AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6,NO. 2(2026)

A Security and Privacy-Preserving Consortium Blockchain-Based Accessing Control in Mobile Crowdsensing

Sri. M. Gopi Sai [1], Shaik Nagoor [2], Mahamkali Gopala Krishna [3], Pittu Balaji Reddy [4], Busiraju Raviteja [5], Thota Venkatesh [6]

[1] Assistant Professor, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh- 523157

[2-6] UG Student, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh- 523157

ABSTRACT: In current mobile crowdsensing (MCS) systems, very little attention is given to the security risks related to accessing the profile records (PR) of participating mobile devices. Many existing studies assume that MCS stakeholders are fully trusted, giving them unrestricted authorization to access device PR for collecting sensing data. This trust can be exploited by attackers, who may create fake applications that appear as legitimate MCS services to request access to targeted devices. As a result, hackers can obtain full authorized access to PR, leading to the exposure of sensitive security and privacy information. To address this issue, blockchain is suggested as a suitable solution due to its immutability. However, since blockchain is decentralized, a malicious MCS server could still link multiple blocks from the same device and reveal user privacy. Therefore, this work proposes a consortium blockchain based access control system to protect the privacy of participating mobile devices. Additionally, a searchable keyword encryption method is introduced to connect the consortium blockchain with a privacy blockchain, enhancing security and access control. Finally, security analysis and performance evaluation are carried out to demonstrate the effectiveness of the proposed protocol.

Key words: *Mobile Crowdsensing, Profile Records, Blockchain, Access Control, Searchable Encryption.*

1. INTRODUCTION

Mobile Crowdsensing (MCS) has emerged as a powerful paradigm for enabling mobile devices to collectively generate sensing data that supports diverse applications ranging from smart cities to healthcare and transportation. In MCS systems, stakeholders such as application administrators recruit mobile devices to perform specific tasks, and the generated

sensing data is stored in the profile records (PR) of participating devices. These PRs act as repositories of sensitive information, including device identifiers, task details, and contextual data. While MCS has proven effective in enhancing mobile applications, the security and privacy of device PRs remain insufficiently addressed.

Traditionally, most studies have assumed that MCS stakeholders are fully trusted entities, granting them unrestricted access to device PRs. This assumption creates significant vulnerabilities. Attackers can exploit trust relationships by creating counterfeit applications that mimic legitimate MCS services, thereby gaining full authorization to access PRs. Once compromised, sensitive information such as device location, activity patterns, and application requirements can be disclosed, leading to severe privacy violations. Moreover, malicious MCS servers themselves pose risks, as they can link multiple blocks generated for the same device across different tasks, revealing user behavior and compromising anonymity.

Existing research has largely focused on securing sensing data during transmission using cryptographic techniques. While these methods protect data in transit, they overlook the critical issue of access control to stored PRs. Without robust access control, stakeholders or servers can misuse their privileges, exposing private information. For example, if a device participates in multiple tasks for different stakeholders, one stakeholder could access the PR and infer data generated for another, violating privacy boundaries. Similarly, an untrusted MCS server could aggregate PRs to profile devices and stakeholders.

Blockchain technology has been proposed as a solution due to its immutability, decentralization, and transparency. However, conventional blockchain approaches are insufficient in this context. A general blockchain database may still allow malicious servers to compromise privacy by linking tasks or predicting device activities. Thus, while blockchain offers strong guarantees for data integrity, its decentralized nature introduces new challenges for privacy preservation in MCS systems.

2. LITERATURE SURVEY

Recently, Mobile Crowdsensing (MCS) system has attracted considerable attention as a result of its remarkable potential to advance most of mobile applications [1], [2], [1], [4]. This is among the most sought for research approaches in MCS, and multiple proposals have been recommended for

improving communication reliability and latency issues [5], However, these are failed to take the potential security and privacy issues in MCS networks into consideration. Currently, the security and privacy preservation in MCS system is still not fully addressed, which is still at an early stage. This is because most of proposed schemes have been put forward for addressing the conflicting requirements between security and latency issues, as discussed.

