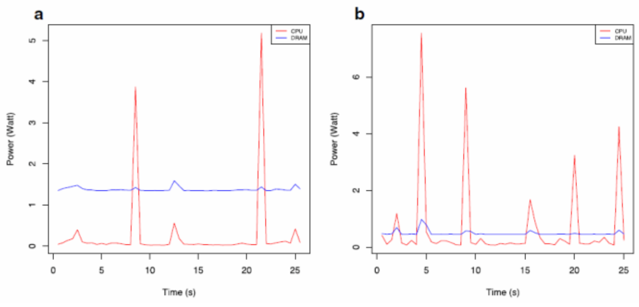
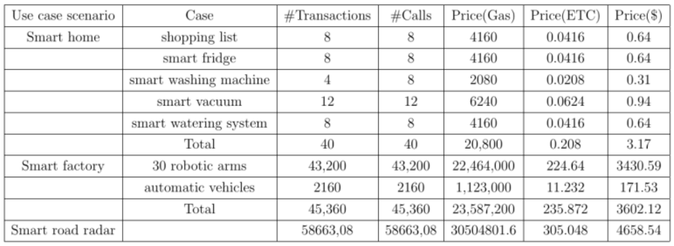


Fig 4: Impact of message process (a) HP (b) Samsung

Cost Estimation for Financial Purposes

In this phase, we have a tendency to depict the monetary fund expense of the use cases introduced during this. Sensible house: for the keen house state of affairs, we have a tendency to contemplate (1) the sensible garments washer sends one solicitation for each week for together with the built-soap powder the searching list that requires one exchange for every week. This exchange includes one decision activity therefore on recover the info. (2) The keen cooler arranges twofold in 7 days. (3) The searching list application makes 2 requests in 7 days. (4) The watering system is used twofold in 7 days. At long last (5) the vacuum is used three times in 7 days. Therefore, forty exchanges and forty calls are triggered each month shown in Table V with an algorithm a chart is also given.

Table V: Per month estimated cost for IoT use cases



Use case scenario	Case	#Transactions	#Calls	Price(Gas)	Price(ETC)	Price($)
Smart home	shopping list	8	8	4160	0.0416	0.64
	smart fridge	8	8	4160	0.0416	0.64
	smart washing machine	4	8	2080	0.0208	0.31
	smart vacuum	12	12	6240	0.0624	0.94
	smart watering system	8	8	4160	0.0416	0.64
	Total	40	40	20,800	0.208	3.17
Smart factory	30 robotic arms	43,200	43,200	22,464,000	224.64	3430.59
	automatic vehicles	2160	2160	1,123,000	11.232	171.53
	Total	45,360	45,360	23,587,200	235.872	3602.12
Smart road radar		58663,08	58663,08	30504801.6	305.048	4658.54

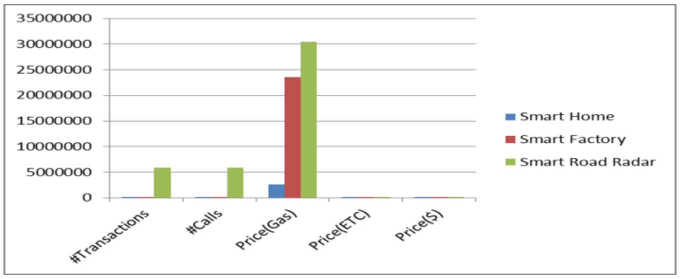


Fig. 5: Overview of Cost Estimation

VII. CONCLUSION AND FUTURE WORK

In this part, we will finalize our work and provide suggestions for future work. The Internet of Things and its applications are rapidly becoming part of our daily lives. We have proposed an approach in which secure zones are created in peer to peer network to achieve decentralization in which nodes can communicate in a secure fashion. This mechanism relies on public blockchain due that all security benchmarks regarding IOT security are achieved. Assessment of our methodology shows its capacity to meet the necessary security prerequisites just as its protection from assaults. Ethereum tool is used for development, validation and testing purposes that emulates interactions to the blockchain. For future work, we want following modifications into the system, 1) change the framework to permit controlled communication between set of trusted zones of choice, 2) Implement revocation mechanism for compromised nodes3) In future study and design a protocol to optimize number of miners and how selected miners can be placed.

REFERENCES

[1] A. Albarqi et al., “Public Key Infrastructure: A Survey,” *J. Inf. Secur.*, vol. 06, pp. 31–37, 2015.

[2] S. Huh, S. Cho, and S. Kim, “Managing IoT devices using blockchain platform,” in 19th *International Conference on Adv. Communication Technology (ICACT)*, pp. 464–467, 2017.

[3] D. Tapscott and A. Tapscott, “*Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio, ” 2016.

[4] R. C. Merkle, “A Digital Signature Based on a Conventional Encryption Function,” in *Advances in Cryptology*, pp. 369–378, 1988.

[5] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” in *Proceedings of 3rd Symposium on Operating Systems Design and Implementation*, pp. 173–186, 1999.

[6] J. R. Douceur, “The Sybil Attack,” in *Peer-to-Peer Systems*, pp. 251–260, 2002.

[7] D. Bong and A. Philipp, “Securing the Smart Grid with Hardware Security Modules,” in *ISSE 2012 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2012 Conference*, pp. 128–136, 2012.

[8] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[9] A. Tandon, “Challenges of Integrating Blockchain with Internet of Things,” 2019.

[10] P. Jahanbin, S. C. Wingreen, and R. Sharma, “A Blockchain Traceability Information System for Trust Improvement in Agricultural supply Chain,” in *ECIS*, 2019.

[11] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, and E. Di Sciascio, “Semantic Blockchain to Improve Scalability in the Internet of Things,” *OJIOT*, vol. 3, pp. 46–61, 2017.

[12] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. (PerCom Work.*, pp. 618–623, 2017.

[13] R. A. Memon, J. P. Li, M. I. Nazeer, A. N. Khan, and J. Ahmed, “DualFog-IoT: Additional Fog Layer for Solving Blockchain Integration Problem in Internet of Things,” *IEEE Access*, vol. 7, pp. 169073–169093, 2019.

[14] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, “NormaChain: A Blockchain-Based Normalized Autonomous Transaction Settlement System for IoT-Based E-Commerce,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4680–4693, Jun. 2019.

[15] Xin Zhou and Xiaofei Tang, “Research and implementation of RSA algorithm for encryption and decryption,” in *Proceedings of 2011 6th International Forum on Strategic Technology*, vol. 2, pp. 1118–1121, 2011.

[16] J. Lee, B. Bagheri, and H.-A. Kao, “A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems,” *Manuf. Lett.*, vol. 3, pp. 18–23, 2015.

[17] S. Wang, J. Wan, D. Zhang, D. Li, and C. Zhang, “Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination,” *Comput. Networks*, vol. 101, pp. 158–168, 2016.

[18] T. LLC, “{Fast Ethereum RPC client for testing and development.} Online Test RPC.” 2018.

[19] G. Gunduz and M. Yuksel, “Popularity-based Scalable Peer-to-peer Topology Growth,” *Comput. Netw.*, vol. 100, no. C, pp. 124–140, May 2016.

[20] N. Kshetri, “Blockchain’s roles in strengthening cybersecurity and protecting privacy,” *Telecomm. Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.