A BLOCKCHAIN FUTURE FOR INTERNET OF THINGS SECURITY

S. Swapna and K. Himabindu, Asst Professor in Computer Science and EngineeringLoyola Academy, Alwal, Telangana,500015 : seguri.swapna@gmail.com ,himabindu.kp@gmail.com

Abstract: Internet of Things(IoT) are being increasingly set up in mercenary and military surrounding, starting from smart areas and smart grids to Internet- of- Medical- effects, Internet- of- Vehicles, Internet- of- service- effects, Internet- of- Battleground- effects, and may be a wide network conforming of Internet- connected objects using installed software, like home appliances, vehicles, and other related devices with detectors, selectors, radio- frequency identification(RFID), and electronics to change data. Within the last two decades, We make variety of compliances, including the deficit of intimately available IoT datasets that can be used by the exploration of communities and multitudinous. IoT results have been developed by small, medium- sized, and enormous enterprises to make our lives easier. The rapid-fire expansion of IoT results multitudinous security enterprises because the underpinning IoT protocols and communication technologies have not considered security. Blockchain has surfaced to come one among the promising technologies that might overcome some of the IoT limitations(security limitations, in particular). Blockchain technology may be a database tally that uses a peer- to- peer(P2P) network and stores deals and asset registries. Blockchain are frequently described as a underpinning list of records (i.e., blocks) with the posterior parcels distributed, decentralized, inflexible, and participated. This paper surveyed recent security advances and attempts to beat IoT limitations using blockchain related to cyber security have been classified into four orders end- to- end traceability; data sequestration and obscurity; identity verification and authentication; and confidentiality, data integrity, and vacuity. Blockchain technology began to be known with the arrival of crypto coins mining as it is a main technology which has been important to do with the IoT. In this environment where the possibility arises to take advantage of the Blockchain armature to authenticate, regularize and cover the relinquishment of data handled by the bias. For IoT safety, the blockchain is suitable to cover the information collected by the detectors, without allowing them to be duplicated by any wrong data by using some the algorithms to encrypt the data for security issues. Detectors can also transfer data using Blockchain technology, without the need for a trusted third party.

Keywords: Internet of Things, Blockchain, Security

INTRODUCTION:

Iotex is a Silicon Valley start-up focused on building the Internet of Trusted Things Using blockchain technology. As the size of the IoTmarket.Worldwide has been increased significantly over the past years. According to the projections file Statistica.The number of connected devices will reach to some more billion by 2025. Which means We will have a huge number of IoT devices connected to the Internet Which are affecting our life. As a data-driven system IoT would is all about making business decisions based on the data Collected by smart devices. We will have a bunch of smart devices that will be responsible for collecting data. They will be attached to physical assets and collect data those data will be transferred to back- end system for further storage and processing. And later on those data, after being further processed will be visualized and shown to Business owners or customers. Based on those data, customers can make decisions for whatever things they want to do.

In practice IoT systems are being realized using a cloud centric approach, which means we have a different type of IoT devices. Some of them are very smaller, like sensors actuators Etc which we will take to the IoT Gateway first. The IoT gateway will now receive the data to the cloud.

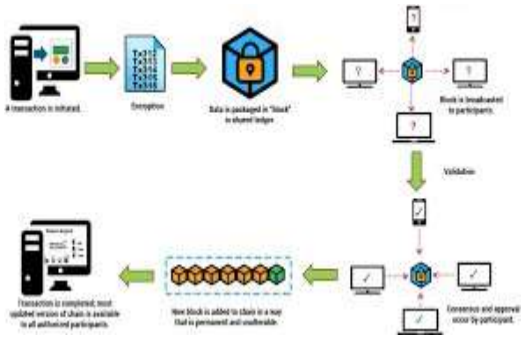
Cloud centric IoT system architecture:

For the IP capable IoT devices they can directly take to the cloud backend so all those data will first go to a connectivity gateway on the IOT cloud and the cloud service will host a bunch of different

types of services to support IoT applications, such as user management, Device management, storage management, digital twins, etc.
Based on those services we can build to different IoT applications and provide insights for our users. So users can access and virtualize those data using different types of devices like laptops, Phones and tablets. There are many popular IoT cloud platforms on the market-Google, Amazon, Microsoft, Azure etc. Those cloud services provide the cloud management, IoT components that will Facilitate the development of IoT solutions. As we can see IOT systems are quite complex so the data will go through different types of entities along the way, which makes securing IoT applications particularly challenging.
Basically, we need to consider the security across different stages, for example, we need to consider secure hardware which will run a secure OS by loading a trusted framework into your smart devices which will be able to establish a secure communication channel With the cloud back end.

