2020 International Conference on Information Science and Communication Technology

Security of IoT Using Block chain: A Review

Misbah Anwer
Dept. of Computer Science
Karachi Institute of Economics and Technology
Karachi, Pakistan
Misbahanwer129@gmail.com

Afshan saad
Dept. of Computer Science
Karachi Institute of Economics and Technology
Karachi, Pakistan
Afshanj2010@gmail.com

Ayesha Ashfaque
Dept. of Com Networks
National institute of computer emerging science -Fast
Karachi, Pakistan
K180791@nu.edu.pk

***Abstract*— IoT has a significant role in our every day schedule and it greatly affects us. Fundamental security goals like confidentiality, integrity, and availability are major challenges in IoT due to its distributive nature and massive scale. The decentralized approach used in BC would create a more reliable system for devices, to run on by eliminating single points of failure. Different cryptographic algorithms used in block-chains, would result in greater privacy of consumer data. Right now have talked about how to determine these issues utilizing block chain and will look at changed proposed arrangements and their issues and whether they are executed or not.**

Keywords—Internet of Things (IoT), Security, Block chain, DDoS, Ethereum, smart contracts.

I. BACKGROUND :

Security is one of the key difficulties in Internet of Things (IoT) because of non-homogeneity with asset imperatives of IoT devices. Gadget characterization strategies are utilizing to upgrade the security of IoT by distinguishing unregistered devices or traffic designs. In recent years, block chain has gotten huge consideration as a dispersed trustless stage to improve the security of IoT. We show that gadget recognizable proof in block chain presents protection chances as the pernicious hubs can distinguish clients' movement design by investigating the transient example of their exchanges in the block chain. We study the probability of ordering IoT devices by dissecting their data put away in the block chain, which as far as we could possibly know, is the principal work of its sort. We utilize a brilliant home as an agent IoT Situation. Initial, a block chain is populating by real-word home traffic dataset. We apply Machine Learning algorithms on the block chain dataset to determine true positive ratio of device classification for aware and unaware attacks. [11]

II. INTRODUCTION :

A. Internet of things (IOT)

Internet is a connection of physical things or objects. This connection is n't limited to computers abut it consist of devices of all type and size, All connection and information sharing based on designated protocols to get smart monitoring and communication. The advancement of innovation has put life in the period where a greater various devices are connected with the web. Around 60 billion associated devices will bring into administration by 2020. Naturally, inhabitants are mobilizing homes with IoT contraptions like net boxes, warming/cooling frameworks, brilliant TVs, House's gadgets, frameworks for lighting, etc. The pervasiveness of assortment of things is the thought behind IoT any place they are ready to move and team up with each other to create a decent assortment of administrations. Along these lines, huge assortment of gadgets will be encasing. Every device should be available and produce content, which will be bringing regardless of address. Devices produce, process, and trade-off a huge amount of important data & knowledge vulnerable to privacy therefore become an appealing target of various cyber-attacks [1]. It is imperative that exclusively real clients utilize the framework. Else, it will be obligated to different dangers like information change, data robbery, and character trespass [2, 3].traditional methods of security are expensive in terms of processing overhead and energy consumption. Moreover, many security frameworks and either not

978-1-7281-6899-9/20//$31.00 ©2020 IEEE

well suited for IoT devices or are highly centralized so there exists difficulty to scale its centralized and many-to-one nature activity [4]. Existing methods result either in incomplete data or in noisy data that may stop applications from providing personalized services [4]. IoT includes flexible, lightweight, and distributed protection & privacy.

Fig 1. IOT Scenarios

B. BLOCKCHAIN(BC)

Blockchains as its center is a shared engineering. BC is picking up prominence and is being utilized in different applications including shrewd agreements, conveyed distributed storage, and digital asset. They are basically blocks that are chained together called ledger which is more precisely an append only ledger.Each look contains set of transactions and every block points to the hash of last block. Hash of the block is hash of header of the previous block thus providing immutability. Any node in network can become a miner node, a node which mines a valid block in chain by solving some cryptographic hash puzzles called proof of work(POW)[5]. Miners need heavy resources in terms of computational power and energy to append a block. Mining difficulty is revised every two weeks thus miners that are competing need to upgrade their resources. Miners only append valid transactions, that have verified signature and there is no double spending. After mining a block it is broadcasted in the network if two miners mine the same block the one ending up in longest chain is considered. Following feature of BC make it attractive security problems in IoT: Decentralization, Transparency and Trust,Anonymity, Immutability, High Availability, Faster Dealing, Cost Saving .

