IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Decentralized Block Chain Authentication For Edge-Iot (Dbaei)

[1]Ms. POOJA.V, [2]Mr. RAMESH E R

[1]Student, [2]Assistant Professor

[1] Ms. POOJA V, M.sc CFIS, Department of Computer Science Engineering, DR.MGR UNIVERSITY, Chennai, India

[2]Mr. RAMESH E R, Assistant professor, Center Of Excellence In Digital Forensic, Chennai, India

Abstract: Internet of Things (IoT) devices at the network edge, ensuring secure and scalable authentication mechanisms has become a significant challenge. Traditional centralized authentication systems are often susceptible to single points of failure and struggle with the scalability demands of modern edge environments by outside attacks or internal cheating. In this project using blockchain technology to securing data without any third person to access data without data user knowledge. Pervious they using cloud services to securing data but now I am using block chain concept to securing data nodes format. in that admin send key to user only they generate and access file any third person access admin can report and block person. In cloud platform we can't use this kind of technology to securing data.

Index Terms - Decentralized authentication, block chain technology, IOT (internet of things), block chain-based IOT (internet of things) to secure data, Authentication Protocols, Access Control

I. INTRODUCTION

As the Internet of Things (IoT) continues to expand, bringing smart devices and systems closer to the edge of networks, the need for secure, scalable, and efficient authentication mechanisms becomes increasingly critical. [1] the edge of networks where real-time processing and responsiveness are crucial. While this growth brings enhanced functionality and convenience, it also introduces significant security and privacy concerns. However, it also introduces unique challenges in terms of security and trust, especially with the growing number of connected devices.

The Decentralized Blockchain Authentication for Edge-IoT (DBAEI) concept addresses these challenges by leveraging blockchain technology for authentication, ensuring that IoT devices at the edge of the network can securely verify each other's. to securing data with permission of admin data owner will access data.[2] In this process using unauthorized person can access the information without user knowledge data that will determine certain problem to data owner.

Decentralized Blockchain Authentication represents a promising solution to the growing security challenges faced by IoT ecosystems, particularly in edge computing environments to provide some data's to more securing block chain technology to authentication in. [3] IOT data When combined with smart contracts and lightweight cryptographic techniques, blockchain can provide secure, automated, and efficient identity management for IoT devices operating at the network edge. nature of edge-based IoT deployments, where intermittent connectivity and resource constraints are common.

By combining the advantages of blockchain's decentralized trust model with the efficiency of edge computing, provides a robust, scalable, and secure authentication framework for the next generation of IoT applications.[4] in that data owner will secure data protected with key that data user can't access easy without data owner generate key to access data use block chain data because owner By distributing trust and enabling peer-to-peer verification, DBAEI addresses key limitations of existing approaches and supports and development

II. LITERATURE REVIEW

Hung-Yu Chien and Jia-Lun Tsai [5] had proposed a comprehensive explanation of the components involved, such as IoT devices, edge servers, and the blockchain network, and how they interact within the Edge-IoT environment. A step-by-step description of the authentication process, detailing how devices register, authenticate, and establish secure communication channels an overview of the cryptographic techniques employed, such as elliptic curve cryptography Their work outlines the authentication workflow in a sequential manner—starting from device registration, moving through the authentication.

T. -D. Nguyen and A. Al-Saffar [6] had proposed analyzing the results obtained from experiments or theoretical evaluations, highlighting the effectiveness and efficiency of the proposed scheme. An assessment of the scheme's resilience against potential attacks, such as replay attacks, man-in-the-middle attacks, or impersonation attempts. the authors discuss the implementation of their authentication model using edge computing and sidechain techniques. They detail how edge nodes handle authentication requests to reduce server.