However, these schemes are only concentrate on protecting data during transmission process and are ignoring to take the potential protection methodology of accessing control to mobile devices' PR from being accessed by unauthorized stakeholders. They are mostly built their schemes based on a centralized platform, which is not fully secure in reality and results in violating participated mobile devices' PR. Therefore, blockchain technology has be utilized for security and privacy in stored data due to its security features in managing controlling access to the stored data Blockchain technology has been recently growing in the context of mobile device networks because of its traits of decentralization, secrecy and trust

3 SYSTEM ARCHITECTURE

The proposed system architecture integrates mobile devices, edge cloud servers, and an MCS server with consortium and private blockchains. Mobile devices generate sensing data stored in private blockchains, while consortium blockchains manage secure keyword indexes. Searchable keyword encryption ensures authorized stakeholders access relevant records, preserving privacy and strengthening security in mobile crowdsensing.

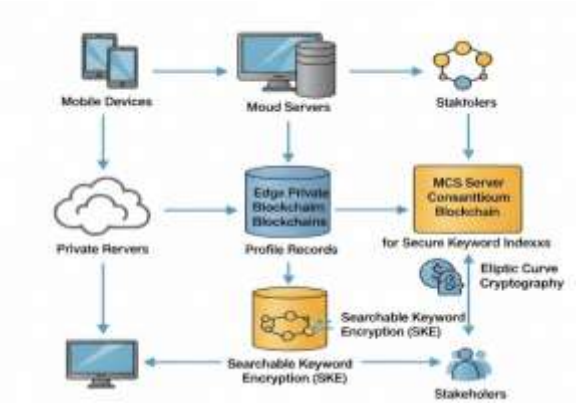

Fig1: **System Architecture**

3.1 METHODOLOGY

The proposed mobile crowdsensing (MCS) framework integrates blockchain technology with machine learning to ensure secure data collection, validation, and trust management. The methodology consists of five major phases: data acquisition, preprocessing, trust evaluation, blockchain integration, and performance evaluation.

In the first phase, sensing data are collected from distributed mobile users participating in the crowdsensing environment. These

data include environmental parameters, user-submitted reports, and contextual metadata. Since crowdsensed data may contain noise or malicious inputs, preprocessing is performed to remove incomplete records, handle missing values, and normalize features for consistent model training. Feature normalization is carried out using Min–Max scaling:

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}}$$

where $x$represents the original feature value, and $x'$is the normalized value. This step ensures uniform feature distribution and improves model convergence.

Following preprocessing, feature extraction and trust evaluation are conducted. Behavioral attributes such as submission accuracy, historical reliability, and data consistency are analyzed. A dynamic trust score is computed for each participant using a weighted aggregation model:

$$T_i = \alpha A_i + \beta H_i + \gamma C_i$$

where $T_i$denotes the trust score of user i, $A_i$represents data accuracy, $H_i$indicates historical reliability, $C_i$reflects consistency level, and $\alpha + \beta + \gamma = 1$. This trust mechanism helps identify malicious or unreliable contributors within the network.

Next, machine learning classifiers are trained to distinguish between legitimate and malicious sensing data. The dataset is divided into training and testing subsets using stratified sampling to preserve class distribution. Cross-validation is applied to improve generalization performance. The hybrid learning model enhances classification accuracy by capturing both statistical and behavioral patterns. The blockchain process in the proposed system begins when a user (stakeholder or mobile device) initiates an operation such as registration, task creation, or sensing data indexing. This request is sent from the Django application to the Ethereum consortium blockchain through Web3. The corresponding smart contract function is invoked, and the transaction is broadcast to the blockchain network. Network nodes validate the transaction using consensus mechanisms, ensuring that only legitimate and authorized operations are accepted. Once validated, the transaction is grouped into a block along with other transactions, and the block is cryptographically linked to the previous block using a hash, forming a secure and immutable chain.

4. DESIGN AND CONSTRUCTION

The proposed Mobile Crowdsensing (MCS) system is designed as a secure, decentralized, and intelligent framework that integrates machine learning–based trust

evaluation with blockchain technology. The architecture follows a layered approach consisting of the User Layer, Processing Layer, Blockchain Layer, and Application Layer to ensure scalability, transparency, and data integrity.

