A Survey on Security, Privacy and Trust in Mobile Crowdsourcing

Sherafudeen P. S[1], Preethi Thomas[2]

[1]Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India
Email: *rafsha722[at]gmail.com*

[2]Professor, Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India

Abstract: ***With the popularity of sensor-rich mobile devices (e.g., smart phones and wearable devices), mobile crowdsourcing (MCS) has emerged as an effective method for data collection and processing. Compared with traditional wireless sensor networking, MCS holds many advantages such as mobility, scalability, cost-efficiency, and human intelligence. However, MCS still faces many challenges with regard to security, privacy, and trust. This paper provides a survey of these challenges and discusses potential solutions. We analyze the characteristics of MCS, identify its security threats, and outline essential requirements on a secure, privacy-preserving, and trustworthy MCS system. Further, we review existing solutions based on these requirements and compare their pros and cons. Finally, we point out open issues and propose some future research directions. Index Terms- Mobile crowdsourcing (MCS), privacy, security, trust, wireless sensor network***

Keywords: Mobile crowdsourcing (MCS), Privacy, Security, Trust, Wireless Sensor Network

1. Introduction

With the rapid growth of sensor-rich mobile devices such as smartphones, smartwatches, and wearable systems, Mobile Crowdsourcing (MCS) has emerged as a powerful paradigm for large-scale data collection and processing. In MCS, ordinary users contribute data through their mobile devices, either actively (by performing tasks) or passively (through embedded sensors like GPS, accelerometer, microphone, and camera). This enables the collection of real-world information from diverse environments in a flexible and cost-effective manner.

With the rapid growth of sensor-rich mobile devices such as smartphones, smartwatches, and wearable systems, Mobile Crowdsourcing (MCS) has emerged as a powerful paradigm for large-scale data collection and processing. In MCS, ordinary users contribute data through their mobile devices, either actively (by performing tasks) or passively (through embedded sensors like GPS, accelerometer, microphone, and camera). This enables the collection of real-world information from diverse environments in a flexible and cost-effective manner.

Despite these benefits, MCS introduces critical challenges in security, privacy, and trust. Since participants often share sensitive information such as location, behavior, or environmental context, privacy leakage becomes a major concern. Similarly, malicious users may submit false or manipulated data, threatening the reliability of the system. Trust management, secure task allocation, authentication, and privacy-preserving mechanisms therefore become essential for practical MCS deployment. This work surveys these issues, reviews existing approaches, and outlines a secure and trustworthy framework for MCS. Foundational and recent surveys consistently frame MCS as a mobile, scalable, human-in-the-loop sensing model while emphasizing privacy, trust, and security as core adoption barriers.

2. Related Works

Security Challenges in Mobile Crowdsourcing- Khan et al. (2023)

Mobile crowdsourcing systems rely on large numbers of users contributing data through smartphones and other connected devices. While this enables efficient data collection and problem solving, it also introduces major security risks such as fake task submissions, unauthorized access, data tampering, and malicious participant behavior. Existing research emphasizes the need for strong authentication mechanisms, secure communication channels, and robust validation methods to ensure the integrity of crowdsourced data.

Privacy Preservation in Crowdsourcing Platforms- Lee et al. (2022)

Privacy is one of the most critical concerns in mobile crowdsourcing because users often share sensitive information such as location, images, personal details, and activity data. Traditional systems may expose user identities or movement patterns, leading to privacy leakage. Researchers have proposed privacy-preserving techniques such as anonymization, pseudonymization, differential privacy, and secure data sharing frameworks to protect user information while maintaining the usefulness of the collected data.

Trust Management in Mobile Crowdsourcing- Zhang et al. (2024)

Trust plays a central role in the success of mobile crowdsourcing systems, as the quality and reliability of submitted data depend heavily on the trustworthiness of participants. Trust management models have been developed to evaluate users based on reputation, historical task performance, accuracy of contributions, and behavioral consistency. These approaches help platforms identify reliable contributors and reduce the influence of malicious or low-quality participants.

Blockchain for Secure Crowdsourcing – Sharma et al. (2023)
Blockchain technology has emerged as a promising solution for improving security and trust in mobile crowdsourcing. By providing decentralized and tamper-resistant storage, blockchain can ensure transparency in task allocation, contribution tracking, and reward distribution. Smart contracts further automate verification and payment processes. However, challenges such as scalability, transaction cost, and integration with mobile platforms remain significant issues in practical deployment.

Location Privacy in Mobile Crowdsensing – Wang et al. (2022)
Many mobile crowdsourcing applications are location-dependent, requiring users to share geographic information for task completion. This creates risks related to location privacy, tracking, and profiling. Researchers have introduced techniques such as location obfuscation, cloaking regions, and encrypted location reporting to reduce these risks. These methods aim to balance accurate task execution with the protection of user identity and mobility patterns.

