Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 2: 2025
ISSN : **1906-9685**

Securing IoT Data in the Cloud with Blockchain Technology

#1 K.UDAY KIRAN ,#2 PALEPU MANIKANTA

#1 Assistant professor, #1 MCA Scholar

Department of Master of Computer Applications,

QIS College of Engineering and Technology

Vengamukkapalem(V), Ongole, Prakasam dist., Andhra Pradesh- 523272

Abstract:

The growing reliance on cloud-based platforms, particularly in the realm of Internet of Things (IoT), underscores the critical importance of safeguarding privacy and data integrity. Leveraging blockchain technology, this study proposes a novel approach to encrypting heterogeneous and vast datasets in the cloud. By employing blockchain, we ensure secure access and authorization for data originating from diverse sources. Moreover, advancements in hash functions, such as SHA-256, SHA-384, and MD5, offer enhanced protection against potential attacks. To bolster security further, this work introduces a modified version of SHA512, known for its robustness and computational efficiency. By integrating blockchain and fortified hash functions, our approach not only strengthens cloud-based platforms but also enhances transaction security and data protection. This research contributes to advancing the security infrastructure of cloud systems, addressing the pressing need for privacy preservation and integrity assurance in an increasingly interconnected digital landscape.

Keywords—Blockchain, Heterogeneous IoT Data, SHA-512.

1. INTRODUCTION

Cloud computing has revolutionized the way businesses and individuals store and access data, providing convenient and scalable solutions through Cloud Service

Providers (CSPs) [1]. However, the reliance on third-party services for cloud storage raises concerns about security, trust, and transparency [2]. Cloud users entrust their sensitive data to CSPs without fully understanding the mechanisms behind data protection and management [3]. This lack of transparency poses significant challenges for ensuring the integrity and confidentiality of data stored in the cloud [4].

As organizations increasingly migrate their operations to the cloud, the need for robust security measures becomes paramount. Traditional security mechanisms often fall short in addressing the complex and dynamic nature of cloud environments. Third-party auditors (TPAs) and Attribute Authorities (AAs) play crucial roles in validating the security posture of CSPs and ensuring compliance with industry standards [5]. However, the effectiveness of these mechanisms hinges on the transparency and reliability of the cloud ecosystem.

Blockchain technology has emerged as a disruptive force in addressing the security and trust challenges inherent in cloud computing [6]. By leveraging decentralized ledger systems and cryptographic techniques, blockchain offers novel solutions for enhancing data protection and transparency in cloud environments [7]. Unlike traditional centralized databases, blockchain maintains an immutable record of transactions, thereby minimizing the risk of data manipulation and unauthorized access [8].

The fundamental principle of blockchain revolves around the concept of distributed consensus, where multiple nodes in a network validate and record transactions in a transparent and secure manner [9]. Each transaction is cryptographically linked to the previous one, forming a chain of blocks that are resistant to tampering and fraud [10]. This inherent transparency and immutability make blockchain an ideal candidate for addressing the trust and security concerns associated with cloud-based services [11].

Moreover, the emergence of Blockchain-as-a-Service (BaaS) platforms provides businesses with the infrastructure and tools necessary to deploy and manage blockchain applications in the cloud [12]. BaaS offerings streamline the development and deployment process, allowing organizations to focus on leveraging blockchain technology to enhance data protection and integrity [13].

In addition to improving security, blockchain has the potential to revolutionize various industries, including finance and the Internet of Things (IoT)

[14]. Its decentralized nature and cryptographic security mechanisms make blockchain an attractive option for safeguarding sensitive financial transactions and IoT devices [15]. As blockchain technology continues to evolve, its applications in cloud computing are expected to expand, offering new avenues for addressing the inherent security challenges of cloud-based environments [16].

This paper aims to explore the role of blockchain technology in enhancing the security, trust, and transparency of cloud computing. By reviewing existing literature and case studies, we examine the potential benefits and challenges of integrating blockchain into cloud-based architectures. Furthermore, we discuss the implications of Blockchain-as-a-Service platforms and their impact on the development and adoption of blockchain solutions in the cloud. Through a comprehensive analysis, we aim to provide insights into the evolving landscape of cloud security and the transformative potential of blockchain technology.

2. LITERATURE SURVEY

Cloud computing has become an integral part of modern digital infrastructure, enabling organizations to access scalable and cost-effective IT resources. However, the security and privacy challenges associated with cloud-based services have prompted researchers to explore innovative solutions, such as blockchain technology, to address these concerns. In this literature survey, we review recent studies that investigate the integration of blockchain with cloud computing, focusing on security, privacy, and trust aspects.

