IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

PRESERVING THE INTEGRITY OF IOTDATA IN THE CLOUD USING BLOCKCHAIN

[1]CHANDAN KUMAR, [2]DHANANJAY KUMAR, [3]GOLU KUMAR,[4] MRS. P. SHOBANA, [5]DR. J. JAYAPRAKASH

[6]DR. G. VICTO SUDHA GEORGE

[1,2,3]CSE Students, [4,5,6]Faculty, Dept of Computer science and Engineering,

DR. M.G.R EDUCATIONAL AND RESEARCH INSTITUTE, Maduravoyal,

Chennai-95, Tamil Nadu, India

Abstract: Safeguarding privacy and maintaining data integrity are paramount necessities for any internet- based platform, particularly those reliant on cloudinfrastructure. Blockchain technology has emerged asa pivotal force in fortifying cloud-based platforms. Inour proposed endeavour, we harness the power of blockchain to provide encryption for cloud-based IoToutcomes. This technology has rapidly evolved into apromising asset for integrating with cloud clusters, amplifying transaction security, and facilitating seamless access to critical data and application codes.Our paramount goal is to utilise blockchain's capabilities to encrypt vast and diverse datasets, ensuring their protection and integrity across diverse sources. Moreover, advancements in hash functions, exemplified by SHA512, have significantly bolstereddata security. The adoption of SHA512, distinguished for its resilience against brute force attacks due to theformidable computational demands it imposes on potential adversaries, reinforces our commitment to robust data protection. Consequently, we haveincorporated a modified SHA512 variant into our proposed framework to augment reliability and fortify data defences.

Keyword: Blockchain, IOT, SHA-512, MQTT

I. INTRODUCTION

IOT bias are using in every places now a days, i.e. healthcare, smart water, smart watch, motorcars and so on, etc. The Internet of effects is used in a variety of ways to optimise manufacturing processes and to help diligence borrow information technology. By the conclusion of 2021, Juniper Research predicts that staggering46 billion bias will be seamlessly connectedwithin the extensive network of the Internet of effects(IoT). Despite the tremendous eventuality of IoT technologies, there's still one issue that has yet to be completely resolved how to guaranteethe delicacy and trustability of the data collected from these technologies. Unfortunately, the data transferred by numerous IoT bias can fluently be interdicted and manipulated. Generally, IoT bias are more susceptible to attacks due to their limited information processing, storehouse and networking capabilities(Jyoti, 2017; Amar Sinh). Different designs, different interfaces or different surroundings are considered necessary for secure communication. One of the biggest challenges, as stressed by Alfonso,(2018) is icing the security of data coming from IoT bias, especially within infrastructures where bias shoot data to central waiters to store and reuse data. According to Dikilitas etal.(2021), blockchain emerges as a feasible result to address the security challenges current in IoT systems.One of the biggest challenges, as stressed by Alfonso,(2018) is icing the security of data coming from IoT bias, especially within infrastructures where bias shootdata to central waiters to store and reuse data. Blockchain is erected on a network of connected blocksthat act as a hedge to manipulation, guarding dataintegrity and security. According to Rui et al. (2019), using blockchain for decentralization ensures security and privacy. Blockchain tech offers robust features likestrong security, privacy, verification, and deviceauthorization for recording data. This makes it valuablefor strengthening systems dependent on IoT data. Researchers disagree on the best way to move data from IoT bais to a blockchain securely. Our study is driven by the idea that combining IoT and blockchain can safely facilitate this data transfer.

II. LITERATURE SURVEY

The Internet of Things (IoT) has become a focal pointin contemporary research, with researchers delving into its future implications. Despite significant stridesin IoT development, the technology remains vulnerable to various threats, leading to numerous attacks even before commercial implementation. Thisstudy explores IoT attacks, categorizes them, and proposes countermeasures, providing a comprehensive survey of IoT system vulnerabilities and the damage they cause [2].

Blockchain emerges as a promising solution to address IoT security concerns due to its foundationalprinciple of 'security by design.' By leveraging features like immutability and transparency, blockchain can mitigate architectural shortcomings inIoT systems. This article presents a survey on integrating blockchain and IoT, analyzing currentresearch trends and potential solutions [3].

Blockchain, a secure digital ledger, is gaining popularity for its ability to ensure anonymity,privacy, and data integrity without centralized control. This report delves into emerging research areas and offers recommendations for future studies,highlighting the expanding influence of blockchain beyond Bitcoin [4].

The goal of the Internet of Things is to connect the physical and digital worlds by collecting data and translating it into actionable commands. To address the heterogeneity of IoT platforms, this studyintroduces an IoT reference architecture rooted in multiple cutting-edge platforms, facilitating understanding, comparison, and evaluation [6].

