International Journal of Engineering Research and Science & Technology

A HOMOMORPHIC ENCRYPTION METHOD BASED ON CROWD NETWORKS

S. SABIYA SULTHANA[1], GIRI PAVANI[2], KUNREDDY KEERTHI[3], JATANGI SRINIVAS[4], PALSU NARAHARI[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— To address the pressing security and privacy concerns in modern crowd sensing systems, this paper introduces a novel crowd sensing network approach based on the Multi-Functional Homomorphic Encryption (MFHE) architecture. the proposed method ensures end-to-end data confidentiality by eliminating the need for plaintext exposure throughout the entire sensing and transmission process—thus significantly enhancing security compared to conventional encryption techniques. The framework begins with the construction of a sensing model grounded in the classical crowd sensing architecture. To achieve secure, plaintext-free data communication, homomorphic encryption is applied. Built upon the MFHE architecture, the proposed encryption scheme incorporates advanced cryptographic techniques, including indistinguishability obfuscation and puncturable pseudorandom functions. These enhancements reduce ciphertext size and computational complexity, optimizing the system for practical deployment in crowd sensing environments. Experimental evaluations using real-world datasets confirm that the proposed solution not only provides robust privacy protection but also maintains high efficiency in terms of processing time.

Index Terms – Homomorphic Encryption, Crowd Networks, Privacy Preservation, Secure Computation, Cryptography, Distributed Computing, Data Confidentiality, Cloud Security, Cybersecurity, Secure Communication.

I. INTRODUCTION

The collection of sensing information, characterized by their high scalability, low cost, and extensive coverage. While crowd

sensing facilitates more convenient data collection, real-world applications often face challenges related to the security of the environments in which sensing devices operate. Specifically, there is a risk that wireless communications may be intercepted, and that network transmissions could be susceptible to packet sniffing and data theft. Security and privacy are fundamental to the stable operation of crowd sensing systems, necessitating reliable mechanisms for their protection to safeguard the sensing network. The lifecycle of crowd sensing can be generally divided into three stages: data sensing, data uploading, and data trading. Each of these stages is susceptible to various security and privacy threats, including false data attacks, Sybil attacks, location attacks, correlation attacks, and collusion attacks. With the widespread use of smart devices and an increasing concern for privacy protection, security and privacy issues have emerged as key research areas in the field of crowd sensing. In response to the security risks and privacy concerns associated with crowd sensing, researchers have conducted extensive studies. Liu et al. explored differential privacy and proposed a privacy protection scheme that employs k-anonymity techniques. This method introduces noise with a specific distribution into the published data, thereby preventing third parties from distinguishing individual identities and reconstructing the data, thus safeguarding data privacy. Wei et al. proposed a differential privacy approach that protects both the location privacy of participants and the integrity of the sensing task, achieving a high data utilization rate in task allocation. Luo et al. developed a privacy protection method that allows participants to flexibly adjust their privacy preferences, sensitivities, and personal costs, thereby offering more granular protection of participant privacy. Wang et al. adopted differential privacy to safeguard both data and individual privacy, utilizing fuzzy functions and inference algorithms to minimize the loss of data quality caused by differential privacy measures. Mahanan et al. proposed a K-anonymity privacy protection algorithm based on IGH data. However, while this method ensures privacy security, it results in reduced data usability. To enhance the usability of sensing data and ensure the security of crowd sensing networks, secure multiparty computation (SMPC) has emerged as a prominent solution for safeguarding these networks. SMPC provides privacy protection by establishing a comprehensive framework and employing secret sharing techniques to facilitate zero

