Realizing IoT Using Blockchain

B.K.Hemant
Assistant Professor, MSIT
Email: bkhemant@msit.in

Shivesh Navin
Student, MSIT
Email: shiveshnavin@gmail.com

Adil Ahmad
Student, MSIT
Email: adil.jackson98@gmail.com

Neha Bansal
Student, MSIT
Email: bansalneha1106@gmail.com

Abstract: *Internet of Things will change the future of technology by unifying everything in our world and would ease the interactivity with real world objects. But with increasing demand of intelligent systems, intrusions and penetrations become inevitable aspects of Internet of Things. The main objective of this paper is to give solution for a robust infrastructure. Moreover, it will give a comprehension for Blockchain technology and certainly provides a scope for research in this field.*

Keywords: Internet of Things, Blockchain, Wi-Fi, Bluetooth, sensors, actuators

1. Introduction

IoT composes of a number of linked smart devices , connecting these devices has been traditionally done by a centralized infrastructure based network where , a single host pledges network access to all the IoT devices . Such a setup poses consequential threats like clustered network breakdowns , compromising all the devices if the core is infected . IoT-Blockchain uses the concepts from Adhoc and Blockchain to counter these problems by means of PBFT [2] , CPS [1], resource mining, end-to-end encryption and additionally providing features like resource sharing, fault isolation .

2. Problems

In a study by Ponemon Institute, Only 30% of respondents say their organization allocates

sufficient budget to protect mobile apps and IOT devices[5] .

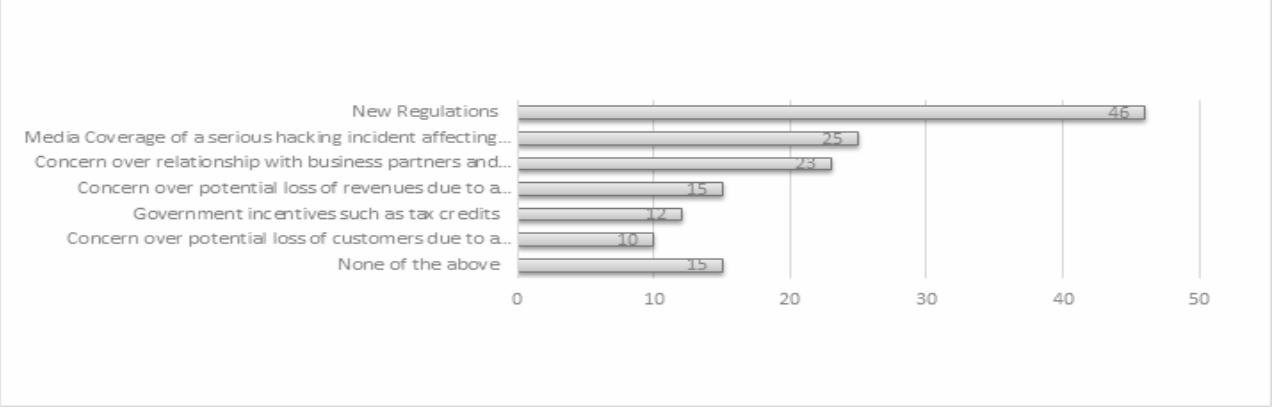

Fig.1. Survey on Losses due to system insecurity

The Internet of Things can simplify and automate our lives for us. However what we often ignore is that under all the convenience, manufacturers of these smart devices can also use the personal data. As the “virtual us” syncs with our personal data in all time, it grows with us and shares all our behaviours. It's like a mandatory contract signed without our consensus as long as we want to use our smart devices, we need to give away our personal data for the benefit of availing the services.

2.1. Why Encryption is Necessary?

Encryption relies on advanced algorithms known as ciphers. The primary purpose of any coding methodology is to protect sensitive data from others by processing information into long series of random or pseudo-random ciphers. In simplified type, a sensitive data is converted into an undecipherable forma and the information is encrypted by employing a special coding key. It will solely be decrypted with that special coding key. The major objective is to make the data encrypted by the network using blockchain technology.

2.2. Why Adhoc can be the face of IOT?

A decentralized network provides greater mobility for a user. In order to reduce the deployment cost in any network, blockchain technology is required to make it happen.

2.3. Resource Allocation in IOT

Resource management is a complex process since any network based upon Internet of Things comprises of heterogeneous components. To extract essential services from the huge amount of data generated by such components, resource management techniques must consider processing and storage capacities.

3. Implementation and solution

3.1 Adhoc

Infrastructureless networks require devices to frame a tight interconnection before any communication takes place . To do so, An Ad-Hoc network[4] inspired by Practical Byzantine Fault Tolerance (PBFT) [2] is implemented , where each node supports AP (Access Point) and STA (Station) modes of WiFi . An adhoc network is thus formed by scanning for nearby connectable nodes by each device and connecting to the most suitable node’s AP among those discovered .

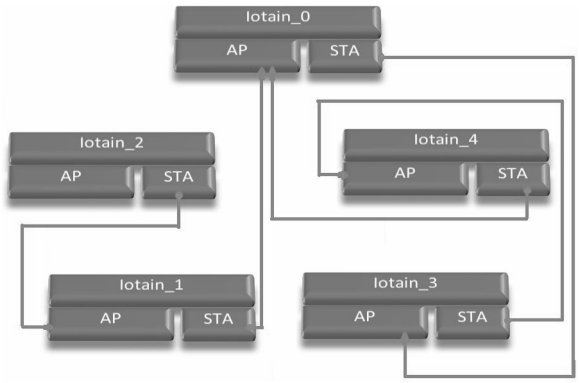

Fig. 2. Adhoc network consisting 5 nodes

Each host is allocated its own IP address space based on a consensus[3] so as to prevent duplicate IP address assignments . Additionally, LEDs are also used to denote the connecting/connected states on each node .In case a node goes down the affected nodes automatically practice the network buildup algorithm and the system recuperates .