Selecting a messaging protocol is crucial for IoTapplications, but it poses challenges due to the diverse needs of IoT systems. In this paper, we'll be lookingat four well-known protocols: MQTT (MQTT-T),CoAP (CoAP-T), AMQP (MQP-T), and HTTP (HTTP)—comprehensively, aiding users in selectingthe most suitable protocol based on their requirements [7].

III. OBJECTIVE

- The project's goal is to showcase the real- world application of blockchain technology in cloudservices, creating a secure, decentralised, and tamper-proof ecosystem for storing and retrievingIoT data.
- Blockchain technology is harnessed in thisproject to establish decentralisation by distributing IoT data across multiple nodes and ensuring data integrity through unique hash codesfor each transaction.
- SHA-512, part of the SHA-2 group of cryptographic hash functions, produces a 512-bit(64-byte) hash result from input data, known forits strong security and resistance to cryptographic attacks.

IV. EXISTING SYSTEM

Traditional methods for securing IoT data heavily rely on data encryption, which, while effective, falls short inthe IoT context due to centralization vulnerabilities andlimited privacy measures. These shortcomings can leadto single points of failure and unauthorised access, while also risking undetected data alterations and undermining the integrity of IoT data. "Disadvantages of Existing Systems" Even after making sure IoT systemsare safe and protected, poses challenges because of inherent constraints in IoT devices, including Withrestricted battery life, abilities for processing, and storage space. Additionally, there are security concernsregarding integrity, accountability, authentication, confidentiality, authorization, and availability. Efficient Automation: Smart contracts streamline processing, reducing time and costs.

V. PROPOSED SYSTEM

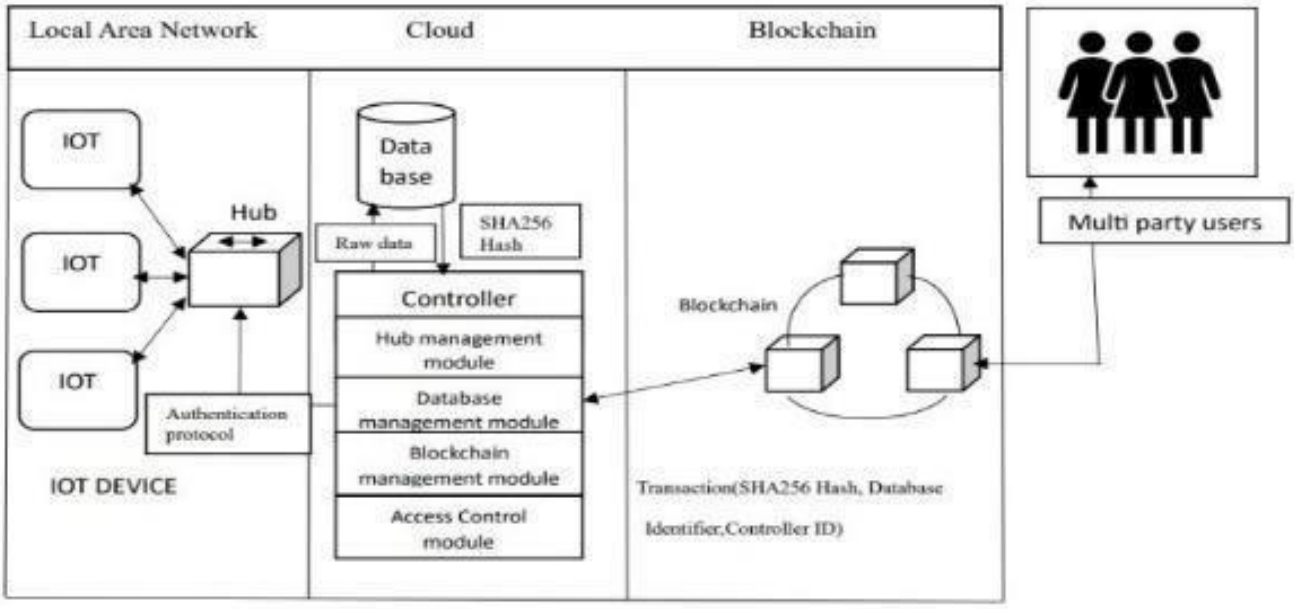
To address the shortcomings of traditional methods, this project introduces an inventive approach that makes full use of blockchain technology's built-infeatures to tackle these challenges comprehensively. Blockchain is a form of digital ledger technology that operates in a distributed and decentralized manner. It records transactions across multiple computers to ensure the security, immutability, and transparency ofstored data. It operates like a chain of connected blocks, where each block holds a list of transactions. Once a block joins the chain, altering the data it holdsbecomes highly challenging, providing a tamper-proof record of information. Successful implementation of adecentralised system using blockchain, where IoT datais distributed across multiple nodes.