Yiwen Han and Chen yang Wang [7] had proposed decentralized authentication, blockchain integration, and Edge-IoT applications. Their study revealed that teens who frequently use social media before bed are more likely to experience poor sleep quality, which can impair cognitive performance and emotional regulation during the day.. An explanation of how the proposed authentication mechanism was implemented in a real-world or simulated environment, including the tools and technologies used.Performance Metrics Presentation of metrics such as authentication latency, computational overhead, communication costs, and energy consumption, demonstrating the efficiency of the scheme.

Jun Zhou and Athanasios V. [8] had proposed IEEE Communications Magazine. discuss the integration of blockchain technology into Internet of Things (IoT) architectures, particularly in edge computing environments. Their work explores how blockchain can enhance data privacy, access control, and trust management across decentralized IoT systems. The authors propose a framework that leverages smart contracts and lightweight consensus mechanisms to enable secure, automated interactions among devices.

Khan and Salah [9] had proposed present a comprehensive survey of security challenges in the Internet of Things (IoT) and examine how blockchain technology can be integrated to address these concerns. The paper systematically outlines vulnerabilities present at various layers of IoT architecture—such as the perception, network, and application layers—and explains how these can lead to issues like unauthorized access, data tampering, and denial-of-service (DoS) attacks. One of the paper's key contributions is its evaluation of blockchain's potential to decentralize trust, eliminate the need for centralized control, and enhance data integrity and transparency in IoT systems. The authors explore several use cases, including smart homes, supply chain management, and healthcare, where blockchain can provide robust security frameworks.

Abubakar and Mwrwan Abdelrazig [10] had proposed Blockchain-based Authentication and Access Control Mechanism for Internet of Things (IoT) The contributions of this thesis are shown over all layers of the IoT architecture. decentralized model for authentication and access control, aimed at ensuring secure and reliable device interaction without relying on centralized systems. For authentication in IoT communication protocols, the thesis proposed a lightweight authentication and authorization mechanism for the MQTT messaging protocol. Additionally, for authentication and access control at the devices layer, the thesis provided a decentralized authentication and access control for wearable medical devices.

Neha S. Suryavanshi, and Dr. Amol Kumar [11] had proposed the convergence of these technologies has significantly enhanced industrial operations by supporting real-time data handling, scalable infrastructures,

and better resource efficiency attest strategies and solutions aimed at addressing key challenges such as trust management, security vulnerabilities, and optimal resource allocation. This paper presents a critical review of state of-the-art methodologies in these domains, drawing innovations and technological developments to present a comprehensive perspective on enhancing reliability and performance in industrial systems.

III. PROPOSED METHODOLOGY

This aim to design securing IOT (internet of things) data to securing in proposed they used cloud services to securing and stored data. Now I am used blockchain technology to securing data in way of splitting data in nodes securing information. Admin have to give permission to data owner admin will send key to data user, so data owner can generate files. in block chain technology advanced way security sensitive information, including device registration, decentralized authentication, and integration with edge nodes. Securing information block chain that will integrity, security, efficient so data can can't access data without owner permission

- Devices registration and login process
- Data owner generate key to data user to access iot data
- Block chain edge nodes
- Decentralized authentication block chain

Devices Registration and Login Process

Block chain data authentication data owner the device sends a registration request to the server, often including Unique device ID (e.g., serial number, MAC address, UUID) Device type/model Firmware version the server verifies the request (e.g., using an API key or a manufacturer certificate). The device stores the credentials securely for future authentication. The public key serves as the device's identity on the blockchain, while the private key is securely stored on the device.

Data Owner Generate Key to Data User to Access Iot Data

Enable secure access to IoT data, the data owner generates a unique access key or token for the data user. This key acts as a form of authorization, allowing the user to retrieve or interact with the requested IoT data while ensuring that only authorized individuals can access it. Before generating the key, the data owner typically verifies the identity and purpose of the request to ensure compliance with security and privacy policies. Once issued, the key is securely transmitted to the data user and is often time-bound or usage-limited to prevent misuse.

Block Chain Edge Node

Blockchain edge nodes are decentralized computing devices located at the edge of a network that participate in a blockchain system. These nodes perform key functions such as data validation, local processing, and secure communication with the blockchain network. By operating at the edge, these nodes reduce latency, improve real-time responsiveness, and minimize the need for constant communication with central servers.