IoT Security Challenges:
On the cloud side If you need to host a number of security related services to ensure the confidentiality, data integrity, and availability based on those security services. Data is super important in IoT systems to ensure data's trustworthiness; we need to realize our vision for the IoTex of Trusted things. Basically, we need to consider security throughout the data lifecycle of the Internet of Trusted. Things which include data collection, data in-Transits, data at-rest, data processing, as well as data retention.

Blockchain In A Nutshell:
How can we use blockchain to realize this end-to-end security for the Internet of Trusted things. blockchain is a chain of blocks and each block contains A number of transactions, which record status of certain events.



Blockchain is classified into two types permissioned and permissionless blockchains. Permissionless blockchains which means everyone can join the network and can read the ledger data and validate transactions. Permissionless nature of block chain is very open and the ledger replicates a high level of trust for a permissionless settings. Permissioned blockchains, on the other side, are formed by a set of known transaction parties. All transactions will be validated and controlled by a selected set of nodes.so this type of blockchain is mainly for enterprise use cases and permissioned ledgers will replicate a high degree of transparency and accountability.

Salient Properties of Blockchains:
Blockchain Technology provides a number of salient properties
Decentralization: Blockchain is run by a committee of nodes in a peer-to-peer manner.
Immutability: Blockchain uses cryptographic hash functions to link all of the block together to ensure data is immutable
Transparency: Blockchain provides a fully auditable and valid ledger of transactions which can be shared in the entire network in a permissionless blockchain setting or shared by a set of nodes in a permissioned setting.
Security and resilience: Each blockchain node or entity is associated with a pair of public and private keys. Blockchain uses the techniques cryptography and digital signatures to provide the

ownership of data. Each transaction, you need to sign the transaction in order to put into the blockchain.so the device which holds the private key, will allow the transfer of ownership of digital assets.

Automation: blockchain enables the users to create streamlined applications to deal with complex business processes that involve multiple intermediaries using a more important concept called "smart contracts". Smart contracts is basically a piece of code stored on a blockchain which enables automation of complex business logic. Blockchain already provides this number of salient properties what are the implications of these properties for securing IoT applications

Security Implications for IoT Applications:

Decentralization: It means if we use blockchain in our system we can remove the single point of failure efficiently. Blockchain are run by a numberof nodes in a peer-to-peer mode, which means there is no single point of failure in the blockchain systems.

Immutability: It will ensure data integrity in our system

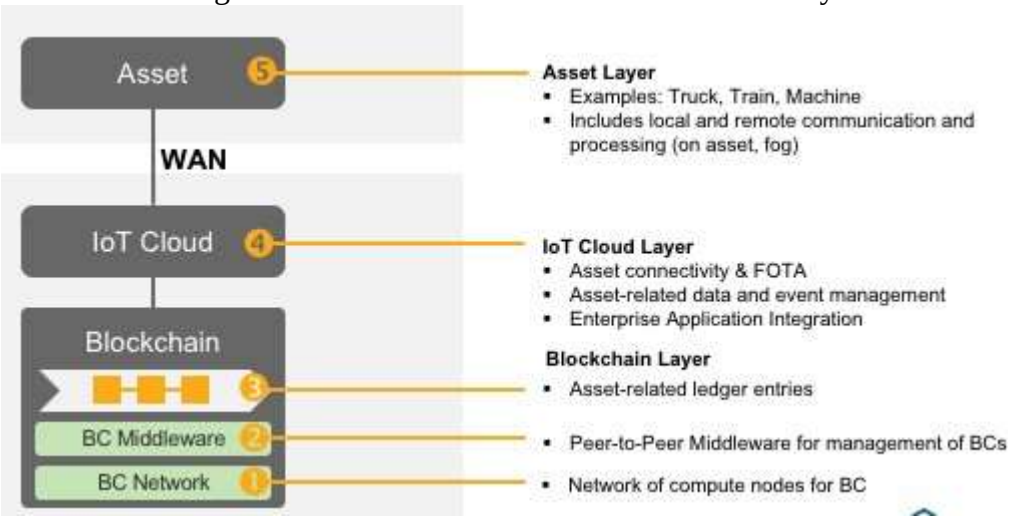
Transparency: This property, supports to track status of our connected devices as well as the associated physical assets.

Security and resilience: It will enable us to authenticate users and devices efficiently. Each user and device in the blockchain ecosystem areassociated with a pair of keys. we can use public key cryptography to quickly authenticate users and device in our IoT system

Automation: Using blockchain we can smart contracts to build trust among the different IoT processes and eventually eliminate trustedintermediaries and reduce the system cost

Blockchain & IoT reference Architecture:

To know how blockchain is integrated to IoT we need to know about Blockchain & IoT reference Architecture. This Architecture was developedby the Trusted IoT Alliance together with IoTex trusted IoT. Blockchain integrated with IoT architecture consists of three layers



Asset layer: The first layer in Blockchain & IoT architecture we attach our device to any physical assets which will send data about the status of our physical asset to a cloud backend which is the second layer.

cloud backend: This layer will host all of the essential security services and other services to manage the IT solutions in the applications. Blockchain layer: It will store asset related entries which are related to our different types of applications.