A demonstration of the tamper-proof nature ofblockchain showcases how once data is added to the ledger, it becomes resistant to unauthorised alterations.

Successful integration of the SHA-512cryptographic hash function for securing IoT data. Verification of data integrity occurs through the generation and comparison of SHA-512 hash codes for each transaction. blockchain network Establishment of secure storage mechanisms within the blockchain, ensuring that only authorised devices can submit and access. "Advantages of the Proposed System" In this, we harness Ethereum's robust smart contract capabilities within the blockchain to enhance IoTdata security, privacy, and integrity. This includes implementing decentralised access control andauthentication for users.

System Requirements: The system requirements include a Windows operating system, an Intel Core i5processor or higher, a minimum of 8GB of RAM, andat least 25GB of available storage on the local drive.Software we used was Node.js of version12.3.1,python's IDLE of version python 3.7 and community version of Visual Studio.

VI. SYSTEM ARCHITECTURE



VII. MODULE

Simulation Application: This application simulates IoT data collection, as shown in Fig. 1,specifically generating random temperature readings as a representation of data from IoT sensors. The generated temperature values are then securely storedwithin the blockchain system. Each simulated temperature reading, along with its associated time stamp and SHA512 hash code, is recorded in the blockchain, demonstrating how IoT data can be securely stored and verified for integrity.

Flask Service Web Application: This web- based application is built using Flask and a server,as shownin Fig. 2. The user interface for interacting with the IoT data stored in the blockchain.

New User Signup: Users can register, as shown in Fig. 3, for an account within the Simulation Application, enabling them to access and utilise the IoT data simulation features.

User Login: After registration, as shown in Fig. 4, users can log in to the simulation application using their credentials.

Access Block Chain IOT: This allows users to select, as shown in Fig. 5, and view IoT simulation temperature data securely stored in the blockchain. This feature provides a user-friendly interface foraccessing and verifying the data, ensuring data integrity and security.

VIII. RESULT AND DISCUSSION

Blockchain as a Security Solution: Discussion on how blockchain technology addresses the security challenges inherent in IoT, providing a decentralised and tamper-proof environment.

Role of SHA-512 in Data Integrity: An Analysis of theRole Played by the SHA-512 Cryptographic HashFunction in Enhancing Data Integrity.

Comparison with other hash functions and discussionon why SHA-512 was chosen for its robustness.

Challenges and Considerations: Discussion onchallenges encountered during the integration of IoT and blockchain, including issues related to processingpower, storage, and network limitations of IoT devices.

Consideration of potential solutions and recommendations for overcoming these challenges.

Practical Implications and Use Cases: Exploration of practical implications for industries adopting this secure IoT and blockchain integration.

Identification of specific use cases and scenarios where this solution can be beneficial.

Future Directions and Research Opportunities: Proposingavenues for future research in securely transferring data from IoT devices to blockchain, considering emerging technologies and advancements Discussion on potential improvements and optimisationsfor the proposed system.

