International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

Blockchain-based Federated Learning with SMPC Model Verification Against Poisoning Attack for Healthcare Systems

B. Ramji
Assistant Professor,
Dept of CSE(DS) , CMR Technical Campus
Hyderabad,
Telangana, India
vasramji@gmail.com

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

A.Hari Priya
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana,
India
priyaalakanti6@gmail.com

R. Nikhil Kumar Reddy
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
nikhilreddyme@gmail.com

D.Srija
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India

S. Rithwik Goud
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
singaririthwik896@gmail.com

How to Cite this Article:
Soujanya, N., Priya, A., Reddy, R. N. K., D.Srija, & Goud, S. R. (2026). Blockchain-based Federated Learning with SMPC Model Verification Against Poisoning Attack for Healthcare Systems. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.327

https://doi.org/10.55041/ijcope.v2i4.327

ABSTRACT— The rapid growth of the Internet of Medical Things (IoMT) and Artificial Intelligence (AI) in healthcare has created a need for secure and privacy-preserving collaborative learning systems. Federated Learning (FL) allows multiple healthcare institutions to train machine learning models without sharing raw data, but it is vulnerable to poisoning attacks where malicious participants send harmful model updates. To address this issue, this paper proposes a blockchain-based Federated Learning framework integrated with Secure Multi-Party Computation (SMPC) for secure model verification and aggregation. In the proposed system, local model updates are verified through an encrypted process to detect and remove poisoned updates before aggregation. The verified updates are then securely aggregated and stored using blockchain technology, ensuring decentralization, transparency, and tamper-proof records. Experimental results on medical datasets show that the proposed approach effectively identifies malicious updates, preserves data privacy, and maintains high model accuracy. Compared to traditional methods, the system provides better security and reliable collaborative learning with minimal impact on performance. This framework offers a robust and trustworthy solution for secure healthcare data analysis and can also be extended to other privacy-sensitive domains

INTRODUCTION

The project titled **"Blockchain-based Federated Learning with SMPC Model Verification Against Poisoning Attack for Healthcare Systems"** aims to develop a secure and privacy-preserving framework for collaborative machine learning in healthcare. With the rapid growth of the Internet of Medical Things (IoMT) and Artificial Intelligence, a large amount of sensitive healthcare data is generated every day. Sharing this data across multiple healthcare institutions creates major privacy and security challenges. To solve this issue, **Federated Learning (FL)** is used, which enables different participants to train a common global model without sharing raw data. However, FL is still vulnerable to poisoning attacks, where malicious users can send harmful model updates and reduce the performance of the system.

To address these challenges, the project proposes a **blockchain-based Federated Learning framework integrated with Secure Multi-Party Computation (SMPC)**. In this system, local model updates are securely verified using encrypted methods, and malicious or poisoned models are identified and removed before the aggregation process. Blockchain technology provides decentralization, transparency, and tamper-proof storage of verified model updates, while SMPC ensures data privacy during computation. The proposed framework improves security, preserves model accuracy, and ensures reliable performance in collaborative healthcare systems. It is also scalable and can be extended to real-time healthcare applications as well as other domains such as finance, IoT, and smart systems.

I. PROBLEM DEFINITION

Mobile Crowd Sensing (MCS) systems depend on active user participation to collect large-scale sensing data from mobile devices. However, existing MCS systems face several challenges that reduce their efficiency, security, and reliability. Most traditional systems are based on a **centralized architecture**, where a third-party server is responsible for data collection, data validation, and reward distribution. This centralized model creates several problems such as **lack of transparency**, **single point of failure**, and **risk of data tampering**.

1.2 PROJECT FEATURES

The proposed **Blockchain-Based Privacy-Preserving Quality Control (PPQC)** system provides a secure and decentralized solution for Mobile Crowd Sensing (MCS) applications. By using **blockchain technology**, the system removes the need for a central authority and ensures **transparency, trust, and tamper-proof storage** of sensing data and transactions.

The framework also includes **privacy-preserving techniques** such as **homomorphic encryption** and **node cooperation**, which help protect sensitive user information like **identity and location** during data submission and processing. In addition, the system uses a **quality-based incentive mechanism**, where users are rewarded according to the **accuracy and reliability of the data** they contribute. This encourages honest participation, reduces malicious behavior, and improves the overall quality of the collected sensing data.