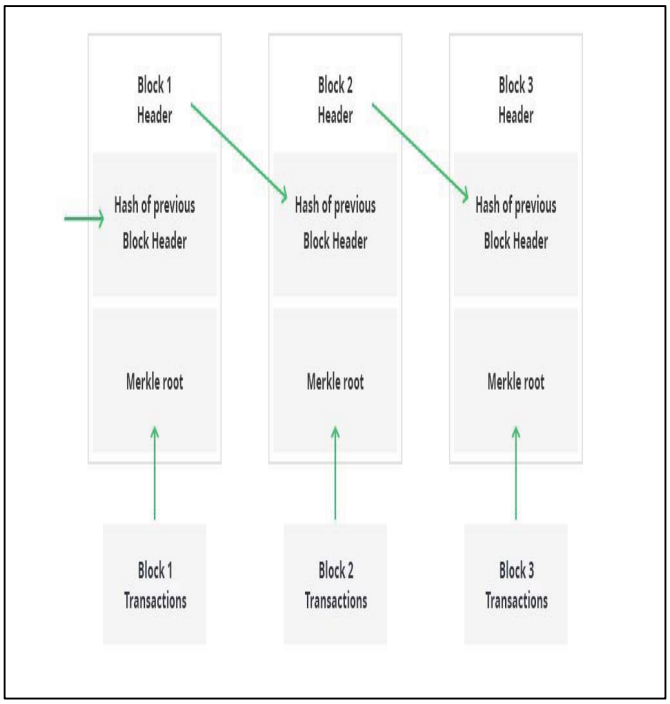

Fig 2 .Block Chain Architecture

III. SECURITY DEMANDS IN IOT

Various parameters and mechanism should be provided in order to achieve a secure environment involving IoT applications. Some of them are describing below.

A. Data privacy, confidentiality and integrity

To ensure the privacy of data a genuine encryption technique is required as data in IoT travels through multiple hops in the network. Due to various integration of devices, services, and network, there are chances of privacy hack if node in the network is compromised. The attacker can alter data stored in these for any malicious purpose, which results in data integrity [6].

978-1-7281-6899-9/20//$31.00 ©2020 IEEE

B. *Authorization, Authentication and Accounting.*

For secure communication, authentication is must between the two or more parties involved in communication. Devices must be authenticated for privileged access to take the services. As heterogeneous devices have different underlying architecture and environments differ in terms of support there is diversity in authentication mechanisms. Diversity of these environments creates challenges for defining any standard authentication and authorization is necessary to provide system access and information only to provide system access and information only to legitimate users, which will eventually result in trustworthiness in the system for secure communication. Resource Usage, Audit, and Reporting accounts provide a robust framework for secure network management [6].

C. *Accessibility of administrations*

An assault on gadget may stop the administrations. Methodologies like sticking enemies, sinkhole assaults, or replay assault may misuse IoT segments at unmistakable layers corrupting the quality of-services (QoS) that gave to clients [7].

D. Energy Efficiency

They are resource-constrained devices that are characterizing with less storage & low power. Any malicious attack on them Can result in higher energy consumption by flooding the network with exhaust resources forged or redundant service requests resulting in denial of services(DoS) to the legitimates user[6].

E. *Single point of failure*

Continuous growth in heterogeneous IoT networks may result in one-point failure, which may deteriorate the services in return that are envisioned. For secure environment in IoT application temper-proof development and fault tolerant network in necessary [7].

