IoT Based E-commerce getting a Secure Connection using Block Chain Methodology

K.S. Anand kumar[1], Prasad A.Y.[2] and R. Balakrishna[3]

[1]Associate Professor, School of Computing & Informatics
College of Engineering and Technology, Dilla University
[2]Research Scholar, RRCE, Bangalore
[3]Professor, Department of CSE, RRCE, Bangalore
***DOI**: https://doi.org/10.34293/acsjse.v1i1.4*

Abstract - *It is one of the growing technology which is very useful in the the particular systems of privacy and the IoT related security which is still one of the unexplored. The flowcharts and all the algorithms are all one of the core part of the IoT technology for the Block chain system, where we have shown the importance of the Block chain system for the IoT system. It is already recorded that more than people there will be things in the future that are why having a particular security for the things which will be all over controlled by the internet calling as the Security for the IoT networks. The block chain system is already useful in many of the other networking system for the security purpose and the security purpose for all the end to end networks. There are many challenging attacks than the other common attacks that are detected for now and here we will discuss about the attacks we are going to prevent.*
Keywords: *E-Commerce using IoT, Security for the IoT system using block chain, Encryption, Performance and Attacks.*

I. INTRODUCTION

IoT (internet over things) is one of the developing technology for any computer related data exchange or communication as we can imagine that in the future or further computers having a computer within themselves as IoT will be used to communicate between this two computers that is internal computer and the external computer.

The IoT is the future of technologies where further it will be used in many domains and purposes where we can't ignore the security for these devices as we don't want anyone one to have a peek inside our data or even steal the data from our own sites. So , for this security of these devices we can use the block chain methodology.

As the IoT is based E-commerce is one of the known new trading model of the era, these realizes the two transactions these are person to person and machine to machine transactions other than directly applying person to person transactions creating high risk.

IoT based E-commerce has a huge amount of layers with the fragmented and the light weight devices to accomplish performance to the device. The scattered structure of all the machine to machine frame work having the block chain methodology with the decentralized networks and block chain is suitable for managing the IoT devices.

As the IoT based devices have the low band width which are also limited and these devices or the device technique has lot of traffic to accomplish the security and privacy

needed for the device, this is where the block chain comes with the block chain based architecture providing the security and privacy with the virtue of the block chain addressing.

No other superior can attack the device as the block chain methodology doesn't leave any other person to attack the further called system and taking the encryption key and decrypt the device user's information which is as encrypted where the block chain gives the security and privacy to the user so they can't crypt analyze the device information or the user's information.

To perform the ethical hacking of the E-Commerce system we need transaction system (a legal supervision system for transactions). They must obtain user's dealings information to a indisputable degree.

An self-governing and a lightweight dealings platform is been planned for IoT and E-Commerce as to which will speech the ratio challenge as this will be the goal for the scalability and a high speed transaction in E-commerce system. As we replace to the three layer sharding block chain from a single layer block chain I.e, conventional single layered block chain.

II. LITERATURE SURVEY

In the Ali Dorri's paper they have proposed in the field of block chain and IoT architecture as they handle all of the securing and all the privacy threats considering all of the constraints and resource of plenty IoT devices. But as architecture if the qualitative over head shows that it has a stable performative access throughout the system architecture atbest, and at worst most of its transaction is all about the clusters number is more than concentrating on network having the same figure of nodes. [1]

Steve Huckle has explored in, as hoe the IoT and Block chain system will help the E-Commerce transaction system.. But they doesn't have any implementations thus holding that its all about the theory and also considered as the theory in the system. As they also don't apply for any IoT applications. [2]

In the Roman Beck's paper has a concept and a proof of prototype that it can replace a simple online transaction system for example a coffee shop transaction system. But the scalability cost and maintenance cost will be high even for a simple transaction system. [3]

Jose L. Hernandez-Ramos, incoming his paper he has given accession control method as support for the certification, acknowledgement and access control systems. But optimization of the signature validation step is really expensive for the block chain system. Delegation in these steps of object has also not been done. [4]

Blockchain Platform	Consensus Model	Transaction speed/sec
Ethereum	Proof of work (Proof of Stake 2018)	15 (1 million)
Hyperledger	Proof of Elapsed time	3500
Ripple	Byzantine Fault Tolerance	1500
IOTA	Directed Acyclic Graph	1000-2000
Neo	Delegated Byzantine Fault Tolerance	1000

While, Ali Dorri, have got developed deeper and distinct the different core constituent and all the functions which contains all the home tier system.Each of the smart house system will have a design to overcome the problems of a system lag best-known as 'miner' which will be accountable for management of all the communications between other systems or the outside system control alignment. But the overheads receive as the proposed methodology are very high and this method is only for the house system and not other than the house scheme (smart house scheme) [5]. Jesse Yli-Huumo, in had the technical perspective on the block chain system with regarding the control over the system. But the paper has excluded the economical, legal document, enterprise, and rule perspectives, and included only the skillfulness perspective. [6]

Jing Liu, mainly analyzed existent certification and access activity methods, and then, a feasible and a easy method to the IoT technology and a DOS attacks aren't flock [7].

