International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Securing and Automating IoT Devices using Blockchain - Smart Light Grid

Satyam Raikar[1], Priyanka Jamadar[2], Akshata Sawant[3], Pratik Mandal[4], Aseema Jana[5]

[1, 2, 3, 4, 5]Dr. D. Y. Patil School of Engineering & Technology, Pune, Maharashtra – 8796518001, India

[1]satyamraikar464[at]gmail.com
[2]priyankajamadar16[at]gmail.com
[3]akshatasawant1805[at]gmail.com
[4]ptmandal64[at]gmail.com
[5]aseema.jana[at]dypic.in

Abstract: ***Most of the Internet of Thing's (IoT) devices are Deployed in Centralized Way as of Today. This System is exposed to many issues: scalability, high overall costing, privacy concerns, security risks and lack of potential functional values. Blockchains decentralization nature can be a perfect solution for this concern. First Blockchain is Elastic enough to solve the Scalability issue with cost effective solution. Second It Retains Data in the most efficient way of integrity and immutability and Third Blockchain with its Smart Contract has Huge Potential in Automating and Intercommunicating with Devices with Functional Values.***

Keywords: Automation, blockchain, decentralization, IoT, immutability, scalability, smart contract.

1. Introduction

In last decade with exponential advancement in existing technologies and newly incorporated technologies IoT and Blockchain has significant role and has more to grow and revolutionize all domains associated with them. Like Automation, Device Efficiency, Device Security, End to End Payments and Interconnection between Smart Devices. [1] Mostly the IoT devices used in the Industry are low energy and lightweight. As the main functionality of these Devices are to Execute the provided commands and Devote most of its energy for computation and executing core applications, to make task affordable. But making Affordable Security Systems and Privacy Concerned Mechanisms are Quite Difficult. There are many State-of-the-Art Security Frameworks but due to centralized nature they are not suitable for IoT Applications to handle huge amount of data and difficulty to scale while managing data Securely.

[2] To handle User Privacy, Existing methods often uses various methods like adding Noisy Data, Partial Data according to Request or even Incomplete Data Sometimes, which may affect the working and Execution of Corporate or Personalized Services. [3] Consequently, IoT demands a lightweight, Scalable, Distributed, and Always Online Network without Much Point of Failures. [4] The Blockchain Technology which is the Base of Bitcoin the First Crypto currency System, has the potential to overcome aforementioned challenges as benefiting from its key values like being Distributed, Secure, Private/Public, Immutable and Trustworthy.

Ethereum is Similar to Bitcoin but with more capabilities then being an Asset or just a Crypto Currency. Ethereum (ERC20 Based Blockchain) users that are known by a Public Key (PK), which generate and broadcast transactions to the network to transfer Asset and Execute Smart Contracts. These transactions are pushed into a block by users. Once a block is full, the block is appended to the Chain by performing a mining process.[5] To mine a block, some specific nodes known as miners try to solve a resource consuming cryptographic puzzle named Proof of Work (POW) as for Ethereum 1.0, and the node that solves the puzzle first mines the new block to the Chain.

We proposed Solution based on Blockchain by Using ERC20 based Blockchains i.e. Ethereum in our case as a Best Feasible Solution to overcome above mentioned issues by eliminating the concept of Centralization and the need for Intermediaries being the Priority. Our proposed framework relies on smart contracts and distributed trust to maintain security and privacy while making it more suitable for the specific requirement of IoT where Transparency being an optional functionality based on type and place of use.We Propose a Smart Solution for Managing Smart City Light Grids by Using Blockchains technology the overcome various Issues like DDOS attacks, Device Authenticity and Proper Governance and On Time Management of Lights.