3.2 Resource Sharing

The resources are compartmented and their interface can be used by any authorized node by means of a request response model . Requests that are made for accessing resources are recognized by the interfacing iotain device i.e. the iotain device physically connected to the IoT

commodity . After executing the job and dispatching back result by callback[1] , the resource is free to serve the next request , thus facilitating resource sharing . For instance , the same LCD can display text sent from any authorized device on the network .

Resources Used :

1. I2C LCD Display
2. Google Cloud
3. Human Proximity Identifier
4. Capacitive Touch Button

3.3 Blockchain - Resource Mining & Cryptography

Concepts of blockchain are used to discover resources scattered through network and secure the communications through a Cyber Physical System (CPS)

3.3.1 Resource Mining

1. A request is generated by compiling a unique id , IP of the requesting node , resource ID and the encrypted payload. It is then broadcasted to all the iotains connected to the requesting node via the *`on_request`* RPC[1] present on all other nodes .
2. On receiving *`on_request`* at the next node , request is saved in the request table and resource is looked up for in the local resource table . If the resource dosen't exists then the request , is passed to the next same as step 1 after replacing the source address with the IP address of the local node .
3. In case of resource table hit i.e. resource is connected locally , the payload is decrypted as per the consensus[2] and the parameters from the payload are used to perform the requested job via *`on_resource`* function . The result is then reverted to the immediate source via the *`on_callback`* RPC.
4. On receiving *`on_callback`* the request ID is used to find the request from the local resource table and subsequently the previous immediate source address . Again the response is forwarded to the *`on_callback`* of that node .This process continues in a chain until the response reaches the ultimate original requester .

3.3.2 Cryptography

The payload that incorporates the information about how the resource will be used and the various associated parameters must be secured from tampering and eavesdropping while in transit . An end-to-end encryption is thus employed for realizing security . The algorithm for encryption is written in Native C and packed in the base iotain flash firmware . It works in conjunction with the calls from mJS through Foreign Function Interfaces (FFI) .

3.4 Hardware Implementation

Hardware implementation of the system involves the use of PCBs to construct boards that will hold the ESP devices connected along with their local resources and a power unit . Proteus ARES is used to develop the PCB schematics[1] and fabrication is done on silicon wafers .

3.6 Emulator

Since the demonstration can be difficult using the actual hardware everytime and for sake of fast demonstration and prototyping , a separate emulator is built in NodeJS capable of running the same mJS code as run on the actual devices. The emulator works by providing the closest approximation of the system APIs of Mongoose-OS . The support for the APIs are limited , but still capable of providing GPIO , Serial , RPC , Config and most of the other APIs used by an iotain device . Thus multiple

instances of iotains can be run on any computer and the iot_blockchain can be demonstrated using the inbuilt GUI .

Fig.3. Iot-Blockchain by 5 Emulator Instances

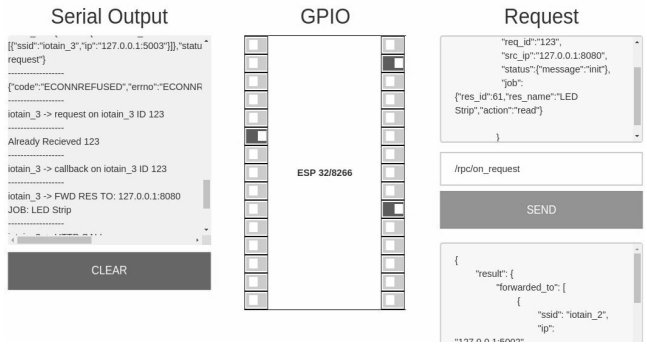

Fig. Emulator Graphical User Interface

4. Future Scope & Conclusion

Both IoT and blockchain are in their emergent stages, with the promise of a future where machine-to-machine communication will be proficient. Currently, firms are putting efforts into merging the two technology powers together. Once combined, IoT and blockchain technology will let several industries thrive by easily monitoring, tracking and securing information. Blockchain technology can surely contribute to the emergence of intelligent infrastructure in the field of Internet of Things. Although the extension of this concept has inevitable shortcomings such as security, scalability, data analysis, etc. which further provides scope for research in various sectors of industrial automation, resource management, etc. This would help the Internet of Things realize its true potential.

5. References

[1] Navin, Shivesh. “iot_blockchain.” *GitHub*, 5 Mar. 2019, http://github.com/shiveshnavin/iot_blockchain .

[2] Castro, Miguel. Practical Byzantine Fault Tolerance. *Institute of Techonology*, 2001.

[3] Navin, Shivesh. “Network Formation iot_blockchain.” *GitHub*, 1 Nov. 2018, https://github.com/shiveshnavin/iot_blockchain/blob/master/ota_server/public/worker_0.js#L337 .

[4] Murthy, C. Siva Ram. Ad Hoc Wireless Networks: Architectures and Protocols. *Prentice Hall*, 2012.

[5] “2017 Study on Mobile and Internet of Things Application Security.” Arxan, *Ponemon Institute*, 2017, https://media.scmagazine.com/documents/282/2017_study_mobile_and_iot_70394.pdf .