Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Search Me If You Can Privacy-Preserving Location Query Services

D.Lakshman Babu[1], A.Umesh Chandra[2], Adinasiddhika[3], B.Vijaya Lakshm[4],

[1]*Assistant Professor*

[2]*UG Scholar*

[3]*UG Scholar*

[4] *UG Scholar*

[1234]*Department Of Computer Science and Engineering, Nalla Malla Reddy Engineering College,Hyderabad,India.*

Abstract: The rise of Location-Based Services (LBS) alongside the proliferation of smartphones and social network services has ushered in a new era of convenience and functionality. However, the use of users' location information by LBS providers poses significant privacy risks, as location data inherently contains sensitive information. Addressing this challenge, our paper introduces a sophisticated Privacy-preserving Location Query Protocol (PLQP). This innovative protocol offers fine-grained control over location queries, allowing different users to access encrypted location information at varying levels of detail. Notably, PLQP is designed with efficiency in mind, making it suitable for deployment on mobile platforms. By striking a balance between utility and privacy, our protocol represents a significant step forward in safeguarding personal privacy in the realm of Location-Based Services.

Key-words: Location-Based Services (LBS), Privacy Preservation, Location Privacy, Fine-grained Control, Location Query Protocol.

I. Introduction

Location-Based Services (LBS) have surged in popularity alongside the widespread adoption of smartphones, offering users a myriad of context-rich functionalities. Equipped with GPS modules, smartphones boast powerful computational capabilities that facilitate the processing of users' location information, catalyzing the proliferation of LBS applications within the smartphone ecosystem. Consider a commonplace scenario: snapping a photo with a smartphone camera automatically embeds the location where the picture was taken, serving as a handy aid for recollection. Moreover, the exponential growth of Social Network Services (SNS) has further propelled the expansion of LBS, forging connections between location information and social networks. For instance, when a smartphone-captured photo, complete with embedded location data, is uploaded to a Facebook album, the system promptly displays the picture's location on a map,

allowing the user's friends on Facebook to view it, unless privacy settings dictate otherwise. Numerous such applications cleverly leverage both LBS and SNS, offering an array of enticing features. However, it's worth noting that location information harbors more than just spatial coordinates; it can inadvertently divulge sensitive personal details. Take, for instance, a scenario where Alice and Bob, both utilizing a check-in application on Facebook, concurrently register their presence at a quaint restaurant. From this, it becomes inferable that Alice and Bob might be on a date, potentially disclosing unintended information. Thus, there arises a pressing need for privacypreserving protocols to forestall significant privacy breaches arising from the intersection of LBS and SNS.

Conventionally, many applications have resorted to employing group-based access controls on shared locations. Social photosharing platforms like Flickr afford users the option to designate access permissions to all users, neighbors, friends, or family members, with SNS behemoths like Facebook and Google+ offering additional

support for custom-defined user groups. However, mobile applications often lag in this aspect. Many of them, such as Circle, Who's Around, and Foursquare, eschew granular control options and instead present users with a binary choice: to disclose or not to disclose their location. Such oversimplified approaches fail to adequately address user needs. From the user's perspective, explicitly defining a user group to restrict location visibility solely to them proves cumbersome. It would be more intuitive to establish conditions such that only friends meeting certain criteria can or cannot access the location information. Furthermore, binary access controls fall short of fulfilling users' nuanced privacy requirements. For instance, consider Alice's scenario again; she may wish to share the precise location of her date at the restaurant with her closest friends while opting to disclose only her general whereabouts to others. Such scenarios necessitate intermediate settings between absolute disclosure and complete secrecy. Existing privacy control mechanisms in LBS suffer from coarseness in two main aspects. Firstly, users can only delineate a predefined group of users who can or cannot access their location information. Secondly, access control policies are binary in nature, limiting users to either enabling or disabling information disclosure. Moreover, these control strategies are marred by privacy leaks concerning server storage. Even if a user opts to disable all location disclosures, their location remains susceptible to access by the server, posing a significant concern for users. Hence, there arises a critical need for fine-grained privacy controls that operate on encrypted location data, a requisite to further foster the growth of LBS and its associated business market.

II. Review Of Literature

1) T. Hashem and L. Kulik,

"Safeguarding location privacy in wireless ad-hoc networks," Ubicomp 2007: Ubiquitous Computing, pp. 372– 390, 2007.