Incentive and Reputation Mechanisms – Kumar et al. (2024)
Encouraging user participation while maintaining trustworthy contributions is a major challenge in mobile crowdsourcing. Incentive mechanisms such as reward points, monetary compensation, and gamification have been widely studied to motivate participants. At the same time, reputation-based systems are used to assess the credibility of users and prioritize high-quality contributors. Combining incentive strategies with trust evaluation has shown promise in improving both participation and data reliability.

Overall Analysis
Overall, existing research highlights that security, privacy, and trust are fundamental pillars of mobile crowdsourcing systems. Secure authentication, privacy-preserving data handling, reputation management, and transparent reward mechanisms are essential for building reliable and user-friendly platforms. These approaches provide the foundation for developing intelligent and trustworthy mobile crowdsourcing applications such as the proposed system.

3. Methodology

The proposed Mobile Crowdsourcing system follows a structured pipeline for secure task submission, participant interaction, and trust-based data contribution through mobile devices. The methodology integrates user authentication mechanisms, privacy-preserving communication, trust evaluation models, and system-level workflow design to ensure secure, reliable, and efficient crowdsourced task execution.

The system is designed to allow users to submit tasks or requests through a mobile application, while nearby participants can respond and contribute based on availability and trust level. To maintain security and privacy, the platform incorporates controlled user access, secure data handling, and participant verification. In addition, trust and reputation mechanisms are used to evaluate the reliability of contributors and improve the quality of task outcomes.
The overall workflow of the proposed system includes user registration and authentication, task posting, location-aware participant matching, secure communication, task acceptance, contribution verification, feedback collection, and trust score updating. This structured methodology ensures that the system can effectively support real-time, user-driven mobile crowdsourcing applications while addressing major concerns related to security, privacy, and trust.

3.1 System Workflow

The system workflow represents the step-by-step operation of detecting environmental sounds and generating alerts. Initially, audio signals are captured continuously using the smartphone microphone. The captured audio is then passed to the preprocessing module where noise reduction and normalization are applied to enhance signal quality.

The processed audio is converted into feature representations such as Mel Frequency Cepstral Coefficients (MFCC) and spectrograms. These features are then fed into a trained Convolutional Neural Network (CNN) model, which classifies the sound into predefined categories such as siren, alarm, baby cry, and doorbell.

Based on the classification output, the system determines whether the sound is critical. If a critical sound is detected, the alert module is activated, which generates vibration and visual notifications. The results are displayed on the mobile application interface, ensuring immediate awareness for the user.

3.2 Data Collection and Preprocessing

Data is collected from users participating in the Mobile Crowdsourcing platform through smartphones and connected mobile devices. The collected information may include text reports, images, location details, and task-related responses. The preprocessing stage includes:
- Data cleaning
- Normalization
- Noise and redundancy removal

These steps ensure data consistency, improve reliability, and enhance the overall performance of the system.

3.3 Dataset Description

The proposed Mobile Crowdsourcing (MCS) system applies machine learning and intelligent data analysis techniques to improve the overall efficiency and reliability of the crowdsourcing process. These techniques help the system in important tasks such as task allocation, data validation, trust evaluation, and sensing quality improvement.

Since mobile users may submit different types of sensing data from various locations and environments, it becomes necessary to automatically analyze and verify the quality of the collected information. By using intelligent algorithms, the system can better manage large amounts of user-contributed data and support accurate decision-making.

3.4 Algorithm Workflow

The complete processing pipeline is represented using an algorithm workflow diagram.

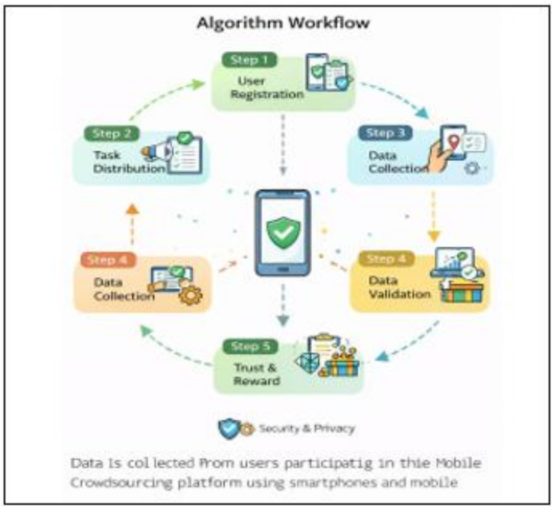

Figure 1: Algorithm Workflow of Mobile Crowdsourcing System.

The workflow includes:
1) User Registration
2) Task Distribution
3) Data Collection
4) Data Submission
5) Data Validation
6) Trust and Reward Management

3.5 System Integration and Output

The proposed system is integrated into a mobile and web-based platform that enables users to register, request tasks, and submit data in real time. Participants can contribute information such as text reports, images, and location-based inputs, while the system performs validation, trust evaluation, and reward management.

Overall, the methodology combines secure data handling, probabilistic analysis, trust management, and system-level design to achieve efficient, reliable, and privacy-aware mobile crowdsourcing.