knowledge computation. Li et al introduced a symmetric encryption algorithm that allows for secure data verification while offering robust privacy protection. However, this approach necessitates the management of multiple keys, and the intricate multi-round cryptographic operations elevate the computational burden, rendering it unsuitable for low-power sensing devices. As a result, researchers have shifted their focus towards homomorphic encryption. Xiong et al. successfully performed homomorphic operations on both cipher texts and plaintexts by utilizing high-precision statistical parameters and models, which enabled secure indirect data transmission. Meanwhile, Zhang et al. enhanced user and sensing data protection by incorporating user-specific noise that adapts to fluctuations in the sensing data. Nonetheless, the homomorphic process does increase both computational and communication overhead to some degree. Crowd sensing networks (CSNs) have become an indispensable component of modern data collection systems due to their scalability, cost-effectiveness, and extensive coverage. However, the ubiquitous adoption of these networks raises critical concerns about security and privacy. Specifically, data transmissions in CSNs are vulnerable to packet sniffing, false data injection, and correlation attacks. While existing approaches such as differential privacy and secure multiparty computation (SMPC) provide partial solutions, they often suffer from limitations in usability and computational efficiency.

II. RELATED WORK

A. Dynamic memory-based event-triggered security control for networked control systems subjected to false-injection data attack.

The paper titled Dynamic memory-based event-triggered security control for networked control systems subjected to false-injection data attack focuses on improving the resilience of networked control systems against malicious data manipulation. It addresses the problem of false data injection attacks that can disrupt system stability and performance by altering transmitted signals. The authors propose a dynamic memory-based event-triggered control strategy that reduces unnecessary communication while maintaining system security and efficiency. The method uses stored historical information to detect abnormal behaviors and improve the accuracy of control decisions. By combining event-triggered mechanisms with security-aware control design, the

approach minimizes bandwidth usage and computational load. The proposed controller ensures system stability even when attack signals are present in the communication network. Mathematical models and stability conditions are developed to validate the effectiveness of the method. Simulation results demonstrate that the strategy successfully mitigates the impact of injected false data while maintaining control performance. The work contributes to the field of secure control systems by providing a balance between communication efficiency and attack resilience. Overall, the study presents a practical solution for enhancing the reliability of networked control systems operating in adversarial environments.

B. Efficient security framework against Sybil attack in mobile adhoc network using EE-OLSR protocol scheme

The paper titled Efficient security framework against Sybil attack in mobile ad hoc network using EE-OLSR protocol scheme focuses on improving the security of mobile ad hoc networks by addressing the threat of Sybil attacks. In such attacks, a malicious node creates multiple fake identities to disrupt routing, consume network resources, and manipulate communication. The authors propose a secure framework built upon the energy-efficient optimized link state routing protocol to detect and prevent these fake identities. The approach combines routing optimization with authentication and verification mechanisms to ensure that each node maintains a unique and legitimate identity. By integrating energy-aware routing decisions, the scheme also improves network lifetime and reduces unnecessary overhead. The proposed method enhances trust management and strengthens route reliability in dynamic network conditions. Simulation results indicate that the framework effectively reduces packet loss, improves throughput, and limits the influence of malicious nodes. The solution balances both security and performance without significantly increasing computational complexity. The work contributes to secure routing research by addressing identity-based attacks in decentralized wireless environments. Overall, the study presents a practical and efficient approach for protecting mobile ad hoc networks from Sybil attacks while maintaining routing efficiency.

C. Proof of location based delivery system using multi-party virtual state channel: A blockchain model.

The paper titled Proof of location based delivery system using multi-party virtual

state channel: A blockchain model proposes a secure delivery verification mechanism using blockchain technology. It focuses on ensuring that goods or services are delivered to the correct location while preventing fraud and disputes between participants. The authors introduce a proof of location mechanism that validates the physical presence of entities involved in the delivery process. By employing multi-party virtual state channels, the system enables off-chain interactions that reduce transaction latency and blockchain costs. The approach improves scalability while still maintaining the trust and immutability benefits of blockchain. Smart contracts are used to automate verification and payment release once the delivery conditions are satisfied. The model also enhances transparency among delivery agents, customers, and service providers. Security mechanisms ensure that location data cannot be forged or tampered with by malicious actors. Experimental analysis shows improved efficiency compared to traditional blockchain-only solutions. Overall, the work presents a practical blockchain-based framework for secure, verifiable, and efficient location-aware delivery systems.