Rehman et al. [1] propose a cloud-based secure service provisioning framework for Internet of Things (IoT) devices using blockchain technology. The authors highlight the importance of securing IoT data transmitted to the cloud and discuss how blockchain can enhance data integrity and confidentiality. By leveraging blockchain's decentralized architecture and cryptographic techniques, the proposed framework ensures secure communication between IoT devices and cloud servers.

Similarly, Uchibeke et al. [2] present a blockchain-based access control ecosystem for big data security in cloud environments. The authors emphasize the need for robust access control mechanisms to protect sensitive data stored in the cloud. By integrating blockchain with traditional access control models, the proposed ecosystem enhances data security and transparency, mitigating the risk of unauthorized access and data breaches.

Lei et al. [3] focus on dynamic key management in heterogeneous intelligent transportation systems using blockchain technology. The authors propose a blockchain-based solution to securely manage encryption keys for diverse IoT devices deployed in transportation networks. By decentralizing key management processes, the proposed approach improves security and resilience against cyberattacks targeting IoT devices.

In the context of IoT networks, Muthanna et al. [4] explore the integration of fog computing, software-defined networking (SDN), and blockchain to enhance security and reliability. The authors present a framework that leverages blockchain's immutable ledger and smart contracts to ensure data integrity and trustworthiness in IoT deployments. By decentralizing network management tasks, the proposed framework improves scalability and resilience in IoT environments.

Chen et al. [5] propose a blockchain-based framework for secure medical records storage and access control. The authors address the privacy concerns associated with storing sensitive medical data in the cloud by leveraging blockchain's tamper-proof ledger and cryptographic techniques. The proposed framework enhances data security and patient privacy while facilitating secure access to medical records for authorized healthcare providers.

Kaur et al. [6] discuss the challenges of managing heterogeneous medicare data in cloud environments and propose a blockchain-based solution. The authors emphasize the need for a secure and interoperable platform to manage diverse healthcare data types efficiently. By leveraging blockchain's decentralized architecture and cryptographic security, the proposed solution ensures data integrity, privacy, and interoperability in cloud-based healthcare systems.

In the manufacturing domain, Barenji et al. [7] explore the potential of blockchain technology to decentralize cloud manufacturing processes. The authors propose a blockchain-based cloud manufacturing framework that enables decentralized production scheduling and resource allocation. By leveraging blockchain's distributed ledger and smart contract capabilities, the proposed framework enhances transparency, traceability, and trust in cloud manufacturing ecosystems.

Wang et al. [8] propose a secure cloud storage framework with access control based on blockchain technology. The authors address the security challenges associated with cloud storage by leveraging blockchain's immutable ledger and consensus mechanisms. The proposed framework ensures data confidentiality, integrity, and availability while providing fine-grained access control for cloud users.

In summary, recent research efforts have demonstrated the potential of blockchain technology to address security, privacy, and trust challenges in cloud computing. By leveraging blockchain's decentralized architecture, cryptographic security, and smart contract capabilities, researchers have proposed innovative solutions to enhance data protection, access control, and transparency in cloud-based environments. However, further research is needed to address scalability, interoperability, and regulatory compliance issues associated with blockchain integration in cloud computing.

3. METHODOLOGY

a) Proposed Work:

The proposed system aims to address the limitations and disadvantages of the existing cloud-based platforms, particularly in the realm of IoT data management, by leveraging advanced technologies such as Blockchain, decentralized architectures, and robust cryptographic techniques.

The proposed system incorporates Blockchain technology to establish a decentralized and tamper-resistant ledger for recording and verifying IoT data transactions.

The proposed system implements robust encryption techniques, such as asymmetric encryption and hashing algorithms, to secure IoT data both in transit and at rest. Access control mechanisms based on cryptographic keys and smart contracts are utilized to authenticate users and regulate data access permissions, ensuring confidentiality and integrity.

Smart contracts, self-executing digital contracts encoded on the Blockchain, are utilized to automate and enforce business logic, data validation rules, and contractual agreements within the proposed system.