IX. IMPLEMENTATION

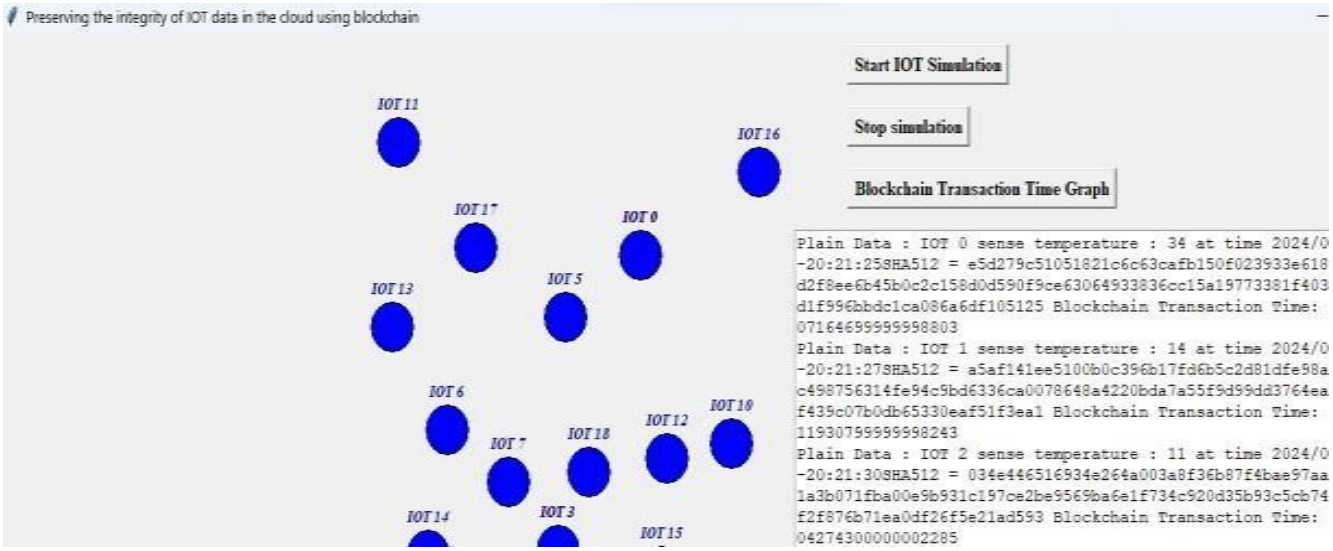


Fig.1.IOT Simulation

Fig.2.Flask server

Fig.3.User signup

Fig.4User login

Fig.5.Access IOT data

IOT ID	Sense Temperature	Sense Time	SHA512 Hashcode
1	14	2024/02/13-20:21:27	a5af141ee5100b0c396b17fd6b5c2d81dfe98a9c97c498756314fe94c9bd6336ca0078648a4220bda7a55f9d99dd3764ea0b1df439c07b0db65330eaf51f3ea1

Fig.6.SHA-512

CONCLUSION

The implementation of blockchain technology in this work bolstered the security and integrity of IoT data stored in the cloud. Blockchain implementation decentralises data storage, mitigating the risksassociated with centralised systems. This work prioritises user access authentication, ensuring that onlyauthorised individuals can interact with IoT data. This work showcases the practical implementation of blockchain within cloud services, providing a foundation for future innovations in securing sensitive data.

REFERENCE

[1] Internet of Things' Connected Devices to Triple by 2021, Reaching Over 46 Billion Units, https://www.juniperresearch.com/press/inter net- of- thingsconnected-devices-triple-2021, last accessed 2021/08/10.

[2] Jyoti D. and Amarsinh V.: Security Attacksin IoT: A Survey (2017).

[3] Alfonso P.: Blockchain and IoT Integration: A Systematic Survey. Sensors, 1424-8220 (2018).

[4] Dikilitas Y., Toka K.O. and Sayar A..: Current Research Areas in Blockchain. European Journal of Science and Technology,

26, pp. 488–492 (2021).

[5] Rui Z., Rui X. and Ling Liu.: Security andPrivacyon Blockchain (2019).

[6] Jasmin G.: Comparison of IoT platform architectures:A field study based on a reference architecture. 2016 Cloudification of the Internet of Things (CIoT), pp. 1–6(2016).

[7] Internet of Things' Connected Devices to Triple by 2021, Reaching Over 46 Billion Units, https://www.juniperresearch.com/press/inter net- of- thingsconnected-devices-triple-2021, last accessed 2021/08/10.

[8] Jyoti D. and Amarsinh V.: Security Attacksin IoT: A Survey (2017).

[9] Alfonso P.: Blockchain and IoT Integration: A Systematic Survey. Sensors, 1424-8220 (2018).

[10] Dikilitas Y., Toka K.O. and Sayar A..: Current Research Areas in Blockchain. European Journalof Science and Technology, 26, pp. 488–492 (2021).

[11] Rui Z., Rui X. and Ling Liu.: Security andPrivacy on Blockchain (2019).

[12] Jasmin G.: Comparison of IoT platform architectures: A field study based on a reference architecture. 2016 Cloudification of the Internet of Things (CIoT), pp. 1–6 (2016).

[13] Nitin N.: Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQPand HTTP. 2017 IEEE International Systems Engineering Symposium (ISSE), pp. 1–7 (2017).

[14] Nabil El I. and Claus P.: A Review of Distributed Ledger Technologies. OTM 2018 Conferences, Vol. 11230, Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, pp.277– 288 (2018).

[15] Gareth P. and Efstathios P.: Understanding Modern Banking Ledgers Through Blockchain Technologies. Future of Transaction Processing and Smart Contracts on the Internet of Money (2015).

[16] Nejc R.: Distributed logistics platform based onBlockchain and IoT. 52nd CIRP Conference on Manufacturing Systems (CMS), pp. 826–831 (2019).

[17] Thomas B.: Blockchains everywhere - a usecase of blockchains in the pharma supply-chain. 2017 IFIP/IEEE Symposium on Integrated Network and Service.

[18] Kristi´an K.: Management and Monitoring of IoT Devices Using Blockchain. Sensors 19.4, p. 856 (2019).

[19] Seyoung H., Sangrae C. and Soohyung K.: Managing IoT devices using blockchain platform.19thInternational Conference on AdvancedCommunication Technology (ICACT), pp. 464– 467 (2017).

[20] Mayra S., Uurtsaikh J. and Ralph D.: Blockchain as a Service for IoT. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp.433–436 (2016).