Access Control for Mobile Crowdsensing using Blockchain

G Jyothi, Boddu Rishika, Sandha Sandhya Rani, Tukkapuram Sanjana

1 Assistant Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women

2.3.4 B,tech students, Department of *Information Technology, Bhoj Reddy Engineering College for Women*

ABSTRACT

Mobile Crowdsensing (MCS) has emerged as an effective paradigm for large-scale data collection using sensor-enabled mobile devices. However, conventional MCS systems rely on centralized architectures that assume complete trust among participants, resulting in critical challenges such as data security vulnerabilities, privacy breaches, unauthorized access, data leakage, and impersonation attacks. To address these limitations, this paper proposes a consortium blockchain-based access control framework that ensures secure and privacy-preserving data management in MCS environments.

The proposed framework adopts a hybrid architecture by integrating off-chain encrypted data storage with on-chain access control and auditing mechanisms. Sensitive user data is encrypted using Fernet symmetric encryption and stored in an off-chain database to maintain confidentiality. A Solidity-based smart contract deployed on a consortium blockchain manages user identities, data ownership, access permissions, and audit logs in a transparent and immutable manner. Additionally, a keyword-based indexed retrieval mechanism is introduced to enable efficient data search without revealing encrypted content.

The system allows users to request access to specific data, while data owners retain full control over permission approvals through blockchain-enforced policies. All transactions, including access requests and approvals, are recorded on-chain, ensuring traceability, accountability, and tamper-proof auditing. The framework is implemented using Flask for backend development, SQLite for off-chain storage, and Ganache to simulate the blockchain environment, demonstrating a practical prototype

Keywords: Mobile Crowdsensing (MCS), Consortium Blockchain, Access Control, Data Privacy, Smart Contracts, Fernet Encryption, Decentralized Systems, Secure Data Sharing, Auditability, Keyword-based Retrieval.

INTRODUCTION

Mobile Crowdsensing (MCS) has emerged as a transformative paradigm that utilizes sensor-enabled smartphones and IoT devices to collect large-scale, real-time data across various domains such as smart cities, healthcare, environmental monitoring, and traffic management. By leveraging the collective sensing capabilities of users, MCS enables cost-

effective and scalable data acquisition. However, despite its advantages, the rapid adoption of MCS systems has raised significant concerns related to data security, user privacy, and trust management.

Traditional MCS systems rely on centralized architectures where data collection and storage are managed by a single server. This approach assumes complete trust among stakeholders, which is often unrealistic in distributed environments. Such systems are vulnerable to risks including data leakage, identity exposure, unauthorized access, and malicious misuse, thereby discouraging user participation and limiting system reliability. Additionally, the absence of fine-grained access control and transparent auditing mechanisms further weakens accountability and trust.

To overcome these challenges, blockchain technology has been explored as a promising solution due to its decentralized, transparent, and tamper-resistant nature. Consortium blockchain, in particular, provides a controlled and collaborative environment suitable for MCS applications. However, limitations such as scalability and storage constraints necessitate a hybrid approach that combines blockchain-based access control with off-chain encrypted data storage, ensuring both security and efficiency in modern MCS systems.

OBJECTIVE

- To implement a **consortium blockchain-based access control mechanism** for decentralized data management.
- To ensure **data confidentiality** using encryption techniques for off-chain storage.
- To provide **fine-grained access control**, allowing data owners to manage permissions.
- To enable **transparent and tamper-proof auditing** of all data access activities.
- To improve **trust, security, and scalability** compared to traditional centralized MCS systems.

NEED FOR STUDY

The need for this study arises from the increasing security and privacy challenges in traditional Mobile Crowdsensing (MCS) systems. Existing centralized architectures are highly vulnerable to data breaches, unauthorized access, and malicious attacks, putting sensitive user information such as location, identity, and activity at risk. Moreover, these systems rely heavily on trusted servers, which may be compromised or misused, leading to a lack of trust among participants. Another major limitation is the absence of fine-grained access control, where users have limited authority over who can access their data. Additionally, the lack of transparent auditing mechanisms makes it difficult to track data usage and ensure accountability. Centralized systems also face scalability issues when handling large volumes of real-time data. Therefore, there is a critical need for a decentralized, secure, and efficient framework that ensures privacy

protection, controlled data sharing, transparency, and improved trust. This study addresses these challenges by proposing a blockchain-based solution that enhances security, eliminates single points of failure, and provides reliable data management in MCS environments.

