A New Approach to Secure IoT Devices Using Blockchain and SmartContract

Mrs.S.C Budruk
Computer science and engineering
Nanasaheb Mahadik College of Engineering.
Peth, India.
scbudruk@nmcoe.org.in

Rohini Rajkumar Mandave
Computer science and engineering
Nanasaheb mahadik college of engineering.
Peth, India.
rohinimandave90@gmail.com

Priyadarshani Sanjay Nanaware
Computer science and engineering
Nanasaheb mahadik college of engineering.
Peth, India.
priyananaware42@gmail.com

Anuja Sangram Mane
Computer Science and EngineeringNanasaheb Mahadik College of Engineering.
Peth, India
anujamane24@gmail.com

Pratiksha Shantaram Jadhav
Computer Science and Engineering Nanasaheb Mahadik College of Engineering.
Peth,India
pratikshajadhav0707@gmail.com

***Abstract*—** The conception of Block chain has penetrated a large vary of scientific areas, and its use is considered to rise exponentially within the close to future. death penalty short scripts of predefined code called sensible contracts on Blockchain will eliminate the requirement of intermediaries and might conjointly raise the multitude of execution of contracts. During this paper, we have a tendency to discuss the conception of Blockchain on with sensible contracts and discuss their pertinence within the web of Medical Things (IoMT) in the e-healthcare domain.In this paper we propose a Smart Solution for Securing IOT Devices using Block chain and Smart Contract. Existing System has many issues. To overcome these various Issues like DDOS attacks, Device Authenticity and Proper Governance and On Time Management, Block chain has potential to solve all the issues within its own Ecosystem and at much lower cost. Leveraging the exponential potential of Block chain we can overcome all the drawbacks faced by IoT Industry Currently.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. 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.

Keywords—: Block chain; Internet of Things; smart contracts; decentralization

Introduction

Block chains and good contracts are a rising, promising technology that has received significant attention. We have a tendency to use the block chain technology, and specifically Ethereum, to implement a large-scale event-based net of Things (IoT) system. We have a tendency to argue that the distributed nature of the "ledger," similarly as, Ethereum's capability of parallel execution of replicated "smart contracts", give the wanted automation, generality, flexibility, resilience, and high convenience. We have a tendency to style a practical block chain-based IOT design, victimization existing technologies whereas by taking into thought the characteristics and limitations of IoT devices and applications. Moreover, we have a tendency to leverage block chain's immutableness and Ethereum's support for custom tokens to make a strong and economical token-based access management mechanism. Our analysis shows that our answer is viable and offers important security and value benefits.

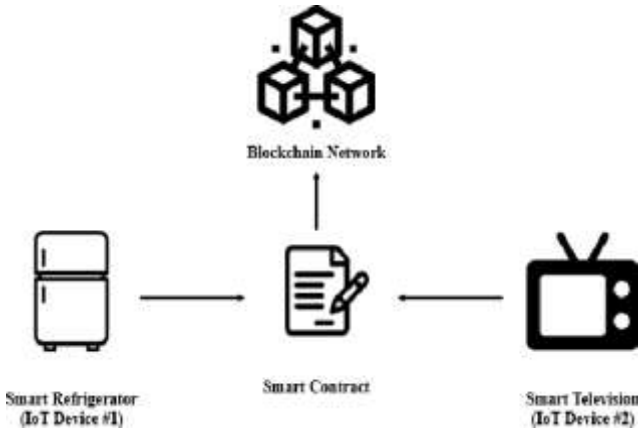
I. BLOCK CHAIN TECHNOLOGY

The exponential increase in connected devices with intrinsic sensing, processing, and communication capabilities has fuelled the event of IOT applications, that creates new ecosystems for device-to-device interactions, supports good environments, and results in new business models. Authorized by these capabilities, IOT devices act with one another and their environments to gather, process, and share knowledge. Security, privacy, and responsibleness of information area unit are the major considerations that require to be addressed for the event of IOT applications. Recently, block chain technology has attracted important interest from researchers and trade leaders thanks to its potential for enhancing security, privacy, and irresponsibleness of the information. Block chain offers distributed and changeless ledgers for IOT communications within the type of tamper-proof records, intrinsic crypto currency support for transactions between devices and alternative entities, and good contracts to execute machine-controlled programs once sure conditions area unit met. Though there are unit potential advantages of the mixing of block chain technology to IOT, the mixing introduces new challenges, like quantifiability, within the style of block chains fitted to IOT applications. During this chapter, we tend to explore key advantages and style challenges for block chain technologies, and potential applications of block chain technologies for IOT.

