International Journal of Modern Agriculture, Volume 10, No.01, 2021
ISSN: 2305-7246

BLOCKCHAIN INTEGRATION WITH IoT FOR SECURITY AND PRIVACY ISSUES

[1]saranya.R, [2] Harithaamagesh,[3] Lakshya.P ,[4]desiyaveni.M

[1]Assistant Professor
Department of Computer Science Engineering
Manakula Vinayagar Institute of Technology
Puducherry, India

[2] UG Scholar
Department of Computer Science Engineering
ManakulaVinayagar Institute of Technology
Puducherry, India

[3]**UG Scholar**
Department of Computer Science Engineering
ManakulaVinayagar Institute of Technology
Puducherry, India

[4]**UG Scholar**
Department of Computer Science Engineering
ManakulaVinayagar Institute of Technology
Puducherry, India

I.ABSTRACT:

Internet of Things and BlockChain are one of the most influencing domains in research perspectives. Security and Privacy are the most important challenges in IoT. The Internet of Things (IoT) is a modern technology where various physical and virtual devices can be connected and communicate with each other over the Internet often without human intervention[5].In this work we've performed a study of Security issues on Internet of Things and various security challenges.To encourage this arising domain, we have performed a survey on the examination progress of IoT and focus on the security.We discuss and examine the status of key innovations including encryption system, ensuring sensor information, cryptographic calculations and quickly find the difficulties.
Key terms – Internet of things, Security , Privacy , Challenges.

II.INTRODUCTION

Internet and Technology has changed the way of communication over years. This would have not been possible without the advancement of studies in technologies. Internet of Things can be defined as a network in which several devices are connection in order to transfer and retrieve information. All the transactions between the different parts of our scenario are made on very sensitive personal data. It is obvious that the medical reports should be confidential and have limited access in a global system that insures the non repudiation[3]. The IoT is completely different from M2M (Machine to Machine) transfer as IoT is more flexible in terms of data transfer.The number of networked devices is increasing explosively.However, security issues of IoT can cause disastrous consequences to our human life[10].The growth of IoT devices is rapidly changing as it crosses the total world population. In IoT , the architecture consists of three layers namely physical , network , data processing and application layer.

International Journal of Modern Agriculture, Volume 10, No.01, 2021
ISSN: 2305-7246

III.INTERNET OF THINGS

Characteristics of IOT:

1. **Intelligence:**
   IoT comes with various combination of algorithm and computation, software & hardware which makes it smarter. Ambient intelligence in IoT enhances its capabilities by facilitating the items responding in an intelligent manner to a specific situation and supports them in completing specific tasks.

2. **Connectivity:**
   Connectivity enhances Internet of Things by bringing together everyday objects in our day to day life.It ensures amdenables network accessibility and compatibility in variousthings. With the connectivity, new market opportunities for Internet of things can be created by the smart things networking and applications.

3.Dynamic Nature:

The primary activity of Internet of Things is to collect data from its environment, this is often often achieved with the dynamic changes that happen around the devices. The states of all these devices can change dynamically, example sleeping and waking up ,whether connected or disconnected and also the context of devices including temperature, location and speed.

4. Enormous scale:

The devices that needs to be managed andthe ones that communicate with each other will be much larger in number when compared to the devices that are connected to the Internet. The data generated from these devices are managed and its interpretation for application purposes arevery much critical.

5. **Sensing:**
   IoTisimpossible without sensors. Any changes in the environment can be detected by the sensors.They can report the status or even interact with the environment.The Sensors provide the way to create capabilities and to reflect the true motive of physical world and the people.

6. **Heterogeneity:**
   Heterogeneity is one of the key characteristics in IoT. IoTdevices are based on various hardware platforms and networks. They can interact with other gadgets or service platforms with different networks. The key design requirements for heterogeneityand its environment in IoT are extensibility, scalability, modularity and interoperability.

7. **Security:**

All IoT devices are generally vulnerable to security threats. As we gain many other experience other than advantages fromIoT, it would be a huge mistake to forget about the security issues associated with it. There is a high level of privacy concernand transparency with IoT.One way to provide trustworthiness in IoT data is through a dis-tributed service trusted by all its participants that guarantees thatthe data remains immutable[7].It is necessary

International Journal of Modern Agriculture, Volume 10, No.01, 2021
ISSN: 2305-7246

to secure the endpoints, network, and the data transmitted across all of it which means,creating a security paradigm.