Hashem and Kulik present strategies for safeguarding location privacy in wireless ad-hoc networks. The paper explores techniques to mitigate location privacy risks inherent in the dynamic and decentralized nature of ad-hoc networks. The paper investigates various privacy-preserving mechanisms, including pseudonymization, location obfuscation, and secures communication protocols. These techniques aim to prevent unauthorized access to sensitive location information and protect user privacy in ad-hoc network environments. Limited Scalability: Some of the proposed privacy-preserving techniques may incur additional overhead, impacting the scalability and performance of ad-hoc networks, especially in large-scale deployments. Trade-offs with Utility: Balancing location privacy with the utility of location-based services remains a challenge, as stronger privacy protections may result in reduced functionality or accuracy of location-based applications. **2) C. Bettini, X. Wang, and S. Jajodia, "Protecting privacy against locationbased personal identification," Secure Data Management, pp. 185–199, 2005.** Bettini, Wang, and Jajodia address the issue of protecting privacy against location-based personal identification. The paper proposes strategies to prevent the inference of sensitive personal information from location data. The paper introduces techniques such as spatial and temporal cloaking, data perturbation, and differential privacy to obfuscate location information and mitigate the risk of personal identification. These methods aim to strike a balance between preserving user privacy and maintaining the utility of location-based services. Complexity of Implementation:

Implementing advanced privacy-preserving techniques may require significant computational resources and expertise, posing challenges for deployment in realworld systems.

Robustness against Attacks: Adversarial entities may attempt to exploit vulnerabilities in the privacy protection mechanisms, highlighting the importance of continuous evaluation and improvement of privacy safeguards.

3) M. Mokbel, C. Chow, and W. Aref,

"The new casper: query processing for location services without compromising privacy," in Proceedings of the 32nd international conference on Very large data bases, VLDB Endowment, 2006, pp. 763–774.

Mokbel, Chow, and Aref introduce the New Casper system, which enables query processing for location services without compromising privacy. The paper addresses the challenge of balancing location utility with

privacy protection in location-based query processing. The New Casper system employs techniques such as spatial cloaking, query transformation, and secure multiparty computation to anonymize location data and protect user privacy during query processing. These mechanisms ensure that location-based queries can be executed efficiently while minimizing the risk of privacy breaches. Computational Overhead:

The overhead associated with anonymization and secure computation may impact the performance and scalability of the New Casper system, particularly in scenarios with high query throughput or large datasets. Practical Deployment: Deploying and integrating privacypreserving query processing techniques into existing location-based services may require substantial changes to infrastructure and software systems, posing challenges for adoption in practice.

4) K. Vu, R. Zheng, and J. Gao, "Efficient algorithms for k-anonymous location privacy in participatory sensing." in IEEE INFOCOM, 2012.

Vu, Zheng, and Gao present efficient algorithms for achieving k-anonymous location privacy in participatory sensing applications. The paper addresses the challenge of protecting user location privacy while enabling collaborative data collection in distributed sensing environments. The paper proposes novel algorithms for anonymizing location data collected from participatory sensing devices, ensuring that each user's location remains indistinguishable among a group of at least k individuals. These algorithms aim to strike a balance between privacy protection and data utility in participatory sensing applications. Trade-offs with Data Utility: Achieving k-anonymity may require sacrificing the granularity or accuracy of location data, potentially impacting the effectiveness of participatory sensing applications that rely on precise location information.

Scalability Concerns: Ensuring k-anonymity in large-scale participatory sensing networks may pose challenges in terms of computational complexity and communication overhead, especially in dynamic and heterogeneous environments.

5) L. Sweeney et al., "k-anonymity: A model for protecting privacy," International Journal of Uncertainty Fuzziness and Knowledge Based Systems, vol. 10, no. 5, pp. 557–570, 2002.

Sweeney et al. propose the k-anonymity model as a means of protecting privacy in data release scenarios. The paper introduces the concept of k-anonymity and outlines its application in anonymizing sensitive information, including location data. The kanonymity model ensures that individual records in a dataset cannot be uniquely identified by combining quasi-identifiers, such as location attributes, with external information. By grouping similar records into anonymized sets of size k or more, the model aims to prevent re-identification attacks while preserving data utility. Vulnerability to Background Knowledge: Achieving k-anonymity may not always guarantee protection against privacy attacks if adversaries possess additional background knowledge or auxiliary information that can be used to de-anonymize individuals. Complexity of Generalization: Generalizing location data to achieve k-anonymity without overly compromising data utility may require careful consideration of spatial and semantic hierarchies, posing challenges for practical implementation. **6) H. Zang and J. Bolot, "Anonymization of location data does not work: A largescale measurement study," in Proceedings of the 17th annual international conference on Mobile computing and networking, 2011, pp. 145–156.**

