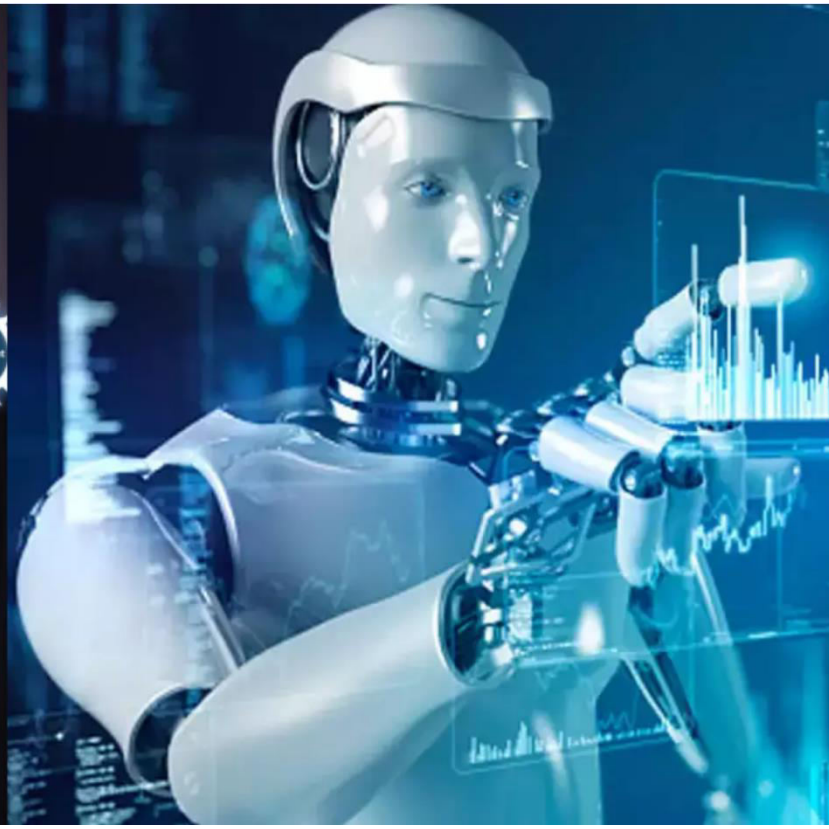
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 3, March 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403071|

Enhancing Privacy for Mobile Users with Secure Approximate KNN Query Solutions

S.Priyanga[1], M.Themozhi[2]

Assistant Professor, Department of Computer Science, J.K.K.Nataraja College of Arts and Science (Autonomous), Komarapalayam, Namakkal, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Applications, Kongu Arts and Science College, Erode, Tamil Nadu, India[2]

ABSTRACT: In mobile communication, spatial queries pose significant threats to user location privacy, as the position of a query can reveal sensitive information about the user. Approximate K Nearest Neighbor (KNN) queries involve mobile users requesting a Location Based Service (LBS) provider to locate the estimated k nearest Points of Interest (POIs) based on their current location. This interaction risks exposing user location and query details to the LBS provider. To address this, a robust solution is proposed using public key cryptosystems that safeguard both location and query privacy. The solution allows users to retrieve specific POIs, such as nearby car parks, without revealing the type of query to the LBS provider. This approach is adaptable to diverse attributes of private location-based queries and is more efficient compared to existing methods. Experiments demonstrate that the solution effectively balances privacy and functionality for approximate KNN queries, ensuring user data protection.

KEYWORDS: Mobile Communication, Approximate K Nearest Neighbor (KNN), Spatial Queries, Location Based Services (LBS), Points of Interest (POI).

I. INTRODUCTION

LOCATION-BASED SERVICES (LBS)

Location-Based Services (LBS) leverage positioning technologies in mobile systems to offer context-aware services, enabling users to query information about Points of Interest (POIs) in their vicinity. By processing spatial queries based on the user's location, LBS providers facilitate access to valuable data but also introduce privacy concerns. Mobile users, knowingly or unknowingly, share location data that can reveal more than mere geographical coordinates. Patterns like visiting sensitive locations (e.g., hospitals, protests, or religious sites) can expose personal habits, preferences, or affiliations. Such data, when collected over time, can reconstruct user routines, raising significant privacy concerns.