IV. PROPOSED BLOCKCHAIN SOLUTIONS

Of late, different works are curious about the mix of block chain into IoT biological networks. Nevertheless, just two or three works were curious about how block chain will encourage in meeting IoT security needs. In the midst of this territory, we keep an eye on outline most of the works that will see such partner degree organization and exhibit the phenomenon of undertakings that grasp the mix to fulfill wellbeing wants. IoT security look into is unpleasant, and the block chain is restricted since the greater part of the work centers on utilizing block chain developments to accomplish IoT benefits, when in doubt. Uzair et al. proposed a technique for mitigation of DDoS using smart contracts for communication between different IoT devices on goeterum. Two types of nodes server and IoT nodes. Server nodes can register and delete IoT needs. Every contract has fixed amount of decided Gas, transaction price, when a device tries to send its data to smart contract it verifies that cumulative gas of individual device do not exceed the gas of smart contract. Thus preventing DDoS. This technique works on assumption that server nodes are not malicious but IoT nodes can be, even if an IoT node become malicious and send large amount of data frequently even then it gas will be finished soon and so this malicious node can be deleted by server nodes.

Limitation: Scalability, Dynamic allocation of gas for each contract. [8]

Biplab et al. proposed a technique for integrity & data provenance for IoT environments. There are two types of nodes server and IoT nodes. Server nodes can register and delete IoT nodes. There are two types of contracts one will communicate with devices and make sure that they are trusted one. Other one will store and retrieve data from block chains. When a device send a data to an smart contract 1 it is verified if it is trusted or not if yes then smart contract will throw a challenge to its PUF if response is positive then only data is stored in block chain by smart contract 2 else process is terminated. Here data

978-1-7281-6899-9/20//$31.00 ©2020 IEEE

provenance is achieved by PUF associated with each IoT device and data integrity is achieved by immutable property of block chain. [9]

Ali Dorri et al. In [4] has described a scenario of smart home. Different techniques are used to handle confidentiality, integrity, user control, authorization and availability. It has also discussed how can DDoS be avoided by using hierarchical defense mechanism. According to author it is difficult to infect any IoT device as they are not directly accessible but even if any device becomes affected even then transaction will be blocked from this malicious device as on the second level of defense all outgoing traffic will be authorize by the minor through policy header. Table I Summarizes how the system mentioned addresses certain safety measures.

Requirement	Employed safeguard
Confidentiality	Achieve using symmetric encryption
Integrity	Hashing is employed to achieve integrity.
Availability	Achieve by limiting acceptable transactions by devices and the miner.
User control	Achieve by logging transactions in local BC.
Authorization	Achieve by using a policy header and shared keys.

Table 1: Security Requirement

Limitations: Greater packed overhead & energy consumption as compare to "base method". Base method is refer as method used to handle transactions without encryption, hashing, and BC.

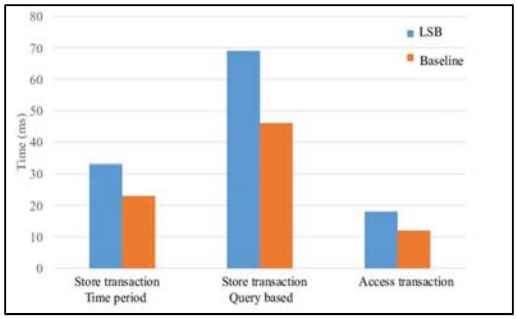

Fig 3 Evaluation of Time overhead

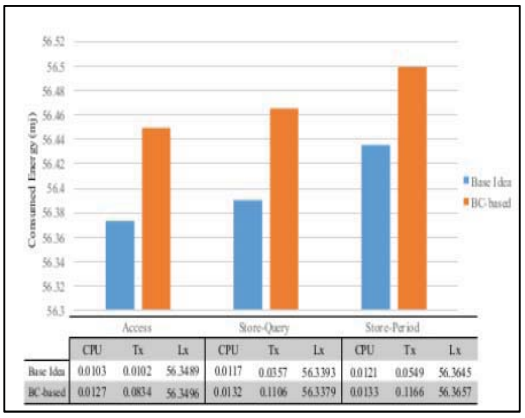

Fig 4 Assessment of energy consumption across different traffic flows.

In the mentioned paper [12] offer a survey of by what means can Block chain and crypto contracts are regularly incorporated in the chain of things.

