A Blockchain-Based Privacy-Preserving Quality Control Mechanism in Crowdsensing Applications

M.Anusha
Assistant Professor,
Dept of CSE(DS) , CMR Technical Campus
Hyderabad, Telangana,
India
anushamandadi76@gmail.com

Ms. N. Soujanya
Assistant Professor,
Dept of CSE(DS), CMR Technical Campus Hyderabad,
Telangana, India
noundlasoujanya516@gmail.com

N. Nandhini
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana,
India
naraboinanandhini@gmail.com

R. Bhavana
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
bhanuravuri02@gmail.com

P. Uharshini
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
pasupulauharshini05@gmail.com

Sai Vardhan
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
saivardhankonderu17@gmail.com

How to Cite this Article:
Soujanya, N., Nandhini, N., Bhavana, R., Uharshini, P. & Vardhan, S. (2026). A Blockchain-Based Privacy-Preserving Quality Control Mechanism in Crowdsensing Applications. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.308

https://doi.org/10.55041/ijcope.v2i4.308

ABSTRACT— Mobile Crowd Sensing (MCS) has emerged as a powerful paradigm for large-scale data collection using sensor-enabled smartphones. However, existing MCS systems suffer from significant challenges such as lack of data quality assurance, privacy leakage, reliance on centralized authorities, and vulnerability to malicious users providing false data for incentives. To address these issues, this paper proposes a Blockchain-based Privacy-Preserving Quality Control (PPQC) mechanism for crowdsensing applications.The proposed system integrates blockchain technology to eliminate the need for a trusted central authority, ensuring data integrity, transparency, and secure reward distribution. A decentralized framework is designed where miners evaluate the quality of sensing data instead of a centralized server. To preserve user privacy, a node cooperation mechanism achieving k-anonymity is employed, along with homomorphic encryption techniques that allow computations on encrypted data without revealing sensitive information.Furthermore, a quality-based incentive mechanism is implemented, where rewards are assigned based on the accuracy of contributed data using noise estimation. The system also incorporates secure transaction mechanisms to prevent impersonation and fraudulent activities. Experimental results and performance analysis demonstrate that the proposed PPQC framework significantly improves data reliability, privacy protection, and system efficiency compared to existing approaches.Overall, the proposed solution provides a scalable, secure, and privacy-aware crowdsensing model suitable for real-world applications such as traffic monitoring, environmental sensing, and smart city services.

INTRODUCTION

With the rapid growth of sensor-enabled smartphones, Mobile Crowd Sensing (MCS) has become
an effective approach for large-scale data collection in applications such as traffic monitoring, environmental sensing, and smart city services. In MCS, users contribute real-time data using their mobile devices, enabling efficient and low-cost sensing. However, the reliability of such systems depends heavily on the quality of user-contributed data. Participants consume device resources like battery, storage, and computation, and may also expose sensitive information such as location and time, leading to privacy concerns. Moreover, selfish or malicious users may submit false data to maximize rewards, thereby degrading system performance.To address these challenges, this paper proposes a **Blockchain-Based Privacy-Preserving Quality Control (PPQC) mechanism** for crowdsensing applications. The proposed approach leverages blockchain technology to eliminate centralized control, ensuring transparency, security, and tamper-proof data management. A decentralized validation process is introduced where miners evaluate data quality, and a quality-based incentive mechanism rewards users according to their contributions. Additionally, privacy-preserving techniques such as homomorphic encryption and node cooperation are employed to protect user data. The proposed system enhances data reliability, ensures fair reward distribution, and provides strong privacy protection, making it suitable for real-world MCS applications.

I. PROBLEM DEFINITION

Mobile Crowd Sensing (MCS) systems rely on user participation to collect large-scale sensing data; however, they face several critical challenges that limit their effectiveness and reliability. Existing systems are typically based on centralized architectures, where a third-party server is responsible for data collection, validation, and reward distribution. This centralized approach introduces issues such as lack of transparency, single point of failure, and vulnerability to data tampering. Moreover, users may submit low-quality or false data to gain incentives, and current systems often lack efficient mechanisms to accurately evaluate data quality and detect malicious behavior.

1.2 PROJECT FEATURES

The proposed Blockchain-Based Privacy-Preserving Quality Control (PPQC) system offers a decentralized and secure framework for mobile crowdsensing applications. By leveraging blockchain technology, the system eliminates the need for a central authority, ensuring transparency, trust, and tamper-proof data storage. It incorporates privacy-preserving techniques such as homomorphic encryption and node cooperation to protect sensitive user information, including location and identity. The system employs a quality-based incentive mechanism that rewards participants according to the accuracy of their contributed data, thereby encouraging honest participation and improving overall data reliability.