Decentralized Authentication Block Chain

Decentralized authentication systems can integrate seamlessly with Zero Trust Architecture (ZTA). Zero Trust relies on the principle of always verifying the identity of users and devices, regardless of their location in the network. In a decentralized IoT environment, this means that every device, every transaction, and every interaction is continuously authenticated, and access is granted based on strict identity and trust rules

Research Design

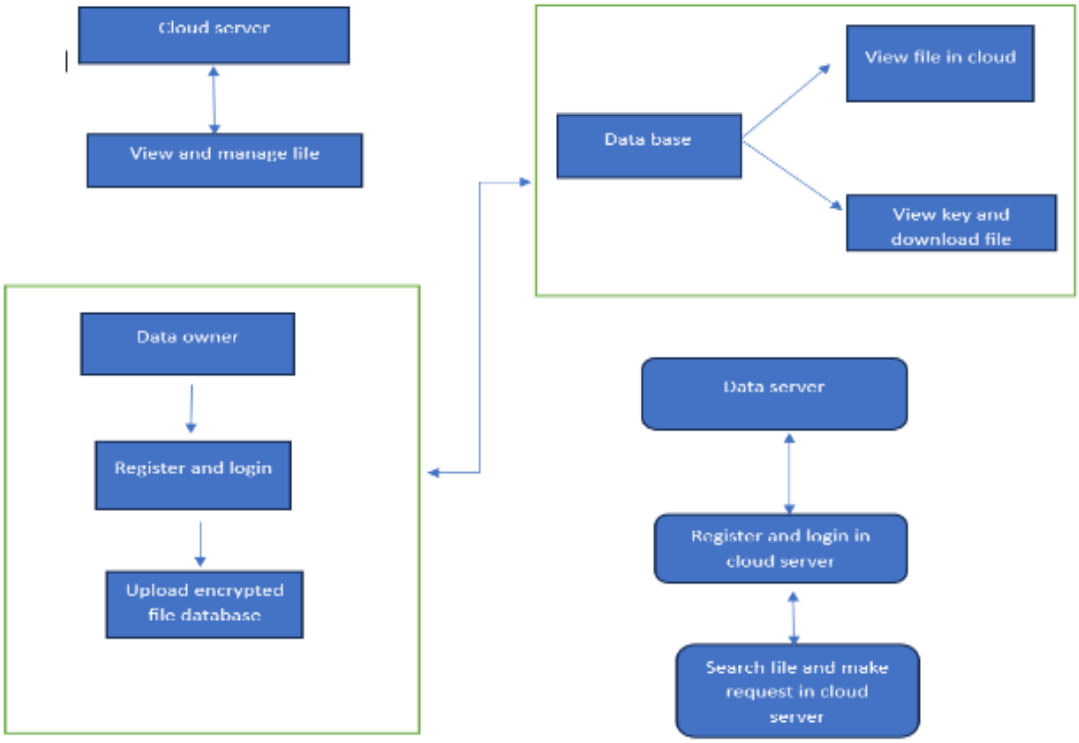

Fig 3.1 System Architecture

In this architecture diagram it will explain concept of decentralized block chain authentication edge -IOT. In that process it will explain how an unwanted activity done in cloud services without using block chain technology Decentralized Blockchain Authentication for Edge-IoT (DBAEI) is an innovative architecture that combines the security benefits of blockchain with the scalability and efficiency of edge computing, specifically designed for Internet of Things (IoT) environments.

In this system, IoT devices, such as sensors or smart devices, initiate authentication requests to edge nodes, which are local processing units that verify the devices' credentials through a decentralized blockchain network. Blockchain serves as a distributed ledger that securely stores device credentials, authentication logs, and smart contracts, ensuring that all data remains tamper-proof and transparent. Smart contracts automatically validate the identity of IoT devices and enforce predefined access control policies, determining whether the device is authorized to access certain resources.