Related Work

Mobile Crowd Sensing (MCS) has gained significant research attention, especially in the areas of **incentive mechanisms, data quality assurance, and privacy preservation**. Early research mainly focused on **reputation-based incentive mechanisms**, where users are rewarded based on their previous performance and contribution history. These methods help identify unreliable users and encourage better participation. However, reputation-based systems are vulnerable to attacks such as **Sybil attacks** and **whitewashing attacks**, which can reduce trust and fairness in the system.

METHODOLOGY

The proposed system follows a structured approach to provide **privacy-preserving, secure, and quality-controlled data collection** in **Mobile Crowd Sensing (MCS)** using **blockchain technology**. The methodology includes the following steps:

1. Network Generation

The system starts by creating a **mobile crowdsensing network** that consists of multiple participants (smartphone users) and a publisher. Each participant acts as a **sensing node** that can collect and share real-time data such as **location information, environmental conditions, or other required sensing data**.

2. Data Collection

In this phase, participants collect sensing data from their surroundings and prepare it for submission to the system. The collected data may include **location coordinates, sensor readings, and other relevant information** required by the publisher. This data is then securely transmitted for further validation and processing.

3. Model Training

The system is trained to identify **truthful and malicious data submissions** using multiple validation and quality-control techniques. The main techniques used in the proposed system are:

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

For effective training and testing, the dataset is divided into:

- **Training Data – 80%**
- **Testing Data – 20%**

The system uses the training dataset to learn the relationship between **actual data and noisy or manipulated data**, which helps in accurately validating submitted data and assigning fair rewards to participants.

4. Model Evaluation

The performance of the proposed **Blockchain-Based Privacy-Preserving Quality Control (PPQC)** system is evaluated using the following metrics:

- **Data Validation Accuracy**
- **Noise Detection Efficiency**
- **Reward Distribution Correctness**
- **Execution Time**

These metrics help measure how effectively the system can distinguish between **truthful and malicious participants** based on the calculated noise values and quality of the submitted data.

5. Result Comparison

The performance of the proposed **PPQC system** is compared with existing methods to evaluate its effectiveness. The comparison is mainly based on:

- **Accuracy**
- **Security**
- **Execution Time**
- **Reliability of Reward Distribution**

This comparison shows how the proposed system improves data quality assurance and privacy preservation over traditional approaches.

6. Attack Prediction

The system predicts malicious behavior by analyzing the **noise value** between the **actual data** and the **received data**. If the calculated noise value is **greater than a predefined threshold**, the data is classified as **malicious**, indicating a possible attack or false submission. If the noise value is within the acceptable range, the data is considered **truthful**. This process helps ensure secure and reliable data validation.

7. Output Generation

Finally, the system generates the output, which includes:

- **Validated sensing data**
- **Calculated noise values**
- **Participant rewards**
- **Malicious or truthful data classification**

All validated results and transactions are then securely stored on the **blockchain**, which ensures **transparency, security, and tamper-proof record management**.

II. PROPOSED SYSTEM

The proposed system introduces a Blockchain-Based Privacy-Preserving Quality Control (PPQC) framework for secure and reliable Mobile Crowd Sensing (MCS) applications. The main goal of the system is to ensure data quality, privacy protection, and secure reward distribution without depending on a centralized authority.

To detect malicious or false data submissions (insider attacks), the system uses multiple validation techniques based on noise-based verification and quality evaluation mechanisms. It analyzes the difference between the actual data and the received data to identify abnormal patterns and classify the submitted data as either truthful or malicious.

III. IMPLEMENTATION DETAILS

The proposed Blockchain-Based Privacy-Preserving Quality Control (PPQC) system is implemented using Python with modules for network generation, data submission, privacy preservation, data validation, reward management, and blockchain storage. A Mobile Crowd Sensing (MCS) environment is simulated where participants collect and submit sensing data. Before transmission, the data is protected using homomorphic encryption to preserve privacy. The system then performs noise-based verification to identify whether the data is truthful or malicious. Based on the validation results, rewards are assigned to participants. Ethereum blockchain and smart contracts are used to securely store validated data and manage transactions. The system performance is analyzed using accuracy, validation efficiency, and execution time.