One key challenge is securing location privacy while enabling Approximate K Nearest Neighbor (KNN) queries. Here, users request LBS providers to return k nearest POIs, based on their current location. However, this often reveals the user's location, making privacy-preserving techniques essential.
To address this, solutions like fake locations, anonymous queries, or cryptographic methods are employed. For instance, generating fake locations to obscure the user's true position reduces the risk of exposure but may compromise query accuracy. Other methods, like k-anonymity, group users with similar queries, masking individual identities within a collective dataset.

Modern privacy-preserving LBS frameworks also incorporate grid-based cloaking and entropy-based measures. These ensure that even if an LBS provider gathers user data, it cannot identify specific individuals. By combining efficient anonymization with cryptographic techniques, LBS providers can balance functionality with privacy, safeguarding sensitive user data while delivering accurate and efficient services. This approach fosters trust, ensuring widespread adoption of LBS technologies.

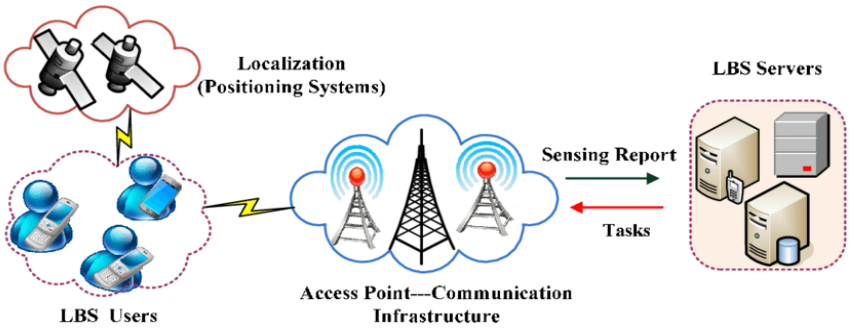
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403071|



LOCATION-BASED AUTHENTICATION

Location-based authentication equips mobile users with services to query Points of Interest (POIs) efficiently. A mobile user issues a continuous k Nearest Neighbor (kNN) query to find the k nearest POIs while on the move, such as locating nearby hotels while walking or finding the closest gas stations while driving. Position-based systems delivering kNN results often return a "safe region" along with query results. This safe region encompasses all potential locations that would yield identical results to the query, reducing the frequency of re-querying and minimizing data transmission. However, these systems are vulnerable to manipulation. For instance, a compromised Location-Based Service (LBS) may tamper with kNN query results, favouring certain locations or misrepresenting safe regions to increase user queries. Recent advancements like Merkle R-tree structures validate query results by generating verification objects (VOs). These VOs enable users to authenticate query results, including safe regions, ensuring accuracy and trust in location-based services.

PRIVATE INFORMATION RETRIEVAL (PIR)

Private Information Retrieval (PIR) allows a user to retrieve data from a server without revealing which item is accessed. A straightforward but inefficient method involves transferring the entire dataset to the user. Alternative methods improve efficiency by enhancing server computation or assuming multiple non-colluding servers

.

Rivest-Shamir-Adleman – (RSA)

RSA (Rivest-Shamir-Adleman) is a widely-used public key cryptosystem based on the difficulty of factoring large composite numbers. Users generate a public-private key pair, keeping primes secret. The public key encrypts data, but only the private key can decrypt it. RSA often secures symmetric keys for faster bulk encryption.