IV. FINDINGS

Create login page for data owner and data owner upload files in block chain. (fig: 4.1) In IoT, this could mean that each device stores its credentials securely in a decentralized network (e.g., blockchain) and can authenticate itself to other devices directly in that processing iot data stored in cloud but in cloud services owner cannot secure iot data that much so we using block chain concept to securing without any third person access data without data owner permission data user can't do anything in that iot data like read data edit and upload block auth, which utilizes blockchain to provide a secure and reliable authentication mechanic in Edge and IoT environments. Each edge device functions as a node within a blockchain network.

Blockchain technology As Edge IoT devices often communicate over untrusted networks, decentralized blockchain authentication ensures that devices can verify each other's authenticity and integrity without relying on centralized authorities Blockchain-based decentralized authentication provides scalability since

each device (or node) can independently verify identities and authenticate devices without burdening a central server. breaching multiple devices in different locations, which raises the difficulty of executing successful large-scale attack. The integration of blockchain-based decentralized authentication in Edge-IoT environments significantly enhances system security and trustworthiness by eliminating reliance on centralized authorities. It aims to address issues of complexity and storage overhead in existing blockchain-based IoT systems, enhancing security and efficiency in device communications.

Data owner like, (admin) for an organization in that data user will request key to data owner to access the iot data which data owner will generate key to user in that authentication user login process that decentralized blockchain-based distributed IoT architecture to enhance service security and efficiency. (fig: 4.2) It addresses vulnerabilities in traditional authentication methods that rely heavily on trusted third parties, aiming to mitigate risks associated with external attacks and internal spoofing. This technology for device authentication within edge computing environments. It highlights the limitations of classical cryptographic algorithms in handling the unique challenges posed by edge-connected IoT devices network for secure communication among IoT-enabled edge devices. points of vulnerability by distributing authentication data across a blockchain network. This distributed ledger ensures that identity records are immutable and transparent, making it extremely difficult for attackers to alter or forge credential.

Fig 4.1 Upload files to generate key

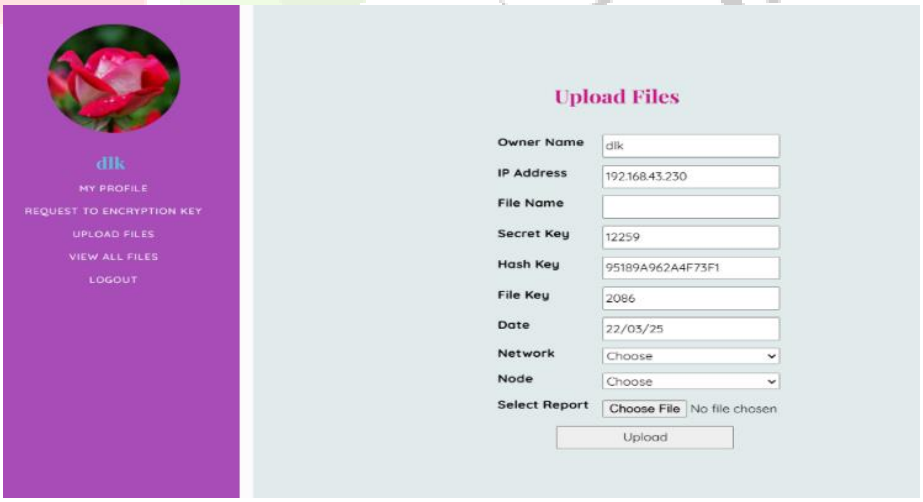

Fig 4.2 app password

V. ACKNOWLEDGEMENT

I would like to express our sincere gratitude to all those who contributed to the successful completion of this research work.

First and foremost, we extend our heartfelt thanks to Dr. M.G.R. Educational and Research Institute, Chennai, for providing us with the necessary infrastructure and academic environment to carry out this project.