IV. BLOCKCHAIN IN IoT

Blockchain, which is most familiar for bitcoin and Ethereum, offers an intriguing solution for IoT security problems. Bitcoin users which are known by a changeable Public Key(PK), generate and broadcasttransactions to the network to transfer money [12].Blockchain contains strong protections against data tampering, locking access to IoT devices, and allows compromised devices in an IoT network to be shut down.

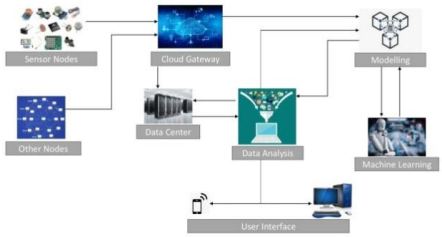

Fig1. Integrating Blockchain with IoT

Cloud Computing provides more storage and assures security to the data.Howeverlately ,maximum of the actual – time tracking IoT software call for processing and computing in the edge of the community.

V. ATTACKS IN IOT LAYERS

Protocols & Possible Attacks in IOT Layers		
Layer	**Protocol Name**	**Possible Security Attacks**
Application	MQTT, CoAP, REST, AMQP	Repudiation Attack, DDos Attack, HTTP Flood Attack, SQL Injection Attack, Cross-Site Scripting, Parameter Tampering, Slowloris Attack
Transport	TCP, UDP, DCCP, SCTP, RSVP, QUIC	SYN Flood, Smruf Attack, Injection Attack, Mitnick Attack, Opt-act Attack

International Journal of Modern Agriculture, Volume 10, No.01, 2021
ISSN: 2305-7246

Network	CLNS, DDP, EIGRP, ICMP, IGMP, IPsec, IPv4, IPv6, OSPF, RIM	IP Address Spoofing, DoS Attack, Black Hole Attack, Worm Hole Attack, Byzantine Attack, Resource Consumption Attack.
Physical	DSL, ISDN, IDA, USB, Bluetooth, CAN, Ethernet	Access control Attack, Physical damage or Destruction, Disconnection of Physical Links

Table.1 Different attacks in IoT layers

VI. TOOLS TO IMPLEMENT BLOCKCHAIN

Hyperledger Fabric and ABAC:

By using distributed architecture, fabric-iot cantrace records, provide dynamic access control management andsolve the access control problem in IoT[9].

1.HYPERLEDGER SAWTOOTH:

It is a platform developed by Intel to build, run, and deploy distributed ledger. It implements transaction-based updates to shared state among partieswhich are untrusted and it is synchronized by a consensus algorithm.

2.HYPERLEDGER IROHA:

It is led by Soramitsu. It provides a developing environment where in the C++ developers and mobile applications can contribute for the Hyperledger. It consists of pre-defined commands, queries, and permissions in order to develop applications for mobile and desktop platform conveniently.

3.HYPERLEDGER FABRIC:

HyperledgerFabric is the most popular Hyperledger project. IBM initiated the hyperledger fabric for Digital Assets. It uses the container technology to host the "chain code" .The blockchain framework allows different components like membership services and consensus.

4.HYPERLEDGER BURROW:

It is from Monax and was co-sponsored by Intel. The burrow gives blockchain client a permissioned smart contract which is developed to specification of the Ethereum Virtual Machine.

Hyperledger, is an open source software. Hence it is adopted and further developed by different companies. It acts as a strong core foundation to develop other functionalities above it. The projects that offerBlockchain-as-a-Service or BMS (Blockchain Management System) majorly includesHyperledger Fabric protocol.

VII. FUTURE OF IoT

In an IoT-enabled world, people will receive uniquely personalised services on demand, while societies will benefit from optimised resource use with minimal impact on the environment. In each

International Journal of Modern Agriculture, Volume 10, No.01, 2021
ISSN: 2305-7246

smart home, there is a local private BC that keeps track of transactions and has policy header to enforce users 'policy for incoming and outgoing transactions. With the fast rise of brilliant devices and high-speed networks,theIoT has gained wide acceptance and fame because it uses the standard called low-power lossy networks (LLNs)[13]. Starting from the genesis transaction, each device's transactions are chained together as an immutable ledger in the BC[4].