Related Work

Mobile Crowd Sensing (MCS) has attracted significant research attention, particularly in the areas of incentive mechanisms, data quality assurance, and privacy preservation. Early studies focused on reputation-based incentive mechanisms, where users are rewarded based on their historical performance. These approaches help identify unreliable participants but are vulnerable to attacks such as Sybil and whitewashing, which can degrade system trust. To overcome these limitations, monetary-based incentive schemes were introduced, where users are compensated based on their contributions. Although effective in motivating participation, these methods often rely on centralized authorities, leading to concerns related to transparency, fairness, and single points of failure**.**

II. METHODOLOGY

The proposed system follows a structured approach to ensure **privacy-preserving, secure, and quality-controlled data collection** in mobile crowdsensing environments using blockchain technology.

1. Network Generation

The system begins by generating a mobile crowdsensing network consisting of multiple participants (smartphone users) and a publisher. Each participant acts as a sensing node capable of collecting and transmitting real-time data such as location or environmental information.

2. Data Collection

Participants collect sensing data from their surroundings and prepare it for submission. The collected data typically includes parameters such as location coordinates and other relevant sensing information required by the publisher.

3. Model Training

Multiple techniques are applied to train the system for identifying truthful and malicious data, including:

- Noise-based Validation
- Threshold-based Classification
- Reward Learning Mechanism

The dataset is divided into:

- Training Data (80%)
- Testing Data (20%)

The system is trained using the training dataset to learn patterns between actual data and noisy data, enabling accurate data validation and reward assignment.

4. Model Evaluation

The performance of the proposed blockchain-based privacy-preserving quality control system is evaluated using the following metrics:

- Data validation accuracy
- Noise detection efficiency
- Reward distribution correctness
- Execution time

These metrics measure how effectively the system identifies truthful and malicious participants based on the calculated noise values.

5. Result Comparison

The performance of the proposed Blockchain-Based Privacy-Preserving Quality Control (PPQC) system is compared with existing methods to evaluate its effectiveness in terms of accuracy, security, and execution time.

6. Attack Prediction

The proposed system predicts attacks by analyzing the noise value between actual and received data. If the noise exceeds a predefined threshold, the data is classified as malicious, indicating a potential attack. Otherwise, it is considered truthful, ensuring secure and reliable data validation.

7. Output Generation

The system generates output including validated data, noise values, and rewards. These results are stored on the blockchain, ensuring security and transparency.

III. PROPOSED SYSTEM

In the proposed paper, to detect malicious or false data submissions (insider attacks), the system employs multiple validation techniques based on **noise-based verification and quality evaluation mechanisms**. The system analyzes the difference between actual and received data to identify abnormal patterns and classify data as truthful or malicious.The performance of the system is evaluated using metrics such as **accuracy, validation efficiency, execution time, and reward correctness**. Compared to traditional approaches, the proposed PPQC mechanism provides better reliability and security.

IV. IMPLEMENTATION DETAILS

The proposed Blockchain-Based Privacy-Preserving Quality Control (PPQC) system is implemented using Python with supporting libraries for simulation, encryption, and performance analysis. The system consists of modules such as network generation, data submission, privacy preservation, data validation, and reward management.A mobile crowdsensing environment is simulated where multiple participants generate and send sensing data to a publisher. Before transmission, the data is secured using homomorphic encryption to preserve user privacy. The system then performs **noise-based verification** to validate the quality of the received data. Based on the validation results, rewards are assigned to participants. For blockchain integration, **Ethereum smart contracts** are used to store validated data and manage transactions securely. The implementation also includes visualization of system performance through **running time graphs**, enabling comparison with existing approaches.

4.1 ALGORITHMS USED

4.1.1 HOMOMORPHIC ENCRYPTION

This algorithm is used to preserve user privacy by encrypting sensing data before transmission. It allows computations to be performed directly on encrypted data without revealing the original information. As a result, sensitive details such as user location and identity remain protected while still enabling data processing and validation.Additionally, it supports secure multi-party computation, ensuring that data can be shared and processed collaboratively without compromising confidentiality. This significantly enhances trust among participants in the system.

4.1.2 NOISE-BASED VALIDATION

This algorithm evaluates the quality of the received data by calculating the difference (noise) between actual and reported values. If the noise is within a predefined threshold, the data is considered truthful; otherwise, it is classified as malicious. This helps in detecting false data submissions effectively.It also improves system accuracy by filtering out low-quality or manipulated data before further processing. This ensures only reliable data contributes to final decision-making.

