A Privacy Protection Mechanism for Mobile Online Social Networks

Dr.C.K.Gomathy[1], Y.Saranya[2], G.Vanisree[3], N.Yaswanthi[4]

[1]Assistant professor, Department of CSE, SCSVMV University, Enathur, Kanchipuram, India
[2,3,4]U.G Scholar, Department of CSE, SCSVMV University, Enathur, Kanchipuram, India

Abstract**—***A Location sharing system is the most critical component in mobile online social networks (MOSNS).Huge number of user's location information will be stored by the service providers. In addition to the location privacy and social network privacy cannot be guaranteed to the user in the earlier work. Regarding the enhanced privacy against the inside attacker implemented by the service provider in (MOSNS), we initiate a new architecture with multiple servers .It introduces a protected solution which supports a location sharing among friends and strangers. The user friend set in each query is submitted to the location server it divides into multiple subset by the location server. If the user makes a query to the server the data can be retrieved only for the registered users instead of all. We use Three Layer of Security likely, High, Medium and Low for the Privacy implementation. Simultaneously with a location sharing it offers check ability of the searching results reoccurred from the servers. We also prove that the new construction is safe under the stronger security model with enhanced privacy.*

Keywords**—*****Privacy location, Check-ability, Insider threats, Mobile social networks.***