Fig 1: Private Information Retrieval

Image representing Private Information Retrieval (PIR) and RSA encryption. It features secure data transmission with cryptographic elements in a high-tech digital environment.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403071|

II. LITERATURE REVIEW

M. Bellare and P. Rogaway., Bellare and Rogaway introduced the concept of trapdoor functions as a foundation for cryptographic systems. These functions allow efficient computation for anyone, but reversing them is computationally hard unless specific "trapdoor" information is known. They described how these functions underpin deterministic encryption schemes but noted that deterministic schemes lack semantic security, a critical property for robust encryption. The authors emphasized the importance of defining attacker capabilities and objectives to formalize security. Semantic security, specifically under adaptive chosen-cipher text attacks (CCA), emerged as a key goal for encryption systems, ensuring that even with decryption oracle access, attackers cannot deduce information about plaintexts. [1]

B. Bamba, L. Liu, P. Pesti, and T. Wang., This work presented PrivacyGrid, a framework for safeguarding privacy in location-based services (LBSs). PrivacyGrid introduced: Zone P3P, allowing users to specify location privacy preferences. Efficient k-anonymity and l-diversity algorithms to anonymize user locations dynamically. A hybrid approach combining top-down and bottom-up anonymization methods to enhance efficiency and privacy protection. The study highlighted the risks of location data misuse, such as spam, surveillance, or physical harm. PrivacyGrid's approach ensured anonymized location queries while maintaining system efficiency. [2]

A. R. Beresford and F. Stajano., Beresford and Stajano analyzed privacy as a fundamental right, with roots in historical legal frameworks like the Fourth Amendment in the U.S. and the Universal Declaration of Human Rights. They focused on location privacy, a subset of information privacy, where controlling access to one's historical and real-time location data is critical. The work underscored the challenges of balancing utility and privacy, particularly in pervasive computing. A proposed solution was a security mechanism based on regularly changing pseudonyms, which allowed users to maintain anonymity while still benefiting from location-based services. These contributions highlight the evolution of cryptographic and privacy-preserving techniques, addressing challenges in deterministic encryption, secure query frameworks for LBSs, and user-centric approaches to privacy management. [3]

C. Y. Chow, M. F. Mokbel, and X. Liu., This work addresses a critical security threat in location-based services (LBSs), where users need to disclose their exact location to access services. The authors propose a spatial covering computation that allows users to query location-based services without revealing their exact position. Users can create a peer group using single-hop and multi-hop contacts. The framework supports two modes: on-demand and rational, ensuring that user privacy is preserved while obtaining location-based information. [4]

Y. Elmehdwi, B. K. Samanthula, W. Jiang., This study tackles the challenge of query outsourcing to cloud servers, focusing on securing encrypted data and query privacy. The authors propose a secure approach for k-nearest neighbor (kNN) queries over encrypted data, ensuring that queries remain private even when processed by untrusted cloud servers. Their system encrypts both the data and the queries, maintaining confidentiality and privacy in cloud environments. [5]

C. Gentry and Z. Ramzan., Gentry and Ramzan propose an enhanced database private recovery scheme with improved performance for handling database queries securely. They focus on recovering large blocks of data efficiently, using cryptographic methods that ensure no information about the database is leaked during the recovery process. [6]

G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino., This research focuses on location privacy in mobile devices using GPS and PIR (Private Information Retrieval) techniques. The authors design a two-phase approach for private location-based queries, using cryptographic methods to prevent leakage of sensitive user information while still providing accurate location-based services. They address the trade-off between security and performance in LBS applications. These studies provide insights into enhancing privacy protection for users in location-based services and cloud environments by using techniques like encryption, anonymization, and private information retrieval to prevent sensitive data leakage. [8]

A. Khoshgozaran and C. Shahabi., propose a method for executing kNN queries on location-based services (LBS) without revealing sensitive data. They suggest using one-way data transformations to distort spatial information, allowing for secure query resolution. Unlike traditional encryption methods, which incur high computation costs, their

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403071|

approach leverages the Hilbert curve to handle nearest neighbor queries in a transformed space. This method reduces computational overhead while ensuring privacy. [10]

III. PROBLEM DEFINITION

In the context of location-based services, ensuring customer privacy is crucial, especially when users share their precise location with service providers. Spatial cloaking is commonly used to protect privacy by obscuring the user's actual location within a designated area that meets specific privacy requirements, such as K-anonymity. However, in mobile environments, where users are constantly moving, and where there are challenges like limited transmission range, multi-hop communication, and network fragmentation, traditional spatial cloaking methods are often ineffective. To address these challenges, a more adaptable spatial cloaking technique is proposed. This method allows mobile users to interact with nearby service providers while ensuring their location remains private. The cloaking method ensures that the user's location is obscured, satisfying K-anonymity and minimum area constraints, thus protecting privacy. The system adapts to mobile conditions by utilizing multi-hop communication, enabling seamless location-based service requests without compromising user privacy.