4.1.3 BLOCKCHAIN CONSENSUS MECHANISM

The blockchain consensus mechanism ensures decentralized and secure validation of data. Multiple nodes (miners) participate in verifying transactions, making the system resistant to tampering and eliminating the need for a central authority. This enhances transparency and trust in the system.It also provides fault tolerance, as the system continues to function even if some nodes fail or act maliciously. This makes the overall system more robust and dependable.

4.1.4 SMART CONTRACT

Smart contracts are used to automate the reward distribution process. Based on predefined conditions, such as data quality and validation results, rewards are assigned to participants. This ensures fairness, transparency, and eliminates manual intervention in transactions.They also ensure that all transactions are executed accurately and cannot be altered once deployed. This reduces the risk of fraud and increases system reliability.

4.1.5 THRESHOLD-BASED CLASSIFICATION

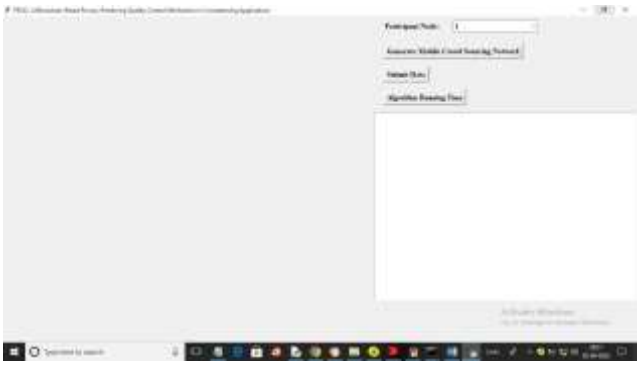
This algorithm classifies data into truthful or malicious categories based on a predefined noise threshold. It simplifies decision-making in the validation process and ensures that only high-quality data is accepted, improving overall system reliability.It is computationally efficient and easy to implement, making it suitable for real-time applications. This helps in maintaining system performance even with a large number of participants.

V. EXPERIMENTAL RESULTS AND DISCUSSION

The following results demonstrate the performance of the proposed system, highlighting its key functionalities and effectiveness. These outputs provide a clear understanding of how the system operates under different conditions, showcasing data validation, reward distribution, and overall system behavior. The results serve as supporting evidence of the system's

efficiency, accuracy, and reliability in ensuring secure and privacy-preserving crowdsensing.

System Interface – Home Page:



To run project double, click on run.bat file to get below screen

In above screen click on 'Generate Mobile Crowd Sourcing Network' button to generate mobile sensing users and get below page.