2. Proposed System

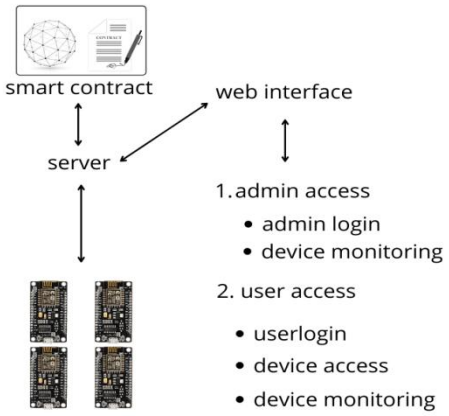

Figure 1: Proposed System

This Model Ensures:

a) The Components Used are Authentic and there is no Corruption in between and legitimacyabout the Light Quality
b) 24/7 365 Days Report of Live Status of the Grid with Original Inputs and no Discrepancy.
c) Repair Reports and Payment Processing without Interruption.
d) Transparent reports.

3. Core Components

The design consists of three core tiers that are: a) Device Security, b) Data Storage and c) Interaction with Blockchain for Automation.

a) Device Security

A list of Unique Authentic Devices is Stored as a Contract which is Immutable and Cannot be Updated unless a certain Criteria is met. Each Device is provided a Unique Hash number comprising of various factors like Issuer, Firmware Version, Device ID, and Device Model. Which has to be in the database or list of authentic devices to join the network to execute Further Commands and Run as an Authentic Device on the Network. This ensures that the hardware device is not Cloned or not Injected with Malware or any Malicious Script.

Input:

```
{
    "Issuer": "ABC Tech",
    "Firmware Version": "v 1.168456546",
    "Device ID": "236Z",
    "Device Model": "A1"
}
```

MD5 Hash Output:

```
d038527a794dc208b8805e708517041c
```

The Official firmware file contains a specific MD5 hash which is key element of the Hash Key Used for the devices Authentication. If there is any tampering with the Firmware file the MD5 hash changes which makethe final hash incapable of confirming its authenticity and will be unable to connect with Chain.

b) Data Storage

Total Report will be Stored on a Server which will push the necessary information further to blockchain which is useful to execute further commands. The Live Data depending on the conditions will trigger smart contracts.

4. Case Study

IoT being a $1000 B. Industry by 2025 will bring new challenges for managing devices and services related to them, our current technology is be inadequate if not properly developed to handle such scalability and data which will adversely effects network security, Data Security, security of devices and Proper Automation.Blockchain has potential to solve all the issues within its own Ecosystem and at much lower cost. Leveraging the exponential potential of Blockchain we can overcome all the drawbacks faced by IoT Industry Currently.

5. Conclusions

We can conclude that without using blockchaintechnology with IoT devices, it is difficult to provide security to respective IoT devices. Thus there is need of blockchain to secure the IoT devices and to give the authentication properly using blockchain. In some technical, non-technical, medical and industrial fields there is need of IoT device and that IoT device handles number of important data and that data needs to be secured and need to be handled by authentic person to prevent attacks and maintain security.

References

[1] Low-Energy Security: Limits and Opportunities in the Internet of Things: January 2015IEEE Security and Privacy Magazine. W. Trappe, W. Trappe
[2] Noise-added selection method for location-based service using differential privacy in Internet of Things: January 28, 2019 SAGE Journals, Zhimin Li, Haoze Lv, Zhaobin Liu
[3] Moore, S.J., Nugent, C.D., Zhang, S. et al. IoT reliability: a review leading to 5 key research directions. CCF Trans. Pervasive Comp. Interact.
[4] S. Nakamoto. (2008).'Bitcoin:A.PeertoPeer.electroniccashsystem,'https://bitcoin.org/bitcoin.pdf
[5] Blockchain for IoT Security and Privacy: The Case Study of a Smart Home: Ali Dorri, Salil S. Kanhere, Raja Jurdak and Praveen Gauravaram
[6] Serguei Popov, IOTA Foundation,and IOTA: Feeless and Free *IEEE Blockchain Technical Briefs*, January 2019