Zang and Bolot present a large-scale measurement study on the effectiveness of anonymization techniques for location data. The paper investigates the limitations and vulnerabilities of existing anonymization methods in preserving location privacy. The study evaluates the effectiveness of location anonymization techniques by analyzing a large dataset of real-world location traces. By examining the re-identification risk and privacy implications of different anonymization approaches, the authors highlight the challenges and shortcomings in protecting location privacy. Deanonymization Risks: The study reveals that existing anonymization techniques may not provide sufficient protection against reidentification attacks, as adversaries can exploit patterns and correlations in location data to infer sensitive information.Tradeoffs with Data Utility: Balancing the level of anonymization with the utility of location data remains a challenge, as stronger anonymization measures may result in decreased data quality and usability for legitimate purposes.

7) H. Kido, Y. Yanagisawa, and T. Satoh, "Protection of location privacy using dummies for location-based services," in 21st International Conference on Data Engineering Workshops, 2005, pp. 1248– 1248.

Kido, Yanagisawa, and Satoh propose a method for protecting location privacy in location-based services (LBS) using dummy locations. The paper introduces techniques to obfuscate users' actual locations and mitigate the risk of privacy breaches. The paper presents algorithms for generating and managing dummy locations that can be used to cloak users' actual locations in LBS applications. By incorporating dummy locations into location queries and responses, the proposed method aims to enhance user privacy without compromising the functionality of LBS. Impact on Location Accuracy: Introducing dummy locations into location-based queries may reduce the accuracy and precision of query results, especially in scenarios where precise location information is required for meaningful interactions. Management Overhead: Generating and managing a sufficient number of dummy locations to ensure effective location privacy protection may introduce additional computational and storage overhead, impacting the efficiency of LBS systems.

8) A. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications

Workshops, 2004, pp. 127–131.

Beresford and Stajano propose the concept of mix zones as a mechanism for enhancing user privacy in location-aware services. The paper introduces techniques to create zones where users' location information is mixed, thereby reducing the risk of location-based tracking. The paper presents algorithms for defining mix zones and managing user interactions within these zones to preserve location privacy. By anonymizing user movements and interactions within mix zones, the proposed approach aims to prevent unauthorized access to sensitive location information. Trade-offs with Location Accuracy: Aggregating user location information within mix zones may result in decreased accuracy and resolution of location data, potentially limiting the usefulness of location-aware services for certain applications. Design and Implementation Challenges: Designing effective mix zone algorithms and integrating them into existing locationaware services may pose technical challenges, requiring careful consideration of factors such as zone boundaries, user mobility patterns, and interaction dynamics.

9) B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J. Herrera, A. Bayen, M. Annavaram, and Q. Jacobson, "Virtual trip lines for distributed privacypreserving traffic monitoring," in Proceeding of the 6th international conference on Mobile systems, applications, and services, ACM, 2008, pp. 15–28.

Hoh et al. propose the concept of virtual trip lines for distributed privacy-preserving traffic monitoring. The paper introduces a decentralized approach to traffic data collection that protects user privacy while enabling effective traffic analysis. The paper presents algorithms for defining virtual trip lines and collecting traffic data from mobile devices as they cross these lines. By aggregating anonymized traffic data locally and transmitting only summary statistics to a central server, the proposed approach minimizes the risk of privacy breaches. Accuracy of Traffic Analysis: Aggregating anonymized traffic data from virtual trip lines may result in less granular and detailed traffic analysis compared to traditional methods that collect individual vehicle trajectories. This could impact the accuracy and effectiveness of traffic monitoring and management strategies. Adoption

Challenges: Deploying virtual trip line systems may require coordination among multiple stakeholders, including government agencies, transportation authorities, and mobile service providers. Overcoming regulatory and organizational barriers to adoption could be challenging. **10) M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: user-centric approaches towards maximizing location privacy," in Proceedings of the 5th ACM workshop on Privacy in electronic society, 2006, pp.**

19–28.