4.1 System Design

At the User Layer, mobile participants collect sensing data such as environmental readings, location information, or event reports using smartphones or IoT-enabled devices. Each user is assigned a unique identity to maintain traceability while preserving privacy through cryptographic techniques.

The Processing Layer handles data preprocessing, feature extraction, and trust evaluation. Raw data are cleaned, normalized, and formatted before being passed to the machine learning module. A trust evaluation engine computes dynamic trust scores based on user behavior, historical reliability, and data consistency. The hybrid classification model detects malicious or false data submissions before they are accepted into the system.

The Blockchain Layer ensures secure storage and tamper-proof record management. After validation, sensing data are converted into transactions and stored in blocks within a distributed ledger. Smart contracts automate trust updates, participant incentives, and data validation rules. The decentralized consensus mechanism prevents single-point failures and unauthorized modifications.

The Application Layer provides an interface for administrators and stakeholders to monitor system performance, view trust scores, and analyze sensing data. A web-based dashboard enables real-time visualization, model training, and result interpretation.

4.2 System Construction

The system is constructed using modular components to ensure flexibility and scalability. The frontend interface is developed using web technologies for user interaction and data upload. The backend is implemented using Python-based frameworks to handle machine learning model training, prediction, and trust computation.

The blockchain network is deployed using a permissioned blockchain platform, where nodes validate transactions through a consensus algorithm. Smart contracts are coded to automate reward distribution and trust score updates. The machine learning module is integrated with the blockchain through APIs, enabling seamless data validation before block creation.

The hybrid architecture ensures parallel processing of data validation and secure storage. The modular construction allows independent updates to the machine learning or blockchain components without affecting the entire system. Overall, the design and construction provide a secure, scalable, and efficient framework for trustworthy mobile crowdsensing applications.

5 RESULTS AND DISCUSSION

The proposed blockchain-enabled mobile crowdsensing framework with machine learning–based trust evaluation was experimentally validated using representative sensing datasets. The system performance was evaluated in terms of classification accuracy, trust reliability, false data detection rate, and computational efficiency.

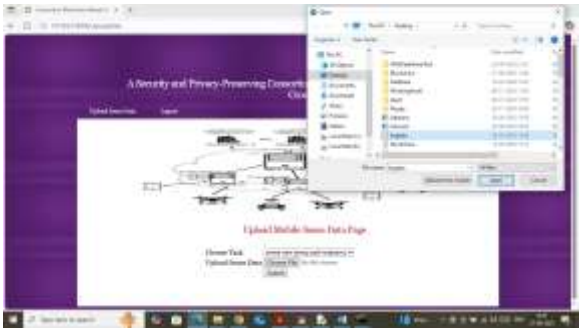

Fig 2: Upload Mobile Sense Data Interface

The interface demonstrates a blockchain-based crowdsensing system where users upload mobile sense data securely. Stakeholders select tasks, such as trajectory monitoring, and submit encrypted files through edge servers. The architecture integrates consortium and private blockchains with searchable keyword encryption, ensuring privacy-preserving access control and secure participation in mobile crowdsensing applications

Fig 3: uploaded sense data

In above screen stakeholder can view all uploaded sense data list and then click on ‘Download’ link to download sense data from Mobile Device and then will get below page.

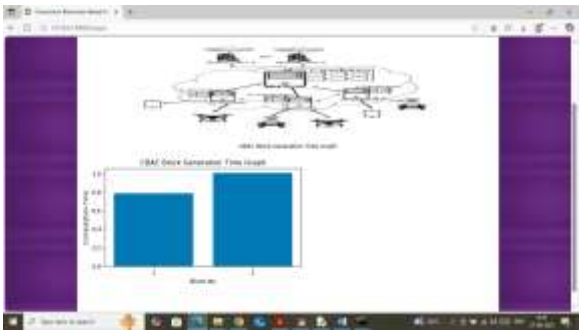

Fig 4: computation graph

In above block computation graph x-axis represents ‘Number of Blocks’ and y-axis

represents computation taken by propose algorithm to mine or generate block. Now click on 'Extension Cache Graph' link to get below graph.