This architecture is a hybrid architecture mixed with Cloud and blockchain which combine to form a very powerful backend to support your IoT applications. So when we integrate the blockchain into the IoT systems you can actually have multiple integration patterns which have been further investigated by the IIC. so, the integration patterns which already cover a wide range of IoT applications and use cases

The blockchain & IoT integration patterns:

Blockchain technology is integrated with IoT by using the patterns. The integration patterns are divided in various steps which are

Asset-IoT Cloud- Blockchain

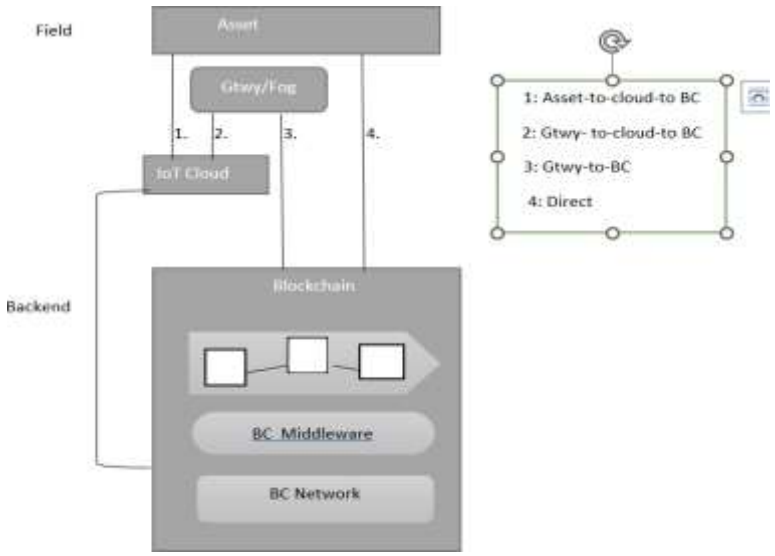
The first one is the asset to IoT cloud to blockchain, in this integration pattern targets IoT devices without the use of power constraints that havecellular connectivity to communicate with the IoT Cloud using IoT data. This layer is very popular and typical integration patterns for enterpriseand industrial IoT applications. In this pattern, the IoT cloud manages all of the asset data and the blockchain serves as the integrity of data andintra organizational data plane across multiple clouds and finally the IoT cloud selects which data to be transmitted and stored on the blockchain. **Asset → Gateway/Fog → IoT Cloud → Blockchain:**

The second one covers resource constrained IoT devices and is mainly focused on the low power IoT devices which need an IoT gateway or fog node to reach the backend. There are certain integration patterns that more aim to target more futuristic computing paradigms such as edge and fog computing. This does not use cloud as one of the components, which means we will be more focused on the edge and fog computation in this case.**Asset → Gateway/Fog → Blockchain**

The third pattern covers emerging computing and will directly go from our smart devices to the blockchain, which is for completely decentralized applications focused on machine-to-machine communications.

Asset → Blockchain

The fourth pattern targets machine- to -machine communication and payment scenarios Where IoT devices are integrated with cellular modules which can run either a light client or full node to communicate with other nodes in a decentralized manner.



EXISITING SYSTEM:

Blockchain technology provides security in existing systems that provide security for IoT applications, but there are many problems such as: Modern malware designers and cyber attackers are constantly trying to innovate and circumvent existing countermeasures (for example, by generating different versions of malware through mutation). Most of his existing IDS and IPS approaches are designed to detect unauthorized access attempts and distributed standard protocols. The goal is to confuse scanning attempts. Also, network paths are changed regularly to prevent unauthorized access and traffic scanning. However, the number of generated packets can be excessive. Olagunju and Samu designed an automated honeypot for real-time intrusion detection, prevention, and remediation using a centralized approach to logging systems (aka puppets and virtual machines). A centralized system gathers information from the attacker's source address, time, and country. This approach uses freely available open source technology to reduce the manual work required to dynamically

change a highly interactivehoneypot
Merlo, Migliardi, and Spadacini proposed an adaptive mechanism that accounts for full account prediction errors and residual traffic. This model was evaluated in a network simulator and the delays were calculated.