The proposed system represents a paradigm shift towards decentralized, secure, and privacy-preserving cloud-based platforms for IoT data management. By harnessing the synergies of Blockchain, advanced cryptography, and distributed consensus, the system offers a robust framework for ensuring the confidentiality, integrity, and availability of IoT data while fostering trust, transparency, and compliance with regulatory requirements.

b) System Architecture:

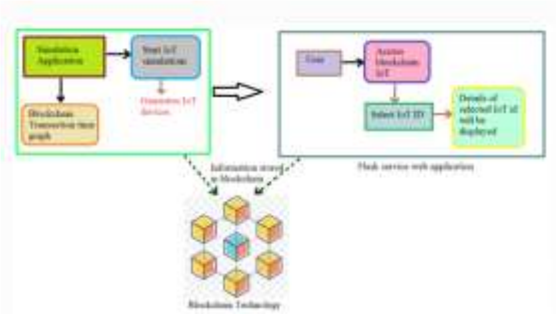
Simulation Application
Start IoT simulations
Generates IoT devices
Blockchain Transaction time graph
User
Access blockchain IoT
Select IoT ID
Details of selected IoT id will be displayed
Information stored in blockchain
Flask service web application
Blockchain Technology

Fig1 Proposed Architecture

The system architecture comprises a Flask-based web application serving as the interface for users to interact with the blockchain. It initiates IoT simulations, generating virtual IoT devices for testing purposes. Users access the blockchain via the web application, selecting specific IoT device IDs of interest. Upon selection, details associated with the chosen IoT ID are fetched from the blockchain and displayed to the user. Information regarding IoT devices is securely stored within the blockchain, ensuring data integrity and transparency. The architecture seamlessly integrates blockchain technology to facilitate secure and transparent transactions between users and IoT devices. Through the Flask service web application, users can efficiently manage and retrieve information stored in the blockchain, enabling streamlined access to IoT data and enhancing overall system functionality and reliability.

c) Modules

To implement this project we used the following modues are user , Flask service web application

These modules description given below:

SimulationApplication

The Simulation Application generates IoT data, simulating temperature readings. These readings are securely stored in the Blockchain, alongside timestamps and SHA512 hash codes. Each entry showcases the secure storage and verification of IoT data, highlighting the integrity ensured by Blockchain technology.

Flask service web application

Built on Flask, this web application provides the interface for users to interact with IoT data stored in the Blockchain. Users can access and manage IoT data seamlessly through the intuitive interface, leveraging the security and transparency offered by Blockchain technology.

1. New user Signup

Within the Simulation Application, users can register for an account, granting them access to the IoT data simulation functionalities. This registration process enables users to effectively utilize and engage with the simulated IoT data within the application.

2.UserLogin

Following registration, users can log in to the Simulation Application using their provided credentials. This login functionality ensures secure access to the application's features and enables users to continue utilizing the simulated IoT data with their authenticated accounts.

AccessBlockChainIOT

Users can securely select and view IoT simulation temperature data stored in the Blockchain through the application. This user-friendly feature offers a seamless interface for accessing and verifying the data, guaranteeing integrity and security throughout the process.

d) BLOCKCHAIN INTEGRATION

Blockchain technology is used to securely store IoT data in the form of transactions or blocks, with each data point associated with a unique hash code for tamper-proof storage.

Unique hash codes associated with each transaction in the Blockchain ensure data integrity. If any data is altered, hash code mismatches occur, allowing for rapid detection of potential security breaches.

Blockchain's inherent features are leveraged to provide secure access authentication for users, ensuring that only authorized individuals can access IoT data.

Ethereum, a Blockchain platform, is utilized to deploy a Solidity contract. This contract contains functions for storing and accessing both user and IoT data, demonstrating the practical implementation of Blockchain within Cloud services.