Aafaf Ouaddah, have planned Fair Access as a new localized onymous and privatizes protective authorization management framework that leverages the coherence of on behalf of the affected devices the block technology is useful . There is no effort of FairAccess and interfacing of IoT devices with Blockchain. [8]

III. PROPOSED MODEL

Proposed Blockchain based on the IoT Architecture

Any IoT set up includes cloud storage. These devices could be a temperature regulator or a security system, whose data is stored in cloud. The architecture consists of 4 divisions – the end devices, a gateway, a block chain which could be private or public and lastly the cloud storage. The data should be available for access, also there should be interaction of devices depending on the access policies.

End Devices

The smart devices should most importantly be capable to store data on cloud keeping based on the access argumentation. All the peripheral devices capable of interacting with each other in a smart home are the end devices. The smart devices are provided with unique identifiers that are addresses to the block chain, as introduced by the proposed model. This was done as the smart devices don't have an unequalled identifier and it is challenging to use access control. Communication between devices is done with the help of private keys which can be termed as transaction. In order to communicate with the cloud or another device, these

unique IDs acts as a pass. This transaction is very crucial and hence the private key should be stored safely and not to be disclosed anywhere.

Gateway

The connection between the peripheral devices or the end devices is done through a gateway. It is also the connection between devices and the cloud. The validity of any device is verified through this medium. Communication between end devices and the server is done via the communication protocol, MQTT (Message Queuing Telepathy Transfer). It's a prescript that uses publish/support dealing to exchange data between clients and the server. Its little size, low quality usage, decreased data packets and ease of execution make the protocol ideal for "machine-to-machine".

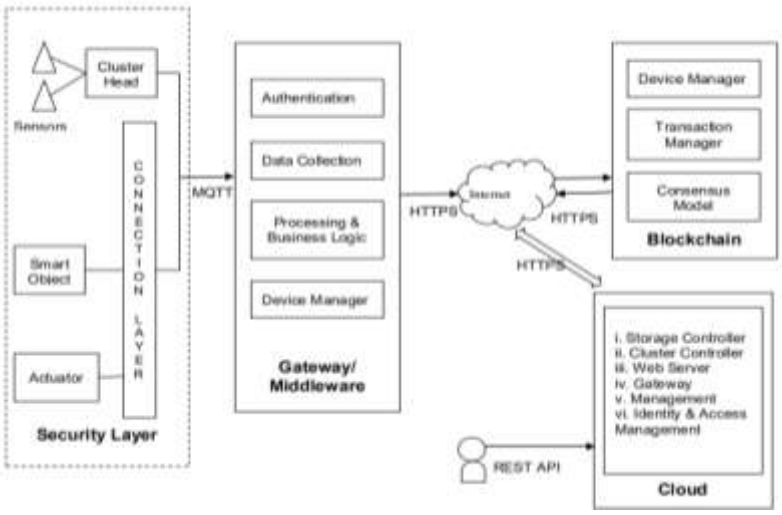
The localized host also talks to Blockchain by calling a smart contract. A smart contract is a self-enforcing agreement embedded in computer code managed by a blockchain. They supply a public and objective way to embed governance concept and business logic in a few lines of code, which can be audited and implemented by the majority agreement of a P2P meshwork.

Blockchain

Blockchain technology is a fast growing area. All the data movement is recorded in the blockchain and is safe. The HTTP protocol is used. Ethereum Blockchain and solidity language is used. Dependability is known as a contract-based, high-level programming language which is influenced by C++, Python and JavaScript. Ethereum is the ultimate smart contract and decentralized application platform. Remix is used to position contract on ganache which is Block chain imitator on local host.

Cloud Storage

All data acquired from the devices are stored in the highly virtualized cloud. This can be retrieved by multiple servers via internet. Think speak is used for storing temperature data on the cloud.



Architecture of IoT with the Block Chain

Storing

As this the most of the storage is done with the help of the cloud storage system. As to access all the data the security will be taken as per the system admin id and other hash function system.

Accessing

As the communication between the control systems are important and thus the communication is made only with the hash code function as this the hash code functions are combined and then the communication between the systems are done as the hash code of both the functions are matching.