Li et al. introduce Swing & Swap, usercentric approaches aimed at maximizing location privacy. The paper presents techniques for users to control and manage their location privacy preferences in various contexts,

including location-based services and social interactions. The paper proposes mechanisms for users to dynamically adjust their location privacy settings based on contextual factors such as their social circles, activity patterns, and privacy preferences. By empowering users to customize their privacy levels, Swing & Swap aims to enhance user control and autonomy over their location information. Complexity of Privacy Management:

Implementing user-centric location privacy approaches may require users to navigate complex settings and decision-making processes, potentially leading to confusion or errors in managing their privacy preferences. Privacy-Utility Trade-offs: Maximizing location privacy through usercentric approaches may entail trade-offs with the utility and functionality of locationbased services, as stricter privacy settings could limit access to location-relevant features and information.

11) X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-aware multiple mix zone placement for protecting location privacy." in IEEE INFOCOM

2012.

Liu et al. propose traffic-aware multiple mix zone placement techniques for protecting location privacy. The paper presents algorithms for strategically placing mix zones in traffic networks to minimize the risk of location tracking while preserving traffic analysis capabilities. The paper introduces optimization models and algorithms for determining the optimal placement of mix zones in traffic networks based on traffic flow patterns, congestion levels, and privacy requirements. By considering traffic dynamics, the proposed approach aims to enhance location privacy without compromising traffic management and analysis. Computational Complexity: Optimizing mix zone placement in largescale traffic networks may involve solving complex optimization problems with high computational overhead, potentially limiting the scalability and real-time performance of the proposed techniques. Practical Deployment Challenges: Deploying and managing multiple mix zones in traffic networks may require coordination among transportation authorities, infrastructure operators, and regulatory agencies. Overcoming logistical and organizational barriers to deployment could be challenging. **12) B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in Proceedings of 25th IEEE International Conference on Distributed Computing Systems, 2005, pp. 620–629.**

Gedik and Liu propose a personalized anonymization model for addressing location privacy in mobile systems. The paper presents techniques for dynamically adjusting the level of location anonymization based on individual user preferences and contextual factors. The paper introduces algorithms for personalized location anonymization, where users can specify their privacy preferences and constraints based on factors such as location sensitivity, social context, and activity patterns. By tailoring anonymization levels to individual users, the proposed model aims to optimize the balance between privacy protection and data utility. Complexity of Personalization:

Implementing a personalized anonymization model may require sophisticated algorithms and user interfaces to capture and incorporate diverse user preferences and contextual factors. The complexity of personalization could pose challenges for usability and adoption.

Privacy-Utility Trade-offs: Personalizing location anonymization may involve tradeoffs between privacy protection and data utility, as stricter anonymization measures could impact the accuracy and usefulness of location-based services for individual users. **13) P. Kalnis, G. Ghinita, K. Mouratidis,**

and D. Papadias, "Preventing locationbased identity inference in anonymous spatial queries," IEEE Transactions on Knowledge and Data Engineering, vol.

19, no. 12, pp. 1719–1733, 2007.

Kalnis et al. focus on preventing locationbased identity inference in anonymous spatial queries. The paper presents techniques for enhancing the privacy of spatial queries by preventing adversaries from inferring sensitive information about users' identities. The paper introduces algorithms for anonymizing spatial queries to prevent identity inference, including query transformation, result perturbation, and access control mechanisms. By obscuring the relationship between spatial queries and user identities, the proposed techniques aim to protect

user privacy in spatial data analysis. Performance Overhead: Applying anonymization techniques to spatial queries may introduce additional computational overhead and latency, potentially impacting the responsiveness and scalability of spatial data processing systems. Vulnerability to Inference Attacks: Adversaries may still attempt to infer sensitive information about users' identities from anonymized spatial queries by analyzing query patterns, access patterns, or auxiliary information. Protecting against inference attacks requires ongoing evaluation and refinement of privacy safeguards.

14) Y. Wang, D. Xu, X. He, C. Zhang, F. Li, and B. Xu, "L2p2: Location-aware location privacy protection for locationbased services." in IEEE INFOCOM

2012.

Wang et al. present L2p2, a location-aware location privacy protection framework for location-based services (LBS). The paper introduces techniques for enhancing location privacy while preserving the functionality and usability of LBS applications. The paper proposes algorithms for dynamically adjusting location privacy levels based on users' preferences, context, and privacy requirements. By integrating location-aware privacy mechanisms into LBS applications, L2p2 aims to provide fine-grained control over location privacy and minimize the risk of privacy breaches. Adoption Challenges: Integrating L2p2 into existing LBS applications may require modifications to software systems, user interfaces, and backend infrastructure, posing challenges for adoption and compatibility. Usability Considerations: Balancing location privacy with the usability and functionality of LBS applications requires careful design and implementation of user interfaces, privacy settings, and interaction mechanisms. Ensuring a seamless user experience while maximizing privacy protection may be challenging.