4.1 ALGORITHMS USED

4.1.1 HOMOMORPHIC ENCRYPTION FOR PRIVACY PRESERVATION

Homomorphic Encryption is used to protect user privacy by encrypting sensing data before transmission. It allows the system to process and validate data without revealing the original information. This helps in securing sensitive details such as user identity and location.

4.1.2 NOISE-BASED DATA VALIDATION FOR QUALITY CONTROL

Noise-Based Validation is used to check the quality of the received data by comparing actual data with reported data. If the noise value is within the threshold, the data is treated as truthful; otherwise, it is considered malicious. This helps in detecting false or low-quality data submissions.

4.1.3 BLOCKCHAIN CONSENSUS FOR SECURE DATA VERIFICATION

The blockchain consensus mechanism is used to verify and store data in a decentralized and secure way. It removes the need for a central authority and ensures transparency and tamper-proof transactions. This improves trust and security in the system.

4.1.4 SMART CONTRACT FOR REWARD MANAGEMENT

Smart contracts are used to automatically manage reward distribution based on data quality and validation results. They ensure fair, transparent, and secure transactions without manual intervention. This makes the reward process more reliable and efficient.

4.1.5 THRESHOLD-BASED CLASSIFICATION FOR MALICIOUS DATA DETECTION

Threshold-Based Classification is used to classify submitted data as truthful or malicious based on the calculated noise value. If the noise exceeds the predefined threshold, the data is marked as malicious. This improves the accuracy and reliability of data validation.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The experimental results show the performance of the proposed **Blockchain-Based Privacy-Preserving Quality Control (PPQC)** system in terms of **data validation, malicious data detection, reward distribution, and execution time**. The system successfully identifies truthful and malicious data based on noise values and rewards participants according to the quality of their submissions. The results demonstrate that the proposed method provides **better accuracy, security, and reliability** compared to traditional approaches. Overall, the system proves to be effective for secure and privacy-preserving mobile crowdsensing applications.