Algorithm 1: Authentication and Access Control

```
hashtoken ← timestamp + deviceId
Append hashtoken to encrypted data
Send this hashtoken + data to the
middleware gateway
whitelist ← Array of whitelisted
deviceId from blockchain
i ← 0
flag ← False
while i<len(whitelist) do
if SHA
(decrypt(whitelist[i]+timestamp) ==
hashtoken then
flag ← True
break
end if
i ← i+1
end while
if flag == True then
Check access policies and send data
to cloud
else
reject the request and block the
device if rejected thrice
end if
```

DKS (Distributed key generation) equation

Distributed key generation (DKG) was enclosed by the famous technician Pedersen in the year 1991. As his goal was to secure the internet or the other technical related systems from the threat as we know that the block chain system is meant for avoiding threats away from the personal systems and data kept in the systems.

In this method we are assigning the n secret key sharing with the α(i) to n as represented as the n different people. Overall the α is almost shared to one of all the parties

which knows the α(i). So that one single party can stock the secret key for their personal use they will need the secret key for their use.

$$DKG(n)=\{\alpha(l)\},\ \alpha(i) \in z(q), i \in \{1,\ldots,n\}$$

As the n is sent to the verifiable secret sharing protocol as these are assigned to n as where assigned to share the n secret key to all the α(i) to n diametric people.

Z(q) is called the finite circle group of the q large foundation. P is known as the prime numbers where the q is called as the subtraction minus to the 1 that is called as the P-1.

The produced secret key ɑ (i) should fulfill the mathematical statement as,

$$\alpha = \sum_{i=1}^{n} \alpha(i)$$

As the each secret key contains of the α(i) system.

IV. CONCLUSION

The security for the blockchain is the pending system as the system needs a security access for the whole system which can control the hackers as they can change the data . So to control the hackers we will be creating a blocker where the system is going to put the hackers in a black list as the other system are going to the white list format.

V. REFERENCES

[1] Dorri, Ali, et al. “Blockchain in internet of things: Challenges and Solutions,” CoRR, 2016.

[2] R. Bhattacharya, M. White, and N. Beloff. “A Blockchain based peer-to-peer framework for exchanging leftover foreign currency,” Proc. Comput. Conf., 2017, pp. 1431-1435.

[3] Beck, Roman, StenumCzepluch, Jacob, Lollike, Nikolaj, and Malone, Simon. “Blockchain - The Gateway to Trust-Free Cryptographic Transactions,” *Research Papers*, 2016.

[4] Hernández-Ramos, José L., et al. “Distributed capability-based access control for the internet of things,” Journal of Internet Services and Information Security (JISIS), 2013.

[5] Dorri, Ali, et al. “Blockchain for IoT security and privacy: The case study of a smart home,” Pervasive Computing and Communications Workshops, 2017.

[5] Yli-Huumo, Jesse, et al. “Where is current research on Blockchain technology? – A systematic review,” PloS One, 2016.

[5] Liu, Jing, Yang Xiao, and CL Philip Chen. “Authentication and access control in the internet of things,” Distributed Computing Systems Workshops (ICDCSW), 2012.

[6] Ouaddah, Aafaf, Anas Abou Elkalam, and Abdellah Ait Ouahman. “Towards a novel privacy-preserving access control model based on Blockchain technology in IoT,” Europe and MENA Cooperation Advances in Information and Communication Technologies, Springer, 2017, pp. 523-533.

[7] Mahalle, Parikshit N., et al. "Identity authentication and capability based access control (IACAC) for the internet of things," Journal of Cyber Security and Mobility, 2013, pp. 309-348.

[8] Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, 2013.

[9] Sun, Jianjun, Jiaqi Yan, and Kem ZK Zhang. "Blockchain-based sharing services: What Blockchain technology can contribute to smart cities," Financial Innovation, 2016.

[10] H. Gross, M. Holbl, D. Slamanig, and R. Spreitzer. "Privacy-Aware Authentication in the Internet of Things," Cryptology and Network Security, Springer International Publishing, 2015, pp. 32-39.

[11] Huckle, Steve, et al. "Internet of things, Blockchain and shared economy applications," Procedia Computer Science, 2016, pp. 461-466.

[12] Beck, Roman, et al. "Blockchain - the Gateway to Trust-Free Cryptographic Transactions," ECIS, 2016.

[13] Ukil, Arijit, Soma Bandyopadhyay, and Arpan Pal. "Iot-privacy: To be private or not to be private," Computer Communications Workshops (INFOCOM WKSHPS), 2014.