EXISTING SYSTEM

The existing Mobile Crowdsensing (MCS) systems are primarily based on centralized architectures where a single server is responsible for collecting, storing, and managing user data. These systems lack robust security, privacy, and verification mechanisms, making them highly dependent on the trustworthiness of the central authority. Data management, access control, and user authentication are handled centrally, which increases the risk of vulnerabilities. Additionally, traditional systems do not implement strong cryptographic techniques or fine-grained access control policies, leading to inefficient and insecure data handling. As a result, these systems face challenges in ensuring data confidentiality, integrity, and trust among stakeholders.

DISADVANTAGES

- **Single Point of Failure:** Centralized architecture makes the system vulnerable to attacks or server failures, leading to data breaches and service disruption.
- **Lack of Fine-Grained Access Control:** Users and stakeholders are often given broad access permissions, increasing the risk of unauthorized data access and misuse.
- **Security and Privacy Risks:** Absence of strong encryption and verification mechanisms exposes sensitive data to leakage, impersonation attacks, and malicious activities.

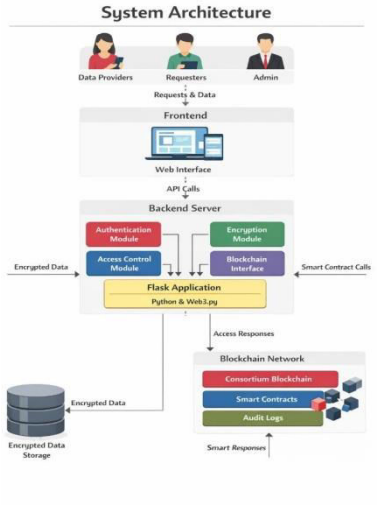
PROPOSES SYSTEM

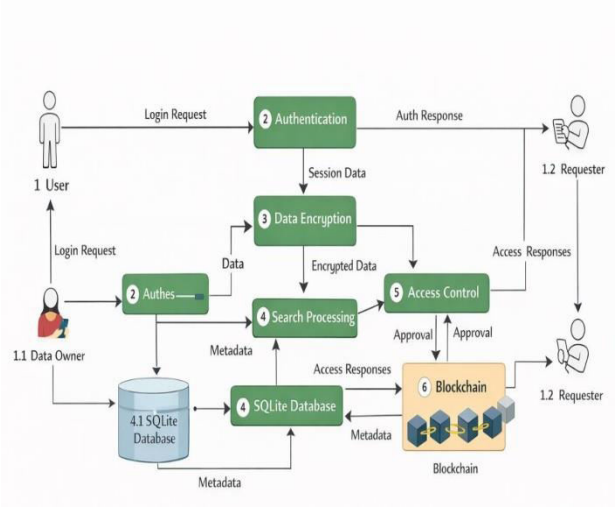
The proposed system uses a consortium blockchain-based framework for secure and decentralized Mobile Crowdsensing (MCS). It combines blockchain with off-chain encrypted storage, where sensitive data is protected using Fernet encryption and only metadata is stored on-chain. Smart contracts manage user identity, access control, and audit logs, ensuring secure and transparent data handling without relying on a central authority.

ADVANTAGES

- **High Security:** Tamper-proof blockchain with encrypted data storage
- **Decentralization:** No single point of failure
- **Data Privacy:** Sensitive data remains encrypted and secure
- **Access Control:** Data owners control permissions
- **Transparency:** All actions are recorded and auditable
- **Efficiency:** Reduced storage cost with hybrid architecture

SYSTEM ARCHITECTURE





technical Architecture

SYSTEM REQUIREMENTS

Software Requirements

Backend: Django

Frontend: HTML,CSS,JavaScript

Data base : SQLite

Editor: VisualStudioCode

HardwareRequirements

Processor:Anyprocessormorethani3

RAM:8 GB

HardDisk:512GB

Web cam : For facial recognition

MODULE DESCRIPTION

5.1 System Modules

1 AI & NLP Module
Uses AI and GPT to understand user queries and convert them into structured formats for better search accuracy.