PROPOSED SYSTEM

In the proposed system we further analyse these cybersecurity attacks against home Ip camera systems, we can see there are many security concerns we need to consider when we design these types like. Firstly, home IP camera systems use the traditional username and password based login solutions. Users in this case often use a very poor passwords without multifactor authentication enabled in this system, which leads to many significant attacks called credential stuffing attacks. So this type of attack, hackers will use a leaked password to try to access our home Ip system camera. Another security concern is about database breaches, which will lead to password leakage as well as ownership compromise. The third one is insecure device binding, which will enable an attacker to also take over the camera ownership. The last one is the data integrity for our local and cloud storage is a concern. Users want to protect the integrity of their data whether they store data locally in the SD card of a home IP camera or store data remotely in cloud storage. So that they can insert, delete and modify of the video will be done.

So blockchain will solve all of these security challenges.

The first idea is can we replace the traditional username and password-based login with a password less ideas by using blockchain wallet which are automatically generated on our mobile app. Each blockchain wallet is associated with a pair of keys- the private key will be securely stored on the mobile phone inside the secure enclave. So, the blockchain address will be passed to IoT cloud for user account registration and each user account in this case will contain a blockchain address and a random challenge. So, the mobile app each time will start a random challenge to complete the login after the user's confirmation and the java web token will be issued to the user to access Cloud storage or other cloud services. After each successful login attempt, the random challenge will also be updated. In this way user does not need to remember their password as the blockchain wallet will manage the users private key in a more secure manner. We can completely remove the username password and similar types of login systems and facilitate users to just use one click login using blockchain technology. So, in this way we can address traditional login solutions.

The second one is how we can further secure the ownership of the camera. The idea here is that we will borrow the resurrecting Duckling security Model. In this model when we open a camera for the first time it will look for blockchain address and recognize it as their owner. The camera will associate its own blockchain address with its owners and invoke a smart contract on the blockchain which will manage the ownership. Each device will restart the device binding and the blockchain will serve as the ground truth regarding device ownership. In this case we can see we can protect device ownership using blockchain technology instead of a centralized server, which enhances the security of the system and protects against hackers taking over the camera ownership.

The third idea is how we can use blockchain-based technology to ensure data integrity. Basically, the user can enable a data integrity feature on the mobile app and specify the time period in days for checkpoint commitments. And then the camera can build a merkle tree dynamically for all the video clips they collected. In the third step, the camera will invoke the checkpoint management smart contract for integrity checkpoint commitments. The user is able to verify the data integrity of the vedio clips retrieved from the SD card or their remote storage with the merkle root. When the user retrieves the data from the local SD card or the remote Cloud storage, they can easily verify whether the data has been manipulated or not. In this idea, the blockchain provides a data integrity layer along with your cloud application. So these are basically three ideas you can use the blockchain to protect your IP camera systems.

CONCLUSION:

we would like to highlight the design methodology here. In home IP camera systems, we replace the traditional username and password-based login with a password-less login using a blockchain wallet. We further enhanced the security of device ownership using a smart contract on the blockchain and data integrity. When blockchain and IoT combine together will provide a powerful approach for new business models and distributed application.

REFERENCES:

1. Q.K.A. Mirza, G. Mohi-Ud-Din, I. Awan **A cloud-based energy efficient system for enhancing the detection and prevention ofmodern malware** 2016 IEEE 30th International Conference on Advanced Information Networking and Applications(AINA) (2016),
2. F. Cadet, D.T. Fokum Coping with denial-of-service attacks on the IP telephony system Southeast Con 2016 (2016), Norfolk, VA
3. D.H. Sharma, C.A. Dhote, M.M. Potey Implementing intrusion management as security-as-a-service from cloud 2016 International Conference on Computation System and Information Technology for SustainableSolutions (CSITSS) (2016), Bangalore
4. Amos O. Olagunju, Farouk Samu In search of effective honeypot and honeynet systems for real-time intrusion detectionand prevention Proceedings of the 5th Annual Conference on Research in Information Technology (RIIT'16), ACM, New York, NY, USA (2016),
5. M. Yevdokymenko An adaptive algorithm for detecting and preventing attacks in telecommunicationnetworks 2016 Third International Scientific-practical Conference Problems of Infocommunications Science andTechnology (PIC S&T) (2016),Kharkiv
6. H. Sedjelmaci, S.M. Senouci, M.A. Messous How to detect cyber-attacks in unmanned aerial vehicles network? 2016 IEEE Global Communications Conference (GLOBECOM) (2016), Washington, DC
7. A. Gharib, I. Sharafaldin, A.H. Lashkari, A.A. Ghorbani An evaluation framework for intrusion detection dataset 2016 International Conference on Information Science and Security (ICISS) (2016),Pattaya
8. V. Chang, M. Ramachandran Towards achieving data security with the cloud computing adoption framework IEEE Trans. Serv. Comput., 9 (1) (Jan.-Feb. 1 2016),
9. Proofpoint **Proofpoint uncovers internet of things (IoT) cyberattack** Proofpoint Release (2014) http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799