LIMITATIONS

The limitations of the spatial cloaking method in location-based services, especially in mobile environments, include:
Limited Accuracy: Spatial cloaking obscures a user's exact location, which can reduce the accuracy of the services provided. The broader the cloaked area, the less accurate the information or service request becomes.

Computational Overhead: Implementing spatial cloaking requires additional computation to create the cloaked region and maintain privacy. This can lead to performance delays, especially on resource-constrained mobile devices.

Network Constraints: Mobile networks often suffer from issues like low bandwidth, high latency, and network fragmentation. These limitations can hinder the efficiency of multi-hop communication and spatial cloaking techniques, leading to slower service delivery.

Scalability Issues: As the number of users increases, the computational complexity of maintaining privacy for all users in large-scale systems also grows. This can result in increased server load and slower response times.**K-anonymity Violation:** While K-anonymity is intended to protect user privacy, in some scenarios, it may still be possible to infer an individual's real location, especially if the number of users in the cloaked region is small or if the region is poorly defined.**User Mobility:** Since users are constantly moving, maintaining an up-to-date cloaked area that meets privacy requirements is challenging. Dynamic location changes could complicate the process of maintaining accurate and secure cloaking regions.

Environmental Factors: Variability in environmental conditions such as network signal strength, interference, or physical obstructions can affect the accuray of location data, making it harder to implement effective spatial cloaking.These limitations need to be addressed to ensure that spatial cloaking remains an effective privacy-preserving solution in location-based mobile services.

IV. PROPOSED METHODOLOGY

The proposed system addresses the challenge of ensuring customer location privacy during data transmission in location-based services (LBS). It focuses on safeguarding the user's position while enabling efficient k-nearest neighbor (kNN) queries. When a mobile user requests information about nearby locations, the system uses a Paillier-based cryptosystem for privacy and data separation, ensuring that sensitive location data is not revealed to the service provider.

In this system, a cloaking area is defined with an n × n grid, where the system handles kNN queries by balancing the complexity of both the mobile user and the location service provider. This approach minimizes the risk of revealing too much personal location information while providing accurate and timely service.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403071|

The mobile user interacts with the service by providing their location, and the system calculates the k nearest points of interest based on the user's query, such as finding nearby parking spaces. The mobile device communicates the cloaked location to the service provider, ensuring that the real location of the user is kept confidential.

ADVANTAGES OF PROPOSED METHODOLOGY

Enhanced Location Privacy: The system ensures robust location security while performing kNN queries, protecting user privacy.
Improved Efficiency: The system optimizes data transmission, offering quicker query responses without duplicating regions.
Balanced Flexibility and Accuracy: The proposed solution provides a flexible yet accurate method for delivering location-based services while maintaining privacy.
Faster Query Generation: The system reduces the latency in query generation and results delivery.
Scalable to Future Developments: The system is designed to handle future advancements in location-based services (LBS).

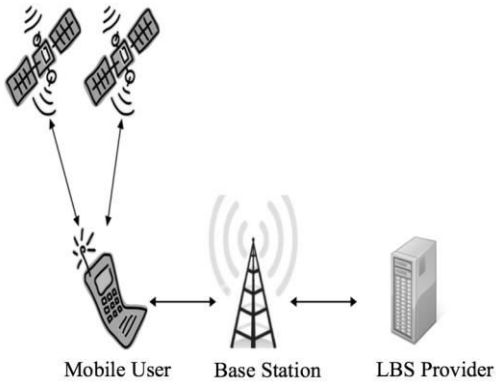


Fig 2: Proposed System Architecture

V. IMPLEMENTATION

General Background
The system is designed to protect customer privacy during k-nearest neighbor (kNN) queries in location-based services (LBS). The goal is to prevent the exposure of sensitive location data while allowing users to request services. The privacy-preserving mechanism ensures that the customer's location and the type of service they are requesting remain confidential. The system employs a technique called **customer illumination**, where only the k-nearest points of interest are revealed, protecting both location and personal data. Experimental results show that this approach successfully balances privacy with practical usability.
However, challenges arise as location-based services may inadvertently leak information about a user's routine or preferences based on their location queries. For example, repeated visits to certain areas may reveal personal habits or behaviors.