15) C. Chow, M. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based service," in Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems, 2006, pp. 171–178.

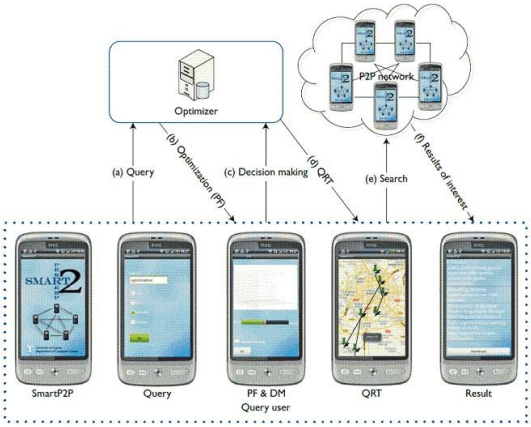
Chow, Mokbel, and Liu introduce a peer-topeer spatial cloaking algorithm for anonymous location-based services (LBS). The paper presents techniques for aggregating and anonymizing location information in a decentralized manner to protect user privacy. The paper proposes algorithms for forming groups of nearby users (peers) and aggregating their location information into cloaking regions. By cloaking individual user locations within these regions, the proposed approach aims to prevent unauthorized access to sensitive location information while enabling effective query processing in LBS applications. Scalability Concerns: The effectiveness and efficiency of the peer-topeer spatial cloaking algorithm may degrade in large-scale LBS deployments with a high volume of users, as the overhead of group formation and maintenance increases. Trade-offs with Query Accuracy: Aggregating location information into cloaking regions may introduce inaccuracies in query results, especially in scenarios where precise location information is required for meaningful interactions. Balancing location privacy with query accuracy remains a challenge.

III. Methodology

In this phase of the project, our focus revolves around introducing innovative protocols aimed at endowing location publishers with the ability to exercise meticulous control over who can access specific location information. This entails devising access control policies that allow for nuanced permissions, tailoring the disclosure of location data based on intricate relationships and contextual parameters. To illustrate, consider the following scenarios: (1) a user may be permitted to discern the city in which the publisher is located if they are listed as a friend; (2) another user, identified as a classmate, might be granted the privilege to ascertain whether the distance between themselves and the publisher falls within a designated radius of 100 meters; (3) yet another user, sharing a common university affiliation, could be authorized to compute the precise distance between them and the publisher. At the crux of our methodology lies the integration of Functional Encryption, an encryption paradigm that diverges markedly from traditional schemes by enabling key holders to discern specific functions of encrypted data while remaining oblivious to other facets of the data. This paradigm shift constitutes a pivotal departure from conventional encryption techniques, wherein decryption is typically uniform across all

recipients. Functional Encryption affords unparalleled flexibility, permitting fine-grained control over the access and utilization of encrypted data based on predefined functions. Delving deeper into the architectural framework, our methodology entails the orchestration of a sophisticated infrastructure designed to facilitate the implementation and operation of the proposed protocols. Central to this architecture is the deployment of cryptographic primitives and protocols tailored to the demands of Fine-grained Access Control (FGAC) in the context of location-based data. These cryptographic tools serve as the bedrock upon which the access control policies are enforced, ensuring that only authorized parties are granted access to specific facets of location information. Furthermore, our architecture incorporates mechanisms for key management and distribution, essential components in the realization of Functional Encryption-based access control. Robust key management protocols ensure the secure generation, distribution, and revocation of keys, safeguarding against unauthorized access and cryptographic attacks. Additionally, the architecture encompasses components responsible for policy enforcement and evaluation, dynamically assessing incoming access requests against predefined policies to ascertain their adherence to stipulated access control criteria. In essence, our methodology represents a holistic approach to addressing the complex challenges inherent in preserving location privacy while enabling utility from location-based data. By leveraging Functional Encryption and designing intricate access control policies, our protocols empower location publishers with unprecedented control over the dissemination of location information, striking a delicate balance between privacy preservation and utility optimization. Through meticulous architectural design and cryptographic underpinnings, our methodology lays the groundwork for a robust and scalable solution to the multifaceted challenges posed by finegrained access control in the realm of location-based services.