2 NLU Module
Processes user input through tokenization, normalization, and keyword extraction to identify meaningful data.

3 Prompt Engineering Module
Refines and structures queries by removing unnecessary words and extracting core intent.

4 Keyword-Based Retrieval Module
Matches extracted keywords with stored data to retrieve relevant records while maintaining privacy.

5 Query Optimization Module
Improves search speed by removing

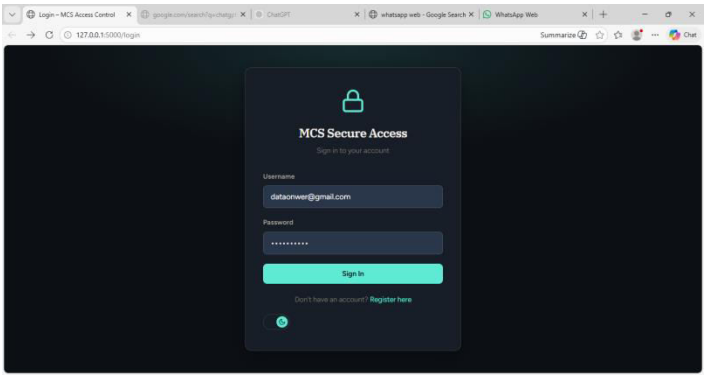
duplicates and using efficient database indexing.

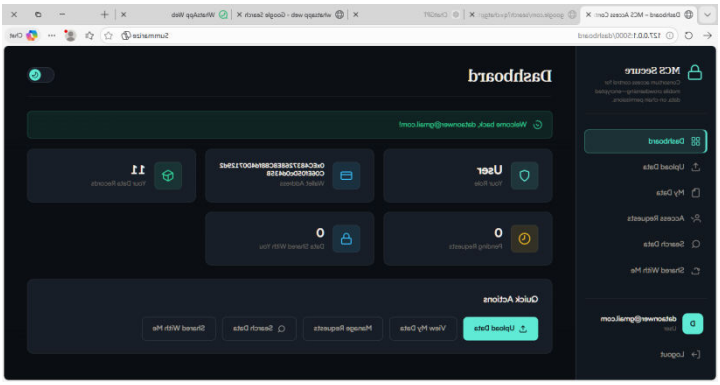
6 Blockchain Integration Module
Connects backend with blockchain using Web3.py for smart contract execution, access control, and audit logging.