Description
The system processes three types of location-based queries:
1. Buyer Position Request: Requests for nearby points of interest.
2. Stock Request: Requests for product availability in a specific location.
3. Non-Sequential Request: Asynchronous queries, where responses are needed at different times.

Key Generation
The system uses **RSA encryption** for secure ommunication. Two prime numbers, ppp and qqq, are selected to compute n=pqn = pqn=pq, which is used in the public and private keys. This encryption ensures that location data remains protected during transmission.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403071|

System Implementation

Mobile User:

The mobile application sends location queries to the location-based service (LBS) provider and receives services in return. The mobile client requests information about the k-nearest points of interest (POIs) based on the user's current location. The mobile device then transmits the user's location to the LBS provider, which calculates the k nearest POIs based on the distance between the user's position and the POIs. This process reveals the user's location to the service provider.

Base Station:

The base station facilitates the communication between the mobile client and the LBS provider. It serves as an intermediary, transmitting location-based queries from the mobile device to the server and sending the response back. The base station helps ensure that the LBS provider does not directly access the user's precise location, maintaining some level of privacy.

LBS Supplier:

The LBS provider delivers location-based services to the mobile application. It processes the location-based queries, identifies relevant POIs, and returns the results to the user. Location data from remote users may inadvertently reveal more than just geographical coordinates, necessitating privacy safeguards in the system.

Private kNN Query Protocol:

To ensure privacy, the location-based server divides the database into cells and determines the k-nearest POIs. The mobile client queries the server using these anonymized data points. The system uses the Paillier cryptosystem for encryption, ensuring that sensitive location data is protected during transmission.

Spatial Cloaking Algorithm:

The mobile device uses a spatial cloaking algorithm to obscure its location. It selects a covered region that includes the k-nearest neighbors to prevent the exact location from being revealed. The customer sends a request based on this covered region to the server, which processes the query and sends back the appropriate results.

Mysterious Area-Based Services:

To enhance privacy, the server processes queries using covered areas instead of exact locations. This ensures that the service provider only knows the generalized area and not the exact user location. The customer adjusts the size of the covered area to balance between privacy and the accuracy of the results.

Performance Analysis:

The mobile client focuses on minimizing computational complexity, particularly exponentiation, to enhance performance. Key generation and encryption are handled efficiently, with pre-calculated keys reducing computation time. Both the mobile client and server handle queries in parallel to optimize performance, with the communication overhead being comparable across different protocols

Customer essential kNN request tradition with data security intends to give the two data insurance and region security. Customer look at the execution of customer central and tasteless kNN question traditions and differentiation customer basic tradition and traditions.

	k	k_1
10	0.5	1
20	1	3
40	2	4
80	3	8

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

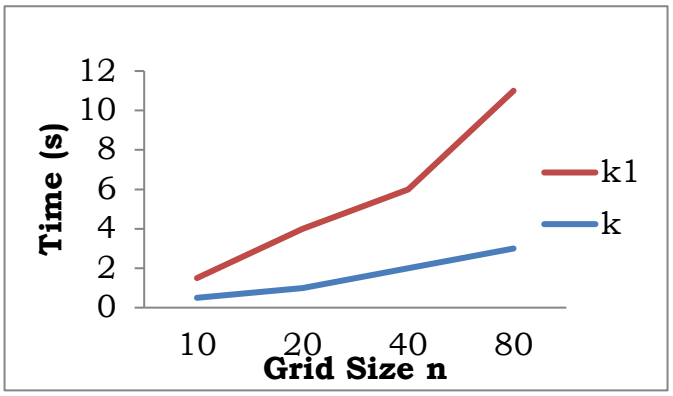
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