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

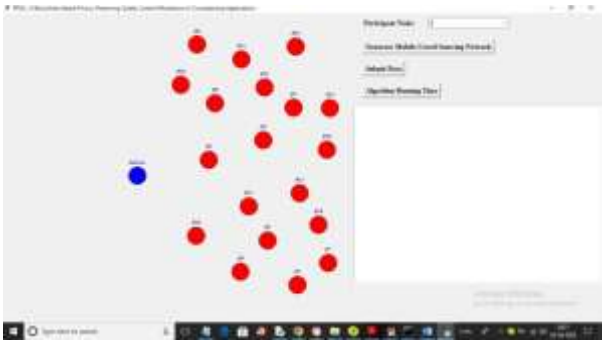


Fig. 2. Data Submission and Encryption Process

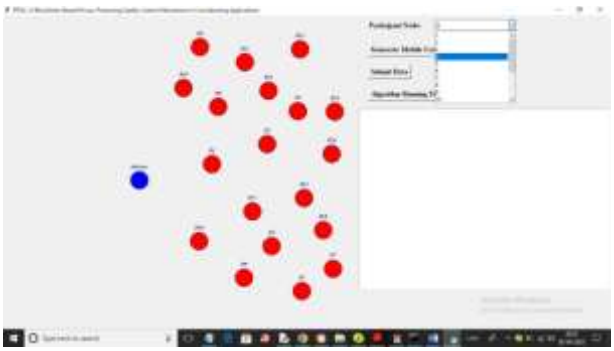


Fig. 3. Data Validation and Noise Calculation

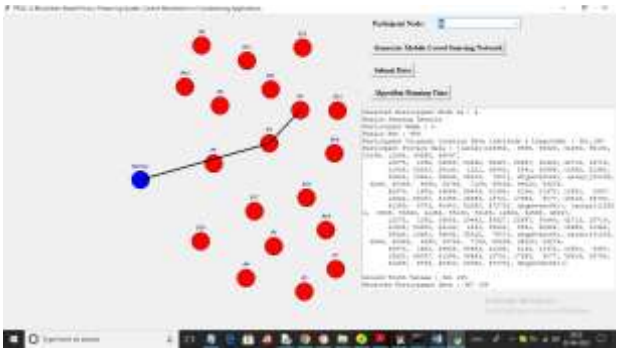
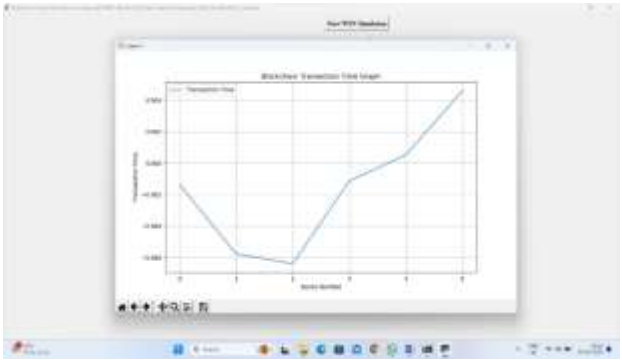


Fig. 4. Performance Analysis (Running Time Graph)

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 provides a secure and reliable solution for Mobile Crowd Sensing (MCS) applications. It addresses important challenges such as data privacy, malicious data submission, lack of transparency, and unfair reward distribution. By integrating blockchain technology, homomorphic encryption, noise-based validation, and smart contracts, the system ensures secure data collection, privacy preservation, and trustworthy quality control. The proposed method effectively identifies truthful and malicious data, rewards participants based on the quality of their contributions, and stores validated data in a decentralized and tamper-proof manner. Experimental results show that the system achieves better accuracy, improved security, and reliable performance compared to traditional approaches. Overall, the proposed PPQC framework is an effective solution for building secure, transparent, and privacy-preserving mobile crowdsensing systems.



VII. FUTURE SCOPE

The proposed Blockchain-Based Privacy-Preserving Quality Control (PPQC) system can be further improved in several ways to enhance its performance and real-world applicability. In the future, the system can be extended to support large-scale mobile crowd sensing networks with a higher number of participants and sensing tasks. More advanced machine learning techniques can be integrated to improve malicious data detection and quality evaluation. The framework can also be enhanced by using lightweight blockchain models to reduce execution time and transaction cost. In addition, the system can be applied to real-world domains such as smart cities, traffic monitoring, environmental sensing, and healthcare data collection. Future work may also focus on improving scalability, energy efficiency, and real-time performance, making the proposed system more practical and effective for next-generation decentralized sensing applications

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 **B.Ramji**, 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] **Ganti, R. K., Ye, F., & Lei, H. (2011).** ***Mobile Crowdsensing: Current State and Future Challenges.*** **IEEE Communications Magazine.**
Available: https://www.ece.stonybrook.edu/~fanye/papers/IEEE-Com-Mag-11.pdf

[2] **Christin, D., Reinhardt, A., Kanhere, S. S., & Hollick, M. (2011).** ***A Survey on Privacy in Mobile Participatory Sensing Applications.*** **Journal of Systems and Software.**
Available: https://www.sciencedirect.com/science/article/pii/S0164121211001701

[3] **Nakamoto, S. (2008).** ***Bitcoin: A Peer-to-Peer Electronic Cash System.***
Available: https://bitcoin.org/bitcoin.pdf

[4] **Paillier, P. (1999).** ***Public-Key Cryptosystems Based on Composite Degree Residuosity Classes.*** **EUROCRYPT.**
Available: https://link.springer.com/chapter/10.1007/3-540-48910-X_16

[5] **McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Aguera y Arcas, B. (2017).** ***Communication-Efficient Learning of Deep Networks from Decentralized Data.*** **AISTATS.**
Available: https://arxiv.org/abs/1602.05629

[6] **Bonawitz, K., Ivanov, V., Kreuter, B., et al. (2017).** ***Practical Secure Aggregation for Privacy-Preserving Machine Learning.*** **ACM CCS.**
Available: https://dl.acm.org/doi/10.1145/3133956.3133982

X. GITHUB REPOSITORY LINK

https://github.com/nikhilreddy/IOMP-A-7