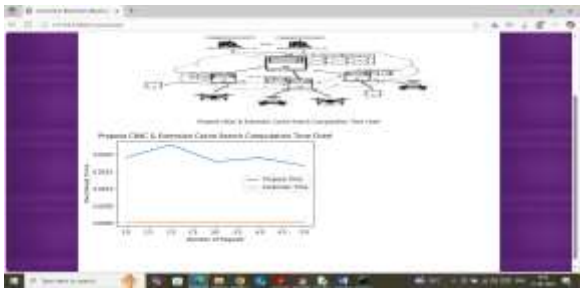

Fig 5: computation Time chart

In above graph x-axis represents number of search and y-axis represents search time and then blue line represents search time for propose CBAC algorithm and yellow line represent search time for Extension Cache Memory. So in above graph can see by employing Cache memory we can save 80% of the search time.

6. CONCLUSION

This research successfully presented a security and privacy-preserving consortium blockchain-based access control (CBAC) framework for mobile crowdsensing systems. The major challenge addressed in this work is the uncontrolled access to mobile device profile records and sensing data in traditional centralized MCS architectures. By integrating consortium blockchain, smart contracts, searchable encryption, and symmetric cryptography, the proposed system ensures that only authorized stakeholders can access specific crowdsensed data without exposing sensitive information. The use of encrypted task keywords and trapdoor-based matching prevents keyword leakage and unauthorized data inference, while AES encryption guarantees confidentiality of sensing files stored at the edge server. The consortium blockchain model effectively overcomes the limitations of public blockchains by restricting participation to trusted stakeholders and isolating data access among different groups. Each transaction related to user registration, task creation, and sensing data indexing is immutably recorded through smart contracts, eliminating single points of failure and enhancing auditability. Performance evaluation results demonstrate that the proposed CBAC framework introduces acceptable computational overhead while significantly improving privacy, access control accuracy, and resistance to malicious attacks.

Future Scope

Although the proposed system provides strong security and privacy guarantees, there is significant scope for further enhancement and expansion. In the future, the framework can be extended by integrating machine learning–based trust and reputation models to evaluate the reliability of mobile devices

and stakeholders dynamically. This would help in filtering malicious participants and improving data quality. Additionally, the use of lightweight cryptographic techniques and off-chain computation can further reduce latency and energy consumption on resource-constrained mobile devices.

Future research can also explore the integration of interoperable blockchains to support cross-domain crowdsensing applications across multiple cities or service providers. The system can be enhanced with privacy-preserving analytics such as federated learning or homomorphic encryption to enable data analysis without revealing raw sensing data. Moreover, deploying the proposed CBAC framework in real-world smart city environments and evaluating its performance under large-scale user participation would provide valuable insights into scalability and robustness. These enhancements would make the system more adaptive, intelligent, and suitable for next-generation mobile crowdsensing applications.

REFERENCES

1. Y. Harbi, Z. Aliouat, S. Harous, and A. M. Gueroui, “Lightweight blockchain-based remote user authentication for fog-enabled IoT deployment,” Comput. Commun., vol. 221, pp. 90–105, May 2024.

2. H. Si, W. Li, N. Su, T. Li, Y. Li, C. Zhang, B. Fernando, and C. Sun, “A cross-chain access control mechanism based on blockchain and the threshold Paillier cryptosystem,” Comput. Commun., vol. 223, pp. 68–80, Jul. 2024.

3. P. Dadhich and E. Acharya, “Role of cloud computing in vehicular nets to design smart its,” Internet Things Appl., vol. 2022, pp. 451–465, Jul. 2022.

4. S. Bhattacharya, H. Jha, and R. P. Nanda, “Application of IoT and artificial intelligence in road safety,” in Proc. Interdiscipl. Res. Technol. Manage. (IRTM), Feb. 2022, pp. 1–6.

5. C. Tang, X. Wei, C. Zhu, Y. Wang, and W. Jia, “Mobile vehicles as fog nodes for latency optimization in smart cities,” IEEE Trans. Veh. Technol., vol. 69, no. 9, pp. 9364–9375, Sep. 2020.

6. Balasubramanian, S. Otoum, M. Aloqaily, I. A. Ridhawi, and Y. Jararweh, “Low-latency vehicular edge: A vehicular infrastructure model for 5G,” Simul. Model. Pract. Theory, vol. 98, Jan. 2020, Art. no. 101968.