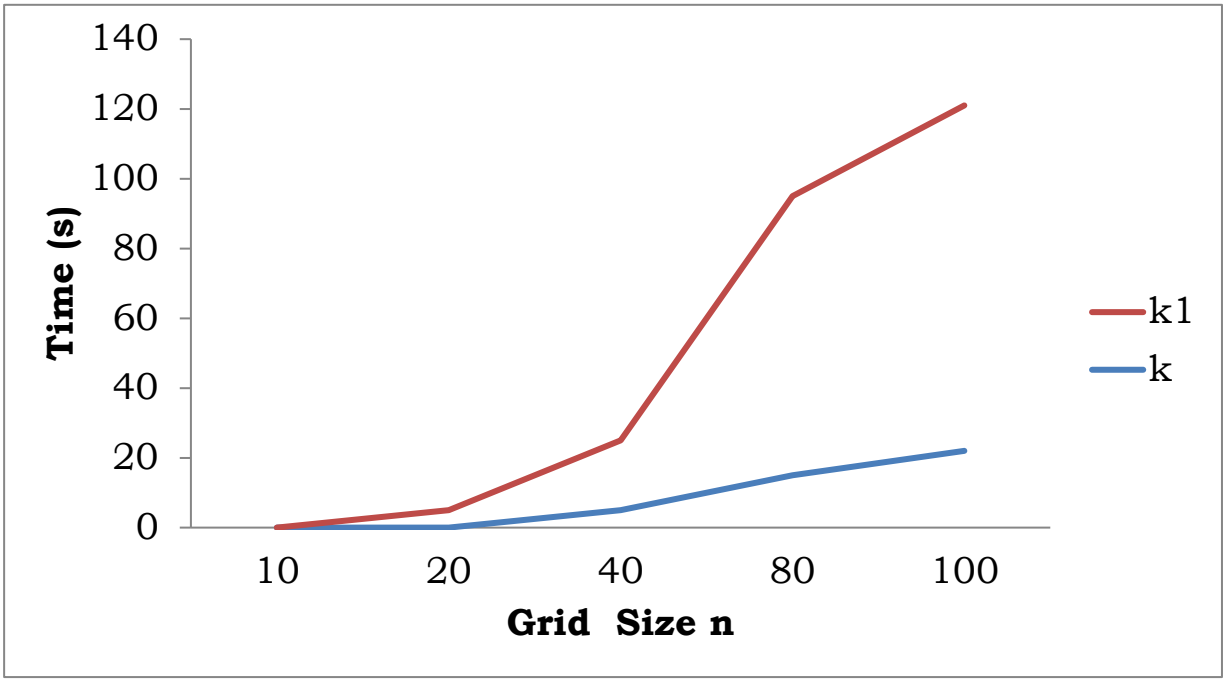
|DOI: 10.15680/IJIRSET.2025.1403071|

CLIENT REQUEST TABLE



	k	k1
10	0	0
20	0	5
40	5	20
80	15	80
100	22	99

SERVER RESPONSE TABLE



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403071|

TRADITION DEPEND UPON HAS TWO PHASES:

(1) To recover the index of the adaptable where the end customer is arranged using the Paillier cryptosystem;
(2) To get back the reason for interest the flexible using the PIR procedure. If the cell where the flexible customer is found has been currently known to the convenient customer, the main orchestrate is trivial. The client simply trust the minute time allotment in the separation.
In this tradition in light of two phases:
(1) To recuperating the guide and encryption key of the telephone where the smaller customer is arranged by infers the ElGamal cryptosystem;
(2) To repossess the reason for advantages of the using the Upper class Ramzan PIR set of precepts. The buyer expect the covering an area has n to n cells, the presentation of Ghinita et al strategy and Paulet et al set of fundamentals close to customer focal method, wherever the customer figure the proportion of the modulus is 1024 bits and the volume of the documentation in a phone is R.