4. EXPERIMENTAL RESULTS

Fig 2 output page

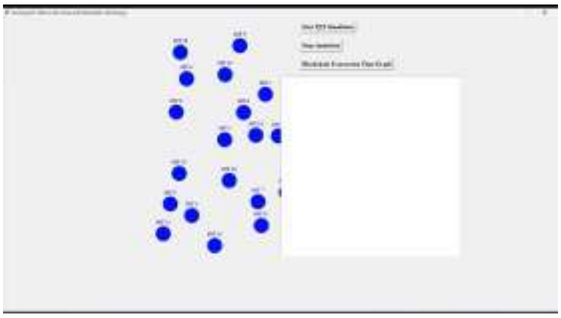

Fig 3 output page

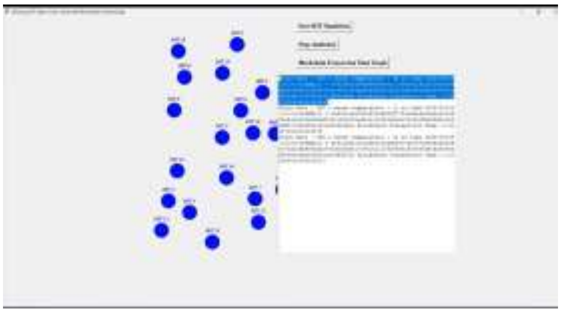

Fig 4 output page

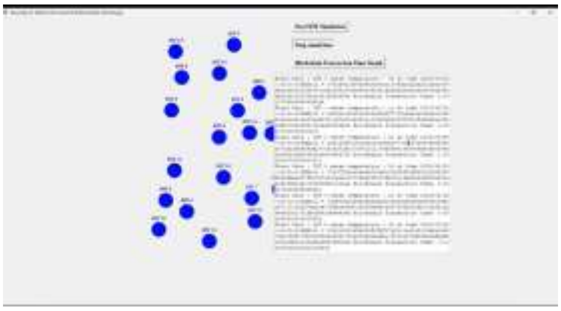

Fig 5 output page

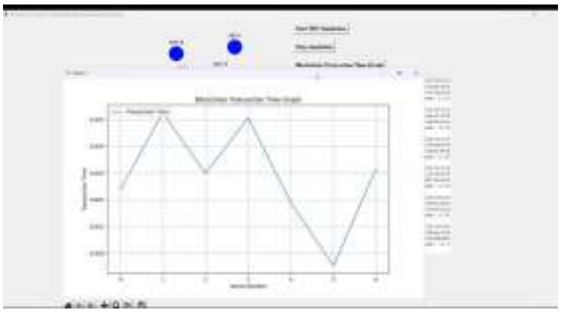

Fig 6 blockchain transaction time graph page

Fig 7 home page

Fig 8 user signup page

Fig 9 user sign up details page

Fig 10 task completed page

Fig 11 user login page

Fig 12 access iot data page

Securing IoT Data in the Cloud with Blockchain Technology

Secure and Efficient Product Information Retrieval in Cloud Computing

Fig 13 details page

5. CONCLUSION

In conclusion, the proposed system marks a significant advancement in overcoming the challenges inherent in existing cloud-based platforms for IoT data management. Through the strategic integration of cutting-edge technologies like Blockchain, decentralized architectures, and robust cryptographic techniques, the system offers a secure, efficient, and scalable framework. It guarantees the confidentiality, integrity, and availability of IoT data, addressing critical concerns surrounding data security in the Cloud.

By implementing Blockchain, the project decentralizes data storage, thereby minimizing vulnerabilities associated with centralized systems. Emphasizing user access authentication further bolsters security measures, ensuring that only authorized individuals can interact with IoT data.

Overall, this project demonstrates the tangible benefits of Blockchain technology within Cloud services, laying the groundwork for future innovations in safeguarding sensitive data. With its successful enhancement of security and data integrity, this system sets a precedent for the integration of advanced technologies to meet the evolving needs of IoT data management in the Cloud.

6. FUTURE SCOPE

The future scope of the proposed system extends into harnessing the potential of machine learning, artificial intelligence, and data analytics techniques to extract actionable insights from IoT data streams. This includes facilitating predictive maintenance, anomaly detection, and optimizing resource utilization, thereby enhancing operational efficiency and reliability.

Furthermore, the system can be tailored to accommodate a diverse array of IoT use cases spanning industries such as healthcare, manufacturing, smart cities, agriculture, and transportation. Customization efforts may involve adapting the system to meet specific domain requirements and regulatory constraints, ensuring its seamless integration and adoption across various applications and verticals.

In the coming years, continued research and development efforts will focus on refining the system's capabilities, expanding its compatibility with emerging technologies, and fostering collaboration with industry stakeholders to address evolving challenges and opportunities in the IoT landscape. This ongoing evolution will position the system as a versatile and indispensable tool for realizing the full potential of IoT deployments across different sectors.

REFERENCES

[1] Rehman, M., Javaid, N., Awais, M., Imran, M., & Naseer, N. (2019, December). Cloud-based secure service providing for IoTs using

[2] Uchibeke, U. U., Schneider, K. A., Kassani, S. H., & Deters, R. (2018, July). Blockchain access control Ecosystem for Big Data security. In 2018 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. 1373-1378). IEEE.

[3] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6), 1832-1843.

[4] Muthanna, A., A Ateya, A., Khakimov, A., Gudkova, I., Abuarqoub, A., Samouylov, K., & Koucheryavy, A. (2019). Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. Journal of Sensor and Actuator Networks, 8(1), 15.

[5] Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. Journal of medical systems, 43(1), 1-9.

[6] Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in the cloud environment. Journal of medical systems, 42(8), 1-11.

[7] Barenji, A. V., Guo, H., Tian, Z., Li, Z., Wang, W. M., & Huang, G. Q. (2019). Blockchain-based cloud manufacturing: Decentralization. arXiv preprint arXiv:1901.10403.