Interactions between human beings and machines are at the verge of a radical shift with the potential to free up large opportunities facilitated through the concept referred to as IoT.International data corporation (IDC) in its 2019 forecast predicts over 40 billion IoTdeviceswill be generating over 75 billion zettabytes (ZB) of data in 2025 (Framingham, 2019)[8].With simultaneous advances in technology inclusive of artificial intelligence and device studying, those conversations can permit devices to assume, react, respond and enhance the physical interactions.

VIII.CONCLUSION

Blockchain technologies can coordinate , track , carry out transactions and storing data from a large amount of devices, enabling the creation of applications that require no centralized cloud [2].Hence Block chain can be implemented to improvise the security in IoT. The Hyperledger Fabric version-2.2 can be used to create the channels and chaincode.In many distributed applications where trust and trans-parency are critical factors, the blockchain technology has shown to be a promising solution[14]. In this paper, we have addressed the issues and vulnerabilities that occur in the IoT technology.

As explained before , integrating Blockchain with IoT makes the communication secure. In future, Blockchain can be implemented in smart based IoT system by using the Hyper ledger platform.However further research must be done to get secured IoT systems.

IX. REFERENCES:

[1] UtkalikaSatapathy ,Bhabendu Ku. Mohanta ,Soumyashree S Panda , SrichandanSobhanayak , Debashis Jena ," A Secure Framework fro Communication in Internet of Things Application using Hyperledger based Blockchain" ,IEEE 10th ICCNT , 2019.

[2] Tiago M. Fernandez-Carames , Paula Fraga-Lamas , " A Review on the use of Blockchain for the Internet of Things" , vol 6 , pp. 32979-33001, IEEE Access , 2018.

[3] OumaimaAttia , Ines Khoufi , AnisLaouiti , Cedric Adjih , " An IoT-Blockchain Architecture based on Hyperledger framework fro healthcare Monitoring Application" , IEEE 2019.

[4] Ali Dorri ,Salil S. Kanhare , Raja Jurdak , Praveen Gauravaram , " Blockchain for IoT Security and Privacy: The Case Study of a Smart Home" , 2nd IEEE PERCOM Workshop on Security Privacy and Trust in the Internet of Things , 2017.

[5] Hany F. Altan , Muhammad Ajmal Azad , Ahmed G. Alzahran , Gary Wills , " A review of Blockchain in Internet of Things and AI" , Big Data and Cognitive Computing , vol 4, MDPI , 2020.

[6] MandritaBanerjee ,Junghee Lee , Kim-Kwang Raymond Choo , " A Blockchain future for Internet of Things security:a position paper" , Digital Communication and Networks , vol 4 , pp. 149-160 , 2018.

International Journal of Modern Agriculture, Volume 10, No.01, 2021
ISSN: 2305-7246

[7] Ana Reyna, Cristian Martin , Jaime Chen , Enrique Soler , Mauel Diaz , " On Blockchain and its integration with IoT Challenges and opportunities" , Future Generation Computer Systems , pp. 173-190 , Elsevier , 2018.

[8] Eben-EzerCHINYATI , " Securing IoT devices using Hyperledger Fabric (Blockchain technology)" ,Research Gate , 2020.

[9] Han Liu ,Dezhi Han , Dun Li , " Fabric-iot: A Blockchain-based access control system in IoT" , vol 8 , pp. 18207-18218 , IEEE Access , 2020.

[10] DonggxingLiu , Wei Pang , Wenping Den , FangyuGai , " A Blockchain-based Authentication and Security Mechanism for IoT" , IEEE , 2018.

[11] NithinM , S Shraddha , NishitaVaddem , Sarasvathi V , " HyperIoT: Securing Transactions in IoT through Private Permissioned Blockchain" , IEEE , 2020.

[12] Ali Dorri ,Salil S. Kanhere , Raja Jurdak , Praveen Gauravaram , " Blockchain for IoT Security and Privacy : The Case Study of a Smart Home " , IEEE , 2017.

[13] AbidSultan , Muhammad AzharMushtaq , "IOT Security issues via blockchain: A review paper" , pp. 60-65, ICBCT , 2019.

[14] Hien Thi Thu Truong , Miguel Almeida , GhassanKarame , Claudio Soriente , " Towards Secure and Decenteralized Sharing of IoT Data", pp. 176-183 , IEEE Conference on Blockchain , 2019.