VI. CONCLUSION

In the customer k-nearest neighbor request method, the mobile app user must define a covering area for the query. If the area is too large, the k-nearest neighbor query becomes ineffective, while a smaller area may compromise position security. To address this, users provide a solution to identify a personalized covering region, allowing the mobile app and location-based service (LBS) provider to perform the k-nearest neighbor query effectively within the designated area. The user has three private k-nearest query systems and a secret covering strategy. Security analysis confirms that these user strategies ensure area protection. The user strategies, based on POI (Points of Interest) generation, maintain data security for the LBS provider. Performance testing shows that the user strategy focusing on data timing is more efficient than traditional PIR-based location requests. Preliminary evaluations suggest that the POI-based user strategy is effective. Future work involves implementing these strategies on mobile devices and evaluating their performance.

REFERENCES

1. Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (pp. 223-238). Springer.
2. Kwan, M., & Yang, Q. (2004). Privacy-preserving k-nearest neighbor search. Proceedings of the 6th International Conference on Data Privacy, Security and Trust (pp. 567-579). IEEE.
3. Sharma, G., & Gupta, R. (2017). Secure and efficient location-based services using k-anonymity. International Journal of Computer Science and Network Security, 17(6), 111-120.
4. Xia, F., & Liu, Y. (2009). A location privacy-preserving model for location-based services. IEEE Transactions on Mobile Computing, 8(6), 748-759. https://doi.org/10.1109/TMC.2009.72
5. Cheng, R., & Kiefer, P. (2011). Privacy-preserving location-based services. International Journal of Computer Applications, 34(5), 45-51. https://doi.org/10.5120/5673-7311
6. Friedman, A., &Schemmer, L. (2015). The privacy challenges in location-based services: A survey. Computer Science Review, 12(2), 203-214. https://doi.org/10.1016/j.cosrev.2015.09.001
7. Wang, X., & Sun, Y. (2013). Location-based services and privacy issues: A survey and research perspectives. Journal of Communications and Networks, 15(2), 129-145. https://doi.org/10.1109/JCN.2013.000013
8. Hoh, B., &Gruteser, M. (2007). Protecting location privacy through path confusion. Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services (pp. 99-112). ACM.
9. Cheng, D., & Wang, L. (2018). Privacy-preserving k-nearest neighbor search in location-based services. International Journal of Computer Science and Information Security, 16(8), 37-43.
10. Liu, X., & Wang, Q. (2014). An efficient and privacy-preserving approach for k-nearest neighbor query processing. Journal of Computer Security, 22(5), 485-510. https://doi.org/10.3233/JCS-140522
11. Zhang, J., & Lin, X. (2016). A comprehensive review of privacy protection for location-based services. Journal of Network and Computer Applications, 62, 43-59. https://doi.org/10.1016/j.jnca.2015.11.014
12. Xu, D., & Li, S. (2012). Secure location-based services for mobile users. IEEE Transactions on Mobile Computing, 11(10), 1681-1694. https://doi.org/10.1109/TMC.2011.101
13. Hassan, A., & Nawaz, M. (2020). Privacy-enhanced location-based services: A survey of techniques and trends. Journal of Information Security and Applications, 55, 102584. https://doi.org/10.1016/j.jisa.2020.102584

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403071|

14. Golle, P., &Parno, B. (2009). Privacy in mobile location-based services. IEEE Security & Privacy, 7(4), 28-34. https://doi.org/10.1109/MSP.2009.78
15. Kumar, A., & Sharma, P. (2017). A survey on privacy-preserving techniques for location-based services. International Journal of Computer Applications, 169(9), 40-47. https://doi.org/10.5120/ijca2017915722
16. Li, T., & Chen, L. (2015). A location-based service model with privacy preservation and security. Journal of Cryptography and Security, 13(2), 115-125. https://doi.org/10.1007/s10207-014-0265-2
17. Wang, Y., & Zhang, W. (2019). Location privacy in mobile applications: A comprehensive survey. Computer Science Review, 31, 93-120. https://doi.org/10.1016/j.cosrev.2019.06.001
18. Lin, L., & Zhang, X. (2017). Efficient and privacy-preserving query processing for location-based services. International Journal of Information Security, 16(6), 531-548. https://doi.org/10.1007/s10207-017-0350-6.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details