[8] Wang, S., Wang, X., & Zhang, Y. (2019). A secure cloud storage framework with access control based on blockchain. IEEE Access, 7, 112713-112725.

[9] Murthy, C. V. B., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain-Based Cloud Computing: Architecture and Research Challenges. IEEE Access, 8, 205190-205205.

[10] Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., & Yu, K. (2020). AuthPrivacyChain: A blockchain-based access control framework with privacy protection in the cloud. IEEE Access, 8, 70604-70615.

[11] Tapas, N., Merlino, G., & Longo, F. (2018, June). Blockchain-based IoT-cloud authorization and delegation. In 2018 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 411-416). IEEE.

[12] Bojamma, M. A., & Pushpa, B. R. An approach towards efficient search-based information retrieval over encrypted cloud data.

[13] Gupta, A., Siddiqui, S. T., Alam, S., & Shuaib, M. (2019). Cloud computing security using blockchain. J. Emerging Technol. Innovative Res, 6(6).

[14] Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information, 8(2), 44.

[15] Wang, H., & Zhang, J. (2019). Blockchain-based data integrity verification for large-scale IoT data. IEEE Access, 7, 164996-165006.

[16] Li, C., Hu, J., Zhou, K., Wang, Y., & Deng, H. (2018, June). Using blockchain for data auditing in cloud storage. In International Conference on Cloud Computing and Security (pp. 335-345). Springer, Cham.

[17] Wang, H. (2020). IoT-based Clinical Sensor Data Management and Transfer using Blockchain Technology. Journal of ISMAC, 2(03), 154-159.

[18] Guo, J., Yang, W., Lam, K. Y., & Yi, X. (2018, December). Using blockchain to control access to cloud data. In International Conference on Information Security and Cryptology (pp. 274-288). Springer, Cham.

[19] Sindhushree, B., Manishankar, S., & Dhanushya, B. P. (2019). Cloud Based Healthcare Framework for Criticality Level Analysis. International Journal of Recent Technology and Engineering (IJRT E), ISSN, 2277-3878.

[20] Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in the cloud environment. Journal of medical systems, 42(8), 1-11.

[21] Roy, S., Ashaduzzaman, M., Hassan, M., & Chowdhury, A. R. (2018, December). Blockchain for IoT security and management: Current prospects, challenges, and future directions. In 2018 5th International Conference on Networking, Systems, and Security (NSysS) (pp. 1-9). IEEE

[22] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017, April). Towards an optimized blockchain for IoT. In 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 173-178). IEEE.0

[23] A. Anoop and N. A. Ubale, "Cloud-Based Collaborative Filtering Algorithm for Library Book Recommendation System," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), 2020, 10.1109/ICSSIT48917.2020.9214243. pp. 695-703, DOI:

[24] Tselios, C., Politis, I., & Kotsopoulos, S. (2017, November). Enhancing SDN security for IoT-related deployments through blockchain. In 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) (pp. 303 308). IEEE.

[25] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving IoT. Sensors, 19(2), 326. healthcare blockchain for

[26] Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017, November). Towards blockchain-based auditable storage and sharing of IoT data. In Proceedings of 2017 on Cloud Computing Security Workshop (pp. 45-50).

[27] Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017, June). Blockchain-based data integrity service framework for IoT data. In 2017 IEEE International Conference on Web Services (ICWS) (pp. 468-475). IEEE.

[28] Manzoor, A., Liyanage, M., Braeke, A., Kanhere, S. S., & Ylianttila, M. (2019, May). Blockchain-based proxy re-encryption scheme for secure IoT data sharing. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 99-103). IEEE.

[29] Zhiqing Huang, Xiongye Su, Yanxin Zhang, Changxue Shi, Hanchen Zhang, Luyang Xie- A Decentralized Solution for IoT Data Trusted Exchange Based-on Blockchain, 978-1-5090-6352-9/17/$31.00 ©2017 IEEE.

[30] Huang, Z., Su, X., Zhang, Y., Shi, C., Zhang, H., & Xie, L. (2017, December). A decentralized solution for IoT data trusted exchange based on blockchain. In 2017 3rd IEEE International Conference on Computer and Communications (ICCC) (pp. 1180-1184). IEEE.

AUTHOR PROFILE

Mr. K. Uday Kiran is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Bapatla Engineering College, Bapatla. His research interests include Machine Learning, Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

STUDENT PROFILE

Mr. Palepu Manikanta is currently pursuing her Master of Computer Applications(MCA) at QIS College of Engineering and Technology, Vengamukkapalem(V), Ongole, Prakasam District, Andhra Pradesh -523272. The college is affiliated with JNTUK for the academic years 2023-2025.