Architecture:



IV. Implementation

In this phase of our project, we aim to develop novel protocols to enable finegrained access control over location information. The primary objective is to empower location publishers with the ability to specify detailed access control policies, dictating precisely who can access which aspects of their location data. Our methodology revolves around the integration of Functional Encryption, a cutting-edge encryption paradigm that enables key holders to extract specific functions of encrypted data while remaining oblivious to the underlying information. Unlike traditional encryption schemes, Functional Encryption allows for differentiated decryption, where key holders can only learn specific functions of the data. At the heart of our approach lies the architectural framework designed to support the implementation of our proposed protocols. This framework encompasses various components, including cryptographic primitives and protocols tailored to facilitate Fine-grained Access Control (FGAC) in the context of locationbased data.

Key elements of our methodology include:

Fine-Grained Access Control: Our protocol allows users to specify a condition instead of a group and exert access control over the users who satisfy this condition. This is more scalable since users can simply add a new

condition for new privacy setting instead of hand-picking hundreds of users to form a new group. Also, this is more userfriendly because users themselves do not clearly know which of their friends should or should not access the information most of time.

Multi-leveled Access Control: The protocol also supports semi-functional encryption. That is, the protocol enables users to control to what extent (or level) others can learn his location. The lowest level corresponds to nothing, and the highest level corresponds to one's exact location. Levels between them correspond to indirect information about one's location. **Privacy-Preserving Protocol:** In our protocol, every location information is encrypted and queries are processed upon ciphertexts. Therefore, a location publisher's friends learn nothing but the result of the location query, which is under the location publisher's control. In addition, since every location is encrypted, even the server who stores location information does not learn anything from the ciphertext. **Euclidean distance:** For simplicity, we assume the ground surface is a plane, and every user's location is mapped to an Euclidean space with integer coordinates (with meter as unit). That is, everyone's location can be expressed as a tuple of coordinates representing a point in a grid partition of the space. This does not affect the generality since there exists a bijection between spherical locations and Euclidean locations. By approximating the coordinates in the Euclidean space to the nearest grid point, we can show that it results in errors of the Euclidean distance between two locations at most $\sqrt{2}$ meters when the space is partitioned using grid of side-length 1 meter.

The Euclidean distance between two users with locations **x**1 = (d1, d2) and **x**2 = (d3, d2) is double xDiff = d1-d3; double xSqr = Math.pow(xDiff, 2); double yDiff = d2-d4; double ySqr = Math.pow(yDiff, 2); double output = Math.sqrt(xSqr + ySqr).

V. Results

The implementation of PLQP yields a notable enhancement in safeguarding personal privacy within Location-Based Services (LBS). Users benefit from increased control and confidence in managing their location information. And effectiveness in protecting user privacy within LBS.

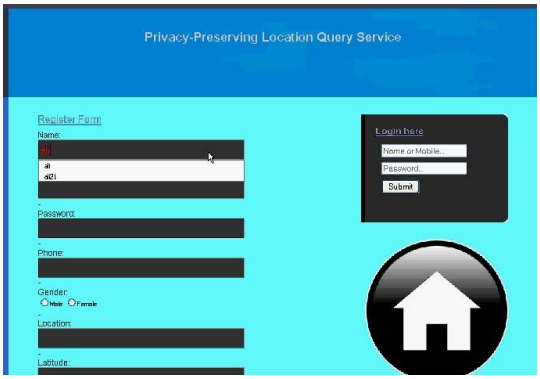


Fig 1: The Registration and Login Page ensures secure access to the platform.

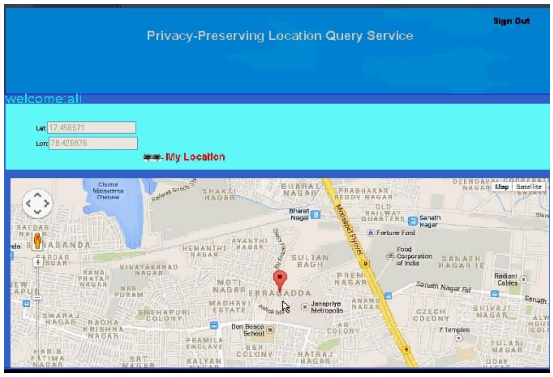


Fig 2: The User Home Page provides a user-friendly interface for accessing LBS functionalities.