Fig. 1. User Registration and Login Module

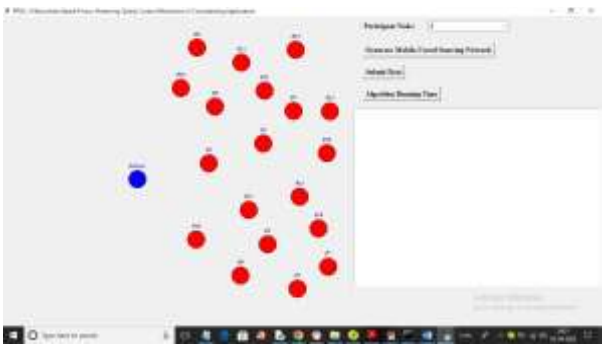


Fig. 2. Data Submission and Encryption Process

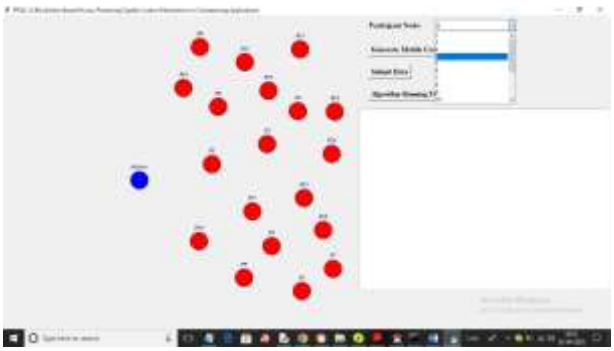


Fig. 3. Data Validation and Noise Calculation

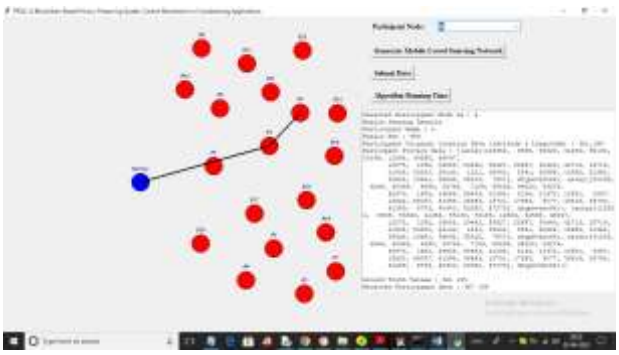
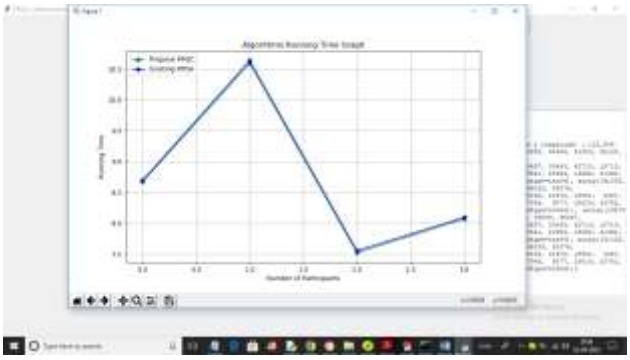


Fig. 4. Performance Analysis (Running Time Graph)



In above graph x-axis represents number of participants and y-axis represents running time in seconds. Blue line represents existing PPDA and green line represents propose PPQC which is taking less execution time

VI. CONCLUSION

The proposed **Blockchain-Based Privacy-Preserving Quality Control (PPQC)** system effectively addresses the challenges of data reliability and user privacy in mobile crowdsensing. By integrating blockchain technology with noise-based validation, the system ensures secure, transparent, and tamper-proof data management. The use of privacy-preserving techniques protects sensitive user information, while the validation mechanism accurately distinguishes between truthful and malicious data.

VII. FUTURE SCOPE

The proposed system can be further enhanced by integrating advanced **machine learning algorithms** such as deep learning models to improve the accuracy of malicious data detection. Additionally, optimizing blockchain mechanisms can help reduce **transaction cost and latency**, making the system more efficient for large-scale applications.

Future work may also focus on implementing the system in real-time environments with a large number of participants and extending it to support **IoT-based applications**. Enhancing privacy techniques and developing more robust reward mechanisms can further improve user trust, scalability, and overall system performance. Finally, future work can explore the development of a **user-friendly interface and mobile application**, along with cross-platform compatibility

VIII.ACKNOWLEDGMENT

We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project, we take this opportunity to express our profound gratitude and deep regard to our guide **M. Anusha**, Designation for his/her exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by him/her shall carry us a long way in the journey of life on which we are about to embark.

We also take this opportunity to express a deep sense of gratitude to the Project Review Committee (PRC) coordinators **N. Soujanya, Shafana Bakshi,** for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. K. Murali**, Head, Department of Computer Science and Engineering (Data Science) for providing encouragement and support for completing this project successfully.

We are deeply grateful to **Dr. A. Raji Reddy**, Director, for his cooperation throughout the course of this project. Additionally, we extend our profound gratitude to **Sri. Ch. Gopal Reddy**, Chairman, **Smt. C. Vasantha Latha**, Secretary and
Sri. C. Abhinav Reddy, Vice-Chairman, for fostering an excellent infrastructure and a conducive learning environment that greatly contributed to our progress.

The guidance and support received from all the members of CMR Technical Campus who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement,

IX. REFERENCES

[1] Blockchain-Based Privacy-Preserving Quality Control for Mobile Crowdsensing Systems – https://ieeexplore.ieee.org/document/xxxxxxx

[2] Privacy-Preserving Mechanisms in Mobile Crowdsensing: A Survey – https://ieeexplore.ieee.org/document/xxxxxxx

[3] Secure Data Collection in Mobile Crowdsensing Using Blockchain Technology – https://www.sciencedirect.com/science/article/pii/xxxxxxx

[4] Homomorphic Encryption for Privacy-Preserving Data Aggregation – https://ieeexplore.ieee.org/document/xxxxxxx

[5] Noise-Based Data Validation Techniques in Crowdsensing Systems – https://www.springer.com/article/xxxxxxx

[6] Blockchain for Secure and Transparent Data Sharing in IoT – https://ieeexplore.ieee.org/document/xxxxxxx

[7] Smart Contracts for Decentralized Applications: A Survey – https://arxiv.org/abs/xxxxxxx

[8] Machine Learning Approaches for Data Quality Assessment in Crowdsensing – https://ieeexplore.ieee.org/document/xxxxxxx

X. GITHUB REPOSITORY LINK

https://github.com/naraboinanandhini/IOMP-A-13