A. What is smart contract

Smart contracts are the theoretical and technical rules and policies, coded among the block chain atmosphere, that govern transactional agreements hosted on a block chain network. They're designed within blockchain applications or created as a complete application that rides on a block chain network. For a group action on a blockchain network to require place, a sensible contract ensures the policies to execute associate degree exchange of data ar glad. as an example, if a automobile sales group action system runs on a blockchain application, rules would be established to represent a fortunate group action involving client credit checks, profit threshold, etc. If these rules aren't met, such the customer's credit history doesn't meet the necessities, the appliance would trigger associate degree alert and also the

group action try would be mechanically denied by the parties on the block chain.



II. Literature Review

Internet of things security being a sizzling topic for researcher today, there is a myriad of publication indicating security and privacy issues in IoT. Due to huge number of IoT devices and machine to machine communication feature of IoT, legacy authentication and authorization techniques are not viable for it. Devices must authenticate each other before exchanging any information between them (M2M communication) which is a challenge for researcher due to massive number of devices. Some of the work related to device authentication and access control in IoT are discussed here.

Chen et al. [6] proposed Capability-based access control model for distributed IoT environment. It supports group access by using single token and guarantee end to end security using IPsec. A requester can use a single token for group access (Group of devices that offer common services) to communicate with any device in the group. Network prefix of unique local identifier (ULA) is used as access group identifier. Each device in the group is identified by a ULA. In a group access token the requester puts its ULA and the network prefix of access group. Hence the devices in the group can verify the token using its ULA and prefix in the token. It can also provide access control based on requester ULA in the token.

The existing standards like TLS and PKI addressed the first three domains of security i.e. confidentiality, integrity and authentication. However access control requires attention. As in multi-agents system different agents have different roles, they require different access levels. Rivera et al. [7] proposed the use of User-Managed Access model, which is profile of OAuth 2.0 and provide different access levels to different agents.

OUADDAH et al. [9] proposed Novel access control framework for IoT environment called "SmartOrBAC" which is based on OrBAC model. This model used web services (RESTFUL approach) to enforce the security policies. Organization based Access Control (OrBAC) have some limitations like, it works better in Centralized system, it does not address the collaboration between Organizations and sub organizations and OrBAC does not translate the security policy in to access control mechanism. Therefore to address these limitations of OrBAC, SmartOrBAC which is an extension of OrBAC is proposed. SmartOrBAC uses web services to ensure secure collaboration between different organizations. They also emphasis on using RESTFULL API for exchanges between organization as it uses a light mechanism.

The interaction between the organizations is defined by agreement between the organizations. The organizations together defined the access rules according to OrBAC format. In SmartOrBAC the contract is not done priori but it can be done on the fly in a spontaneous and dynamic way. SmartOrBAC provides efficient access control for collaborative entities with low power and energy constrained scenarios like such as IoT. Gaikwad et al. [10] used three level secure Kerberos authentication for smart home system using IoT. It uses secure hash algorithm SHA 1 and advance encryption standard (AES) for security. However neither Kerberos is sustainable solution for authentication nor AES is practical for constrain IoT devices.

Periera et al. [11] proposed Service level access control framework for power constrained devices. The framework allows per service fine grained access control. It merge the idea of Kerberos and RADIUS access control systems for reliable access control framework. It uses the best features of Kerberos, Constrained Application Protocols (CoAP) and RADIUS to create a low power platform for Access control and authentication aspects. The CoAP client get the ticket from the CoAP server, and use this ticket in each future CoAP request. There are Two Steps for Authentication and second for Access control. The user is first authenticated based on credentials like shared key, password or other validator. On successful authentication the CoAP-NAS is informed about the users and its permission, time out of ticket, group etc. CoAP-NAS send a ticket to the user for future requests. In access control step the server will only respond with the correct message if the request message have a valid ticket otherwise it will generate an error message.

III. Proposed System

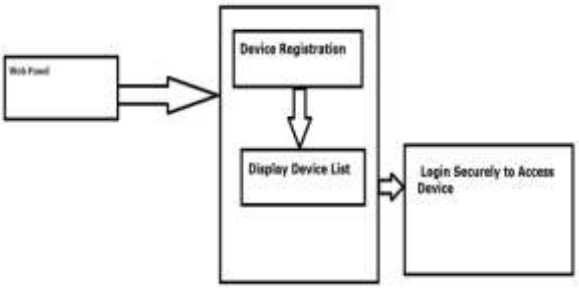


Figure 1.Work flow of Proposed System

We Propose a Solution based on block chain by using ERC20 based block chain Etherium network In our case a feasible solution is a decentralized software platform

Our Proposed framework relies on smart contracts & distributed trust to maintain security & privacy.

This model ensures

- The component is used for authentic & there is no corruption in between & legitimacy about light quality
- 24/7 365 days Report of live status with original IP & no discrepancy
- Repair reports & payment processing without interruption
- Transparent reports

How it works

- Device connect to chain to request permission
- If device is genuine the chain returns as a token & serve information
- The device connects with the server with given token and stores all data

- The Information can then be accessed via website.