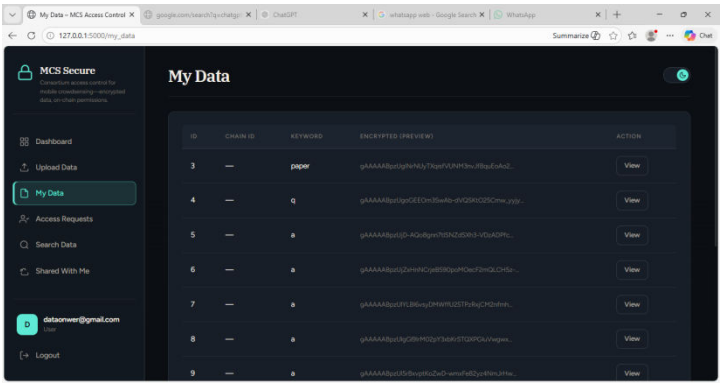
CHALLENGES&RISKS

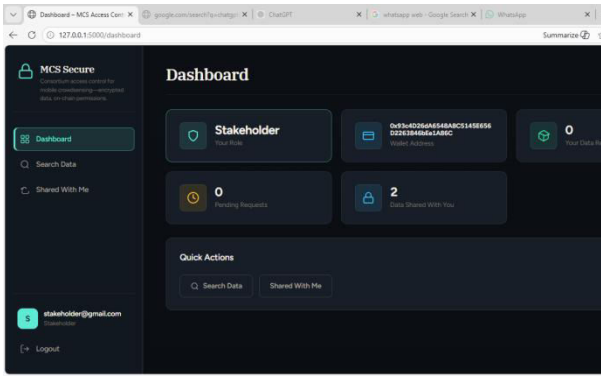
- . **Scalability Issues:** Blockchain networks may face performance limitations when handling large volumes of MCS data and frequent transactions.
- **Integration Complexity:** Combining blockchain with off-chain storage and encryption increases system design and implementation complexity.
- **Latency and Transaction Cost:** Blockchain operations (even in consortium setups) can introduce delays and computational overhead.
- **Key Management Risks:** Loss or compromise of encryption keys or wallet credentials can lead to permanent data loss or unauthorized access.
- **Security Vulnerabilities:** Smart contracts may contain bugs or vulnerabilities that can be exploited if not properly audited.
- **Data Availability Risk:** Off-chain storage failure or misconfiguration can affect access to encrypted data.
- **User Adoption Challenges:** Users may find blockchain-based systems difficult to understand and use.
- **Regulatory and Compliance Issues:** Handling sensitive user data must comply with data protection laws and regulations.
- **Consortium Trust Management:** Requires proper coordination and trust among participating organizations in the consortium network.

SCREEN SHOTS









Conclusion

This project presents a secure and privacy-preserving Mobile Crowdsensing (MCS) framework using a consortium blockchain-based access control mechanism. By integrating blockchain technology with off-chain encrypted storage, the system effectively addresses the limitations of traditional centralized approaches, including security vulnerabilities, lack of trust, and poor access control. The use of smart contracts ensures transparent, tamper-proof, and decentralized management of user identities, permissions, and audit logs.

The proposed solution enhances data confidentiality, ensures fine-grained access control, and improves trust among stakeholders while maintaining system efficiency through a hybrid architecture. Overall, the framework demonstrates that combining blockchain with encryption techniques provides a reliable, scalable, and practical approach for secure data sharing in modern MCS environments.

FUTURE ENHANCEMENT

- **AI Integration:** Incorporate machine learning algorithms for intelligent data analysis and anomaly detection.
- **Interoperability:** Enable integration with other blockchain networks and IoT platforms for wider applicability.
- **Advanced Encryption:** Use stronger cryptographic techniques like homomorphic encryption or differential privacy for enhanced data security.
- **Real-Time Processing:** Improve system performance to support real-time data access and decision-making.
- **User-Friendly Interface:** Develop intuitive UI/UX to increase user adoption and ease of use.
- **Cloud Integration:** Combine with cloud storage solutions for better availability and scalability.
- **Regulatory Compliance:** Enhance mechanisms to meet global data protection standards and legal requirements.
- **Scalability Improvement:** Implement advanced blockchain solutions such as sharding or Layer-2 techniques to handle large-scale MCS data efficiently.

REFERENCE

- Christin, D., Reinhardt, A., Kanhere, S. S., & Hollick, M., "A Survey on Privacy in Mobile Crowdsensing Applications," *IEEE Communications Surveys & Tutorials*, 2011.
- Ganti, R. K., Ye, F., & Lei, H., "Mobile Crowdsensing: Current State and Future Challenges," *IEEE Communications Magazine*, 2011.
- Li, M., Zhu, L., Lin, X., & Shen, X., "Efficient and Secure Data Sharing in Mobile Crowdsensing Systems," *IEEE Transactions on Vehicular Technology*, 2018.
- Dorri, A., Kanhere, S. S., & Jurdak, R., "Blockchain in Internet of Things: Challenges and Solutions," *IEEE Internet of Things Journal*, 2017.
- Zhang, Y., & Wen, J., "The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things," *Peer-to-Peer Networking and Applications*, 2017.
- Zyskind, G., Nathan, O., & Pentland, A., "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *IEEE Security and Privacy Workshops*, 2015.
- Wood, G., "Ethereum: A Secure Decentralized Generalized Transaction Ledger," Ethereum White Paper, 2014.
- Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
- Conti, M., Kumar, E. S., Lal, C., & Ruj, S., "A Survey on Security and Privacy Issues of Blockchain Technology," *IEEE Communications Surveys & Tutorials*, 2018.
- Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A., "MedRec: Using Blockchain for Medical Data Access and Permission Management," *IEEE Open & Big Data Conference*, 2016.