Fig 3: The Find Nearby Friends feature enables users to locate friends while preserving privacy.

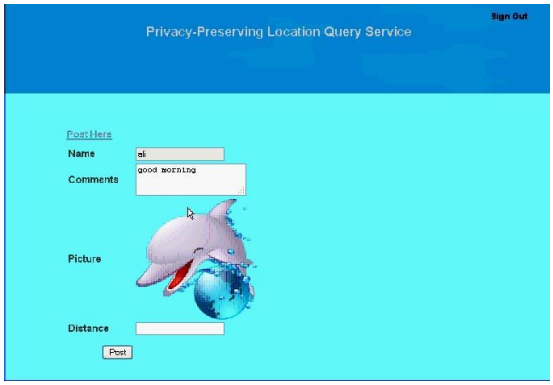


Fig 4: The Send Post functionality allows users to share updates without compromising location privacy.

Each figure illustrates key aspects of

PLQP's usability

VI. Conclusion

Our project introduces the Privacypreserving Location Query Protocol (PLQP), addressing privacy concerns in existing Location-Based Services (LBS) by enabling fine-grained access control. PLQP utilizes a novel distance computation and comparison protocol to implement semifunctional encryption, supporting multilevel access control. Additionally, CP-ABE is employed to enhance access control granularity. Through experimental evaluation, our protocol demonstrates practical applicability in real mobile networks, ensuring location information confidentiality unless specified otherwise by the publisher.

References

1. T. Hashem and L. Kulik, "Safeguarding location privacy in wireless ad-hoc networks," *Ubicomp 2007: Ubiquitous Computing*, pp. 372–390, 2007.

2. C. Bettini, X. Wang, and S. Jajodia, "Protecting privacy against locationbasedpersonal identification," *Secure Data Management*, pp. 185– 199,2005.

3. M. Mokbel, C. Chow, and W. Aref, "The new casper: query processingfor location services without compromising privacy," in *Proceedings of the 32nd international conference on Very large data bases*, VLDB Endowment, 2006, pp. 763–774.

4. K. Vu, R. Zheng, and J. Gao, "Efficient algorithms for k-anonymouslocation privacy in participatory sensing." in *IEEE INFOCOM*, 2012.

5. L. Sweeney *et al.*, "k-anonymity: A model for protecting privacy,"*International Journal of Uncertainty Fuzziness and Knowledge Based Systems*, vol. 10, no. 5, pp. 557– 570, 2002.

6. H. Zang and J. Bolot, “Anonymization of location data does not work:A largescale measurement study,” in *Proceedings of the 17th annual international conference on Mobile computing and networking*, 2011,pp. 145–156.

7. H. Kido, Y. Yanagisawa, and T. Satoh, “Protection of location privacy using dummies for location-based services,” in *21st International Conferenceon Data Engineering Workshops, 2005*, pp. 1248–1248.

8. Beresford and F. Stajano, “Mix zones: User privacy in location-awareservices,” in *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004*, pp. 127–131.

9. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J. Herrera, A. Bayen,M. Annavaram, and Q. Jacobson, “Virtual trip lines for distributed privacypreserving traffic monitoring,” in *Proceeding of the 6th internationalconference on Mobile systems, applications, and services*, ACM, 2008, pp. 15–28.

10. M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, “Swing &swap: usercentric approaches towards maximizing location privacy,” in *Proceedings of the 5th ACM workshop on Privacy in electronic society*,2006, pp. 19–28.

11. X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, “Traffic-awaremultiple mix zone placement for protecting location privacy.” in *IEEE INFOCOM 2012*.

12. B. Gedik and L. Liu, “Location privacy in mobile systems: A personalized anonymization model,” in*Proceedings of 25th IEEE InternationalConference on Distributed Computing Systems, 2005*, pp. 620–629.

13. P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventinglocationbased identity inference in anonymous spatial queries,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, no. 12, pp.1719–1733, 2007.

14. Y. Wang, D. Xu, X. He, C. Zhang, F. Li, and B. Xu, “L2p2: Locationawarelocation privacy protection for location-based services.” in *IEEE INFOCOM 2012*.

15. C. Chow, M. Mokbel, and X. Liu, “A peer-to-peer spatial cloaking algorithm for anonymous location-based service,” in *Proceedings of the 14th annual ACM international symposium on Advances in geographicinformation systems*, 2006, pp. 171–178.