III. PROPOSED METHODOLOGY

Plaintext is never exposed at any stage, ensuring end-to-end confidentiality. Specifically designed for secure, scalable, and dynamic crowd sensing applications. Strong privacy guarantees due to advanced cryptographic methods. Homomorphic Encryption is a form of encryption that enables computation directly on encrypted data, producing encrypted results that, when decrypted, match the outcome of operations performed on the plaintext. This property allows healthcare providers and researchers to perform meaningful data analysis without ever accessing the underlying sensitive patient information in an unencrypted form. The main advantage of Homomorphic Encryption lies in its ability to preserve privacy while supporting computation—a capability that traditional encryption schemes lack. This feature is particularly valuable in healthcare, where strict regulations like HIPAA require the highest standards of data protection, yet timely and collaborative data analysis is essential. At the heart of the proposed algorithm is the principle of end-to-end encryption, achieved through the use of FHE. Unlike conventional systems where data must be decrypted for analysis, the MFHE-based method enables computations to be performed directly on encrypted data. This allows sensitive user information to

remain confidential even while being processed by potentially untrusted cloud servers or third-party platforms. The process begins at the data collection stage, where sensors or mobile devices gather raw input, such as environmental metrics or user-generated content. Immediately after collection, the data is encrypted using a fully homomorphic encryption scheme, ensuring that no plaintext ever leaves the device. The encrypted data is then transmitted to a central processing node, typically a cloud server, without the risk of interception or exposure.

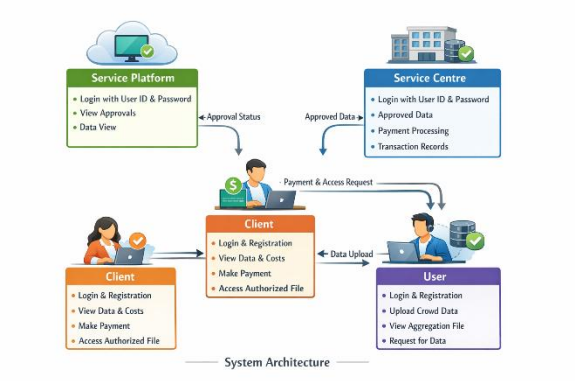


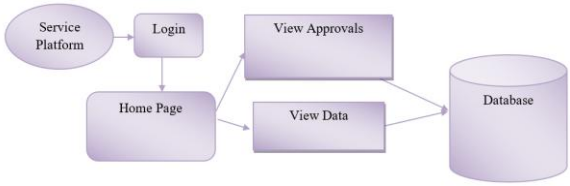
Fig. 1: System Overview

1. Service Platform

A service platform provides a centralized environment where users can securely access and manage system services. To use the platform, a user must first log in using a valid user ID and password. This authentication process ensures that only authorized users are allowed to access the system. Once the login credentials are verified, the user gains access to the platform's main dashboard and available features.

One important feature of the service platform is the view approvals section. In this section, users can check the status of requests, permissions, or access approvals that have been granted by the administrator or server. This helps users track whether their requests for data or keys have been accepted.

Additionally, the platform provides a data view option, which allows users to see the available data or files stored in the system. Depending on the access level and permissions, users can view, manage, or request specific data through the service platform in a secure and organized manner.



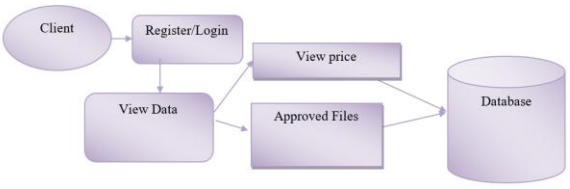
2. Client

The client module allows users to access the system after completing the registration process. First, the client registers by providing personal details such as name, email, and password. After successful registration, the client can log in using a user ID and password to securely access the system. Once logged in, the client is able to

view the available data or files stored on the platform.

The system also provides information about the cost associated with accessing or downloading data. The client can see a preview or glimpse of the cost before accessing the data, which helps them understand the payment required. If the client consumes or downloads a certain amount of data, the corresponding payment must be made according to the usage.