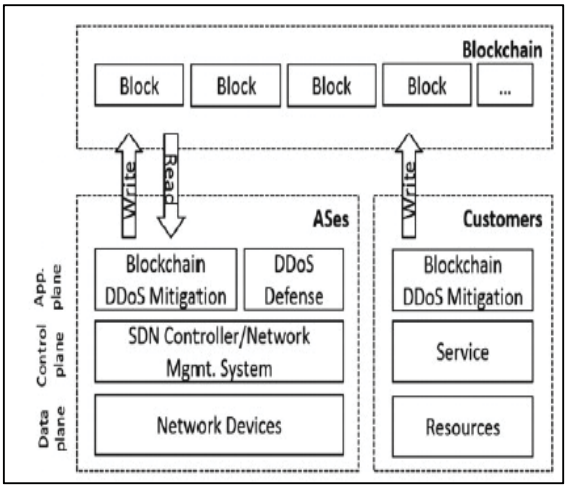

Fig 5 System Architecture

We first create a smart contract. This smart contract will have different subscribers. A smart contract needs to register in other smart contract thus all AS will listen these changes. When attack any web server, AS or customer can store, blacklisted IP addresses in block chain. Different As can have different mitigation techniques. AS or customers can now use these records to block traffic from theses IP addresses.

978-1-7281-6899-9/20//$31.00 ©2020 IEEE

V. CONCLUSION

The use of IoT and its application is expanding gradually, it is currently developed into an unavoidable piece of our standard everyday presence, and where its uses are developing other hand security issues are additionally expanding. The information ought to be safely traded between the gadgets to approved substances paying little heed to their area.

I have looked at the proposed arrangement of various specialists' strategies of Block chain to make IoT verify and talk about their restrictions. Various procedures of various specialists are contrasted with whether they execute the proposed arrangement. Comparison of papers can be seen in table 2.

Approach	Confidentiality	Integrity	Availability	Authenticity	Authorization	Immutability	Single Point Of Failure
Uzair et al.	Y	Y	Y	Y	N	Y	Y
Biplab et al.	Y	Y	N	Y	N	Y	Y
Ali Dorri et al.	Y	Y	Y	Y	Y	Y	Y
B. Rodrigues et al.	Y	Y	Y	N	N	Y	Y

Table 2 : Summary of comparison

REFERENCES

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini,"Security, privacy and trust in internet of things: The roadahead," Computer Networks, vol. 76, pp. 146–164, 2015.

[2] Hammi, Mohamed Tahar, et al. "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT." Computers & Security 78 (2018): 126-142.

[3] Banerjee, Mandrita, Junghee Lee, and Kim-Kwang Raymond Choo. "A blockchain future for internet of things security: A position paper." Digital Communications and Networks 4.3 (2018): 149-160.

[4] Dorri, Ali, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. "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, 2017.

[5] Decker, Christian, Jochen Seidel, and Roger Wattenhofer. "Bitcoin meets strong consistency." In Proceedings of the 17th International Conference on Distributed Computing and Networking, p. 13. ACM, 2016.

[6] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future Generation Computer Systems 82 (2018): 395-411.

[7] Agrawal, Rahul, Pratik Verma, Rahul Sonanis, Umang Goel, Aloknath De, Sai Anirudh Kondaveeti, and Suman Shekhar. "Continuous security in IoT using Blockchain." In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 6423-6427. IEEE, 2018.

[8] Javaid, Uzair, Ang Kiang Siang, Muhammad Naveed Aman, and Biplab Sikdar. "Mitigating IoT Device based DDoS Attacks using Blockchain." In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pp. 71-76. ACM, 2018.

[9] Javaid, Uzair, Muhammad Naveed Aman, and Biplab Sikdar. "BlockPro: Blockchain based Data Provenance and Integrity for Secure IoT Environments." In Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, pp. 13-18. ACM, 2018.

[10] Ouaddah, Aafaf, Anas Abou Elkalam, and Abdellah Ait Ouahman. "FairAccess: a new Blockchain-based access control framework for the Internet of Things." Security and Communication Networks 9, no. 18 (2016): 5943-5964.

[11] Rodrigues, Bruno, Thomas Bocek, Andri Lareida, David Hausheer, Sina Rafati, and Burkhard Stiller. "A blockchain-based architecture for collaborative DDoS mitigation with smart contracts." In IFIP International Conference on Autonomous Infrastructure, Management and Security, pp. 16-29. Springer, Cham, 2017

978-1-7281-6899-9/20//$31.00 ©2020 IEEE