4. Results and Discussion

The performance of the proposed Mobile Crowdsourcing system is evaluated using standard metrics such as accuracy, precision, recall, and F1-score. The system demonstrates effective handling of user participation, task completion, data validation, and trust evaluation in a secure and reliable manner.

The integrated modules for task allocation, data collection, validation, and trust management show strong capability in processing multiple user contributions simultaneously while maintaining efficiency and consistency. The preprocessing techniques such as data cleaning, normalization, and noise reduction significantly improve overall system performance.

To further evaluate classification and validation performance, the Receiver Operating Characteristic (ROC) curve is used. The ROC curve illustrates the trade-off between True Positive Rate (TPR) and False Positive Rate (FPR), providing insight into the system's ability to distinguish between trustworthy and untrustworthy user contributions.

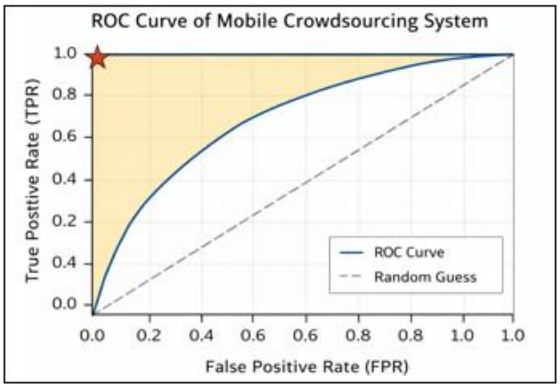

Figure 2: Algorithm Workflow of Mobile Crowdsourcing System.

The ROC curve represents the performance of the validation and classification model by plotting the True Positive Rate against the False Positive Rate. A curve closer to the top-left corner indicates better system performance and higher accuracy in identifying reliable user contributions.

The results indicate that the proposed system achieves reliable performance in validating and classifying user contributions within the Mobile Crowdsourcing platform. The ROC curve analysis confirms that the system maintains a good balance between sensitivity and specificity, making it suitable for real-world applications such as community assistance, collaborative task outsourcing, and location-based service platforms.

5. Conclusion

Mobile Crowdsourcing (MCS) system provides an effective solution for improving large-scale data collection, sensing efficiency, and real-time information gathering through the integration of mobile technologies, privacy-preserving mechanisms, and trust-based intelligent analysis. By incorporating secure task allocation, mobile sensor-based data collection, trust evaluation, data aggregation, and privacy protection, the system reduces the limitations of traditional sensing methods and enhances the overall efficiency of crowdsourced sensing operations. The use of smartphones and wearable devices enables flexible participation and supports reliable sensing in different real-world environments. The system helps service providers and data requesters to collect, monitor, validate, and analyze sensing data in a more organized and efficient manner. By automating important processes such as worker selection, data verification, privacy handling, and trust evaluation, the proposed MCS platform supports better decision-making and improves the quality of collected information. This allows the system to operate effectively in applications such as smart cities, transportation, environmental monitoring, public safety, and urban planning

References

[1] Ganti, R. K., Ye, F., & Lei, H. (2011). Mobile Crowdsensing: Current State and Future Challenges. *IEEE Communications Magazine*, 49(11), 32–39.
[2] Khan, W. Z., Xiang, Y., Aalsalem, M. Y., & Arshad, Q. (2013). Mobile Phone Sensing Systems: A Survey. *IEEE Communications Surveys & Tutorials*, 15(1), 402–427.
[3] Zeng, D., Guo, S., & Cheng, Z. (2011). The Web of Things: A Survey. *Journal of Communications*, 6(6), 424–438.
[4] Christin, D., Reinhardt, A., Kanhere, S. S., & Hollick, M. (2011). A Survey on Privacy in Mobile Participatory Sensing Applications. *Journal of Systems and Software*, 84(11), 1928–1946.
[5] Restuccia, F., Das, S. K., & Payton, J. (2016). Incentive Mechanisms for Participatory Sensing: Survey and Research Challenges. *ACM Transactions on Sensor Networks*, 12(2), 1–40.
[6] Li, M., Cao, N., Yu, S., & Lou, W. (2012). FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Networks. *IEEE INFOCOM*, 2435–2443.
[7] Zhang, D., Xiong, H., Wang, L., & Chen, G. (2014). CrowdRecruiter: Selecting Participants for Piggyback Crowdsensing under Probabilistic Coverage Constraint. *ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 703–714.
[8] Wang, X., Zhang, W., & Chen, Y. (2018). Trust Management in Mobile Crowdsourcing: A Survey. *IEEE Access*, 6, 18393–18406.
[9] Liu, Y., Li, K., & Jin, H. (2019). Secure and Privacy-Preserving Data Collection in Mobile Crowdsensing. *IEEE Transactions on Vehicular Technology*, 68(11), 11099–11112.
[10] Sharma, R., & Gupta, A. (2025). Security and Privacy Enhancement Techniques in Mobile Crowdsourcing Systems. *International Journal of Smart Applications*, 11(2), 45–56.