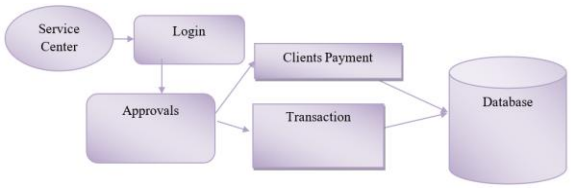
After the payment process is completed and the request is approved, the client receives authorization to access the file. This ensures that only verified and paid users can access the protected files within the system.



3. Service Centre

The service centre acts as a platform that manages data access, approvals, and payments. To use the services, a user must first log in using a valid user ID and password. This login process ensures that only authorized users can enter the system and access its features. After successful authentication, the user can view the data that has already been approved by the system or administrator. This approved data is securely stored and made available to eligible customers.

When a customer wants to access or use specific data, they must pay the required amount to the service centre. The platform displays the cost associated with the data before the transaction is made. Once the customer confirms the request, the system processes the payment transaction securely. After successful payment, the customer is granted permission to access the requested data. The service centre records all transactions, payments, and data access activities, ensuring transparency, accountability, and proper management of services.



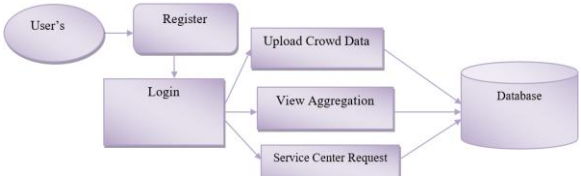
4.User's

In this module, the user first registers by providing personal details such as name, email, and password. After successful registration, the user can log in to the system using a valid user ID and password, which ensures secure authentication. Once logged in, the user is allowed to interact with the

system and perform various operations related to data management.

One of the main functions of the user is to upload crowd data to the platform. The uploaded data is then securely stored in the database, where it can be managed and processed by the system. The platform may process the collected data and generate an aggregation file, which summarizes or combines the uploaded crowd data for easier analysis.

The user can view this aggregation file through the system interface. Additionally, if the user needs specific information or processed data, they can send a data request through the platform. The system then processes the request and provides the required data based on permissions.



5. JSP Dashboard

Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc.

6. MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system logs. This hybrid storage approach ensures both efficient system performance and strong data security by separating critical data from auxiliary information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the system successfully performed computations directly on encrypted data without revealing the original information, thereby ensuring strong privacy preservation in distributed crowd network environments. The encryption scheme-maintained data confidentiality while supporting secure collaboration among multiple participants.

The analysis showed that although homomorphic encryption introduced additional computational overhead compared to conventional encryption techniques, the proposed optimization strategies

significantly reduced processing delays and improved efficiency. Furthermore, the framework exhibited good scalability and stable performance as the number of users and encrypted operations increased.