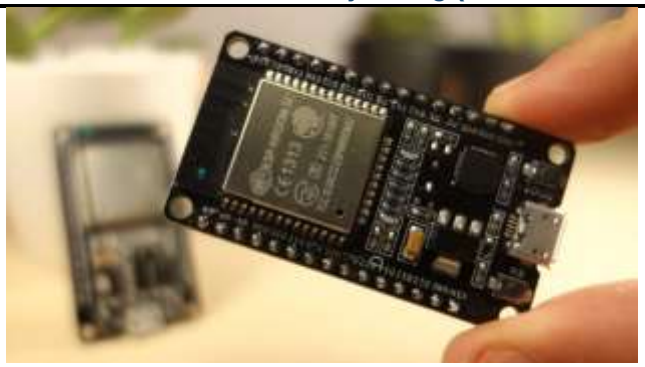
A. Hardware Description

1. ESP8266

The ESP8266 may be a cheap Wi-Fi micro chip, with a full TCP/IP stack and microcontroller capability, The chip initial came to the attention of Western makers in August 2014 with the ESP-01 module, created by a third-party manufacturer Ai-Thinker. this small module permits microcontrollers to connect to a Wi-Fi network and build straightforward TCP/IP connections victimization Hayes-style commands. However, at first, there was nearly no English-language documentation on the chip and so the commands it accepted. The really low price and so the incontrovertible fact that there are solely some external parts on the module, that suggested that it should eventually be really low-cost in volume, attracted many hackers to explore the module, the chip, and so the code thereon, still on translate the Chinese documentation. The ESP8285 is associate ESP8266 with one MiB of inherent flash, allowing the building of single-chip devices capable of connecting to Wi-Fi. These microcontroller chips ar succeeded by the ESP32 family of devices, yet because the pin-compatible ESP32-C3

2. ESP32

ESP32 may be a series of cheap, low-power system on chip microcontrollers with integrated Wi-Fi and dual-mode Bluetooth. Xtensa LX6 kick in every dual-core and single-core variations and includes inherent antenna switches, RF balun, power equipment, low-noise receive equipment, filters, and power-management modules. ESP32 is created and developed by Espressif Systems, a Shanghai-based Chinese company, and is ready-made by TSMC victimization their forty nm methodology.[2] it is a successor to the ESP8266 microcontroller.



CONCLUSION

Block chain technology is revolutionary. it will produce life simpler and safer, energizing the strategy personal information is hold on and also the method transactions for goods and services unit created. Block chain technology creates a permanent and changeless record of every dealings. This impenetrable digital ledger makes fraud, hacking, data theft, and information loss insufferable. The technology will have a bearing on every business among the planet, alongside manufacturing, retail, transportation, healthcare, and assets companies. A block chain could also be a tamper-evident, shared digital ledger that records transactions terribly} very public or personal peer-to-peer network. The block chain acts joined provider of truth, and members terribly} very block chain network can scan only those transactions that unit relevant to them. In the on the point of future, we've an inclination to expect to ascertain some innovation in block chains to boost performance and quality, which will be a special challenge for public block chains.

REFERENCES

[1] Guessoum, M. T. Laskri, and J. Lieber, “RespiDiag: A case-based reasoning system for the diagnosis of chronic obstructive pulmonary disease,” Expert Systems with Applications, vol. 41, no. 2, pp. 267–273, 2014.

[2] El-Sappagh, M. Elmogy, A. Riad, H. Zaghlol, and F. A. Badria, “EHR Data Preparation for Case Based Reasoning Construction,” in Advanced Machine Learning Technologies and Applications, Springer, 2014, pp. 483–497.

[3] Bahga and V. K. Madisetti, “A cloud-based approach for interoperable electronic health records (EHRs),” Biomedical and Health Informatics, IEEE Journal of, vol. 17, no. 5, pp. 894–906, 2013

[4] Abdel Nasser H. Zaied, Mohammed Elmogy and SehamAbd Elkader, ‘’Electronic Health Records: Applications, Techniques and Challenges” International Journal of Computer Applications, June 2015.

[5] SanketGoyal, Pranali Desai, and VasanthSwaminathan “Multi-Level Security Embedded with Surveillance System” DOI 10.1109/JSEN.2017.2756876, IEEE Sensors Journal

[6] Aleksey Burdakov, UriyGrigorev, Andrey Ploutenko, Eugene Ttsviashchenko “Estimation Models for NoSQL Database Consistency Characteristics” 978-1-4673-8776-7/16 $31.00 © 2016 IEEE DOI 10.1109/PDP.2016.23

[7] San Murugesan, yogeshdeshpande,” Meeting the Challenges of Web Application Development: The Web Engineering Approach” ICSE’O2, May 19-25,2016, Orlando, Florida, USA

[8] Truica, “Performance evaluation for CRUD operations in asynchronously replicated document oriented database,” 20th International Conference on Control Systems and Computer Science, in 2015.