I deeply thankful to Mr RAMESH E R, Assistant Professor, Center of Excellence in Digital Forensics, Chennai, India, for her invaluable guidance, continuous support, and insightful feedback throughout the research. Her expertise and mentorship were instrumental in shaping the direction and quality of this work.

I also extend our appreciation to our colleagues and peers who provided constructive suggestions and moral support throughout this journey. Special thanks to the faculty of the Department of Computer Science Engineering for their encouragement and academic assistance.

VI. CONCLUSIONS AND FUTURE SCOPE

The Decentralized Blockchain Authentication for Edge-IoT (DBAEI) system represents a significant step forward in enhancing the security, reliability, and scalability of Internet of Things (IoT) systems deployed at the edge of networks. With the rapid growth of IoT devices and the increasing complexity of edge computing environments, traditional centralized models for authentication and security are becoming inadequate. The model leverages the unique strengths of blockchain technology and decentralization to overcome these limitations, providing a robust framework for secure authentication in distributed IoT ecosystems. distributing authentication processes across a secure and immutable ledger, DBAEI ensures trustworthy device identity management, enhances data integrity, and mitigates risks associated with single points of failure. While challenges remain in terms of performance, interoperability, and energy efficiency, the benefits of improved security, privacy, and trust position DBAEI as a forward-thinking solution for the next generation of IoT systems.

In the future scopes of this paper Scalability to Support Massive IoT Networks: As IoT ecosystems continue to grow exponentially, the need for scalable, secure authentication mechanisms becomes critical. The proposed DBAEI system can be further enhanced to support millions of edge devices while maintaining decentralized trust and low latency. Integration with Anomaly Detection: Future iterations of DBAEI can incorporate artificial intelligence and machine learning algorithms to detect unusual patterns or behaviors in authentication requests, adding an additional layer of intelligent security.

VII. REFERENCES

[1] Edge Computing: Vision and Challenges, Weisong Shi; Jie Cao; Quan Zhang; Youhuizi Li; Lanyu Xu, IEEE Internet of Things Journal (Volume: 3, Issue: 5, October 2016), DOI: 10.1109/JIOT.2016.2579198

[2] [2] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops*

[3] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303.DOI**:** 10.1109/ACCESS.2016.2566339

[4] Mollah, M. B., Zhao, J., & Niyato, D. (2019**).** Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal*, 6(5), 8050–8073. DOI**:** 10.1109/JIOT.2020.2993601

[5] Chien, H.-Y., & Tsai, J.-L. (2020). A secure and efficient authentication protocol for edge computing based on blockchain. *IEEE Internet of Things Journal*, 7(6), 5062–5072., https://doi.org/10.1016/j.jnca.2020.102710

[6] Nguyen, T.-D., & Al-Saffar, A. (2020). A secure edge and sidechain-based authentication scheme for IoT environments. *IEEE Internet of Things Journal*, 7(10), 9562–9573.

[7] Blockchain-Based Edge Computing Resource Allocation in IoT: A Deep Reinforcement Learning ApproachYing He; Yuhang Wang; Chao Qiu; Qiuzhen Lin; Jianqiang Li; Zhong Ming DOI: 10.1109/JIOT.2020.3035437

[8] Security and Privacy for Cloud-Based IoT: Challenges Jun Zhou; Zhenfu Cao; Xiaolei Dong; Athanasios V. Vasilakos IEEE Communications Magazine (Volume: 55, Issue: 1, January 2017)

[9] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411.

[10] Abubakar, M. A. Blockchain-based Authentication and Access Control Mechanism for Internet of Things (IoT). (Thesis). Edinburgh NapierUniversity. http://researchrepository.napier.ac.uk/Output/3406748,https://doi.org/10.17869/enu.2023.3406748

[11] A Trust-Security-Resource Optimization Framework for Cloud-Edge-IoT Collaboration in Industrial Applications, Volume 16, Issue 1, January-March 2025, https://doi.org/10.71097/IJSAT.v16.i1.1626