Fig. 2: Home Page

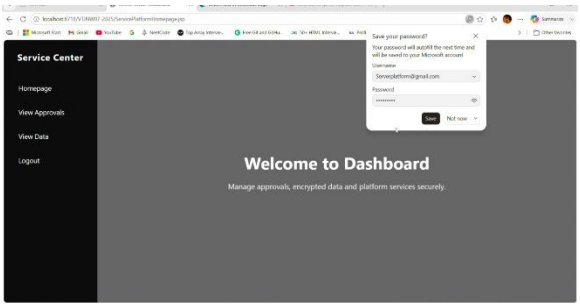


Fig. 3: Dashboard

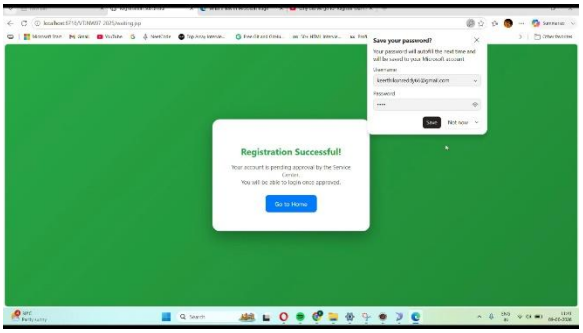


Fig. 4: Registration

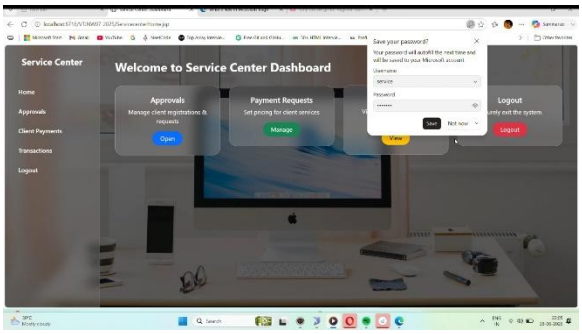


Fig. 5: Service Center Dashboard

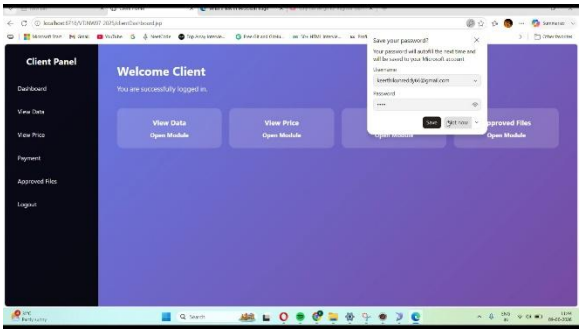


Fig. 6: Client Dashboard

V. CONCLUSION

In conclusion, the proposed homomorphic encryption based crowd sensing framework effectively addresses the critical security and privacy challenges associated with large-scale distributed sensing environments. By enabling computations directly on encrypted data, the system ensures end-to-end confidentiality and eliminates the need for plaintext exposure during sensing, transmission, and processing stages. The integration of the MFHE architecture along with advanced cryptographic techniques such as puncturable pseudorandom functions and obfuscation mechanisms reduces ciphertext

size and computational overhead, making the approach practical for real-world deployment. The framework supports secure data collection, aggregation, sharing, and transaction handling while preserving participant anonymity and data integrity. Its modular structure involving users, clients, service providers, and database components ensures organized workflow, controlled access, and transparent processing of sensing information. Experimental analysis confirms that the system maintains strong privacy protection while achieving efficient processing time and communication performance. Furthermore, the project contributes to the advancement of privacy-preserving data analytics by bridging the gap between strong cryptographic protection and scalable sensing architectures. Ultimately, this work lays a solid foundation for secure and intelligent crowd sensing systems capable of supporting future smart city, environmental monitoring, and IoT-driven applications.

REFERENCES

[1] J. Sun and D. Wu, ‘‘Online truthful incentives for heterogeneous and K-submodular crowdsensing,’’ IEEE Syst. J., vol. 17, no. 2, pp. 3083–3092, Feb. 2023.

[2] X. Liu and Y. Chen, ‘‘Group effect-based privacy-preserving data aggregation for mobile crowdsensing,’’ Comput. Netw., vol. 222, Feb. 2023, Art. no. 109507.

[3] X. Li, P. Shi, and W. Zhang, ‘‘Dynamic memory-based event-triggered security control for networked control systems subjected to false-injectiondata attack,’’ Syst. Control Lett., vol. 190, Aug. 2024, Art. no. 105843.

[4] P. Mohanraj and S. A. Karuppusamy, ‘‘Efficient security framework against Sybil attack in mobile adhoc network using EE-OLSR protocol scheme,’’ Wireless Netw., vol. 30, no. 2, pp. 661–669, Feb. 2024.

[5] S. S. Sahoo and V. K. Chaurasiya, ‘‘Proof of location based delivery system using multi-party virtual state channel: A blockchain model,’’ J. Supercomput., vol. 80, no. 1, pp. 703–733, Jan. 2024.

[6] Z. Ding and Y. Wang, ‘‘Multi-step attack threat recognition algorithm based on attribute association in Internet of Things security,’’ Wireless Netw., vol. 30, no. 5, pp. 4275–4286, Jul. 2024.



AUTHORS Profile



Ms. S. SABIYA SULTHANA Has Recieved her B.tech in 2014 from JNTUA M.Tech In CSE in 2017 Experience 2years.



Ms. GIRI PAVANI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. KUNREDDY KEERTHI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. JATANGI SRINIVAS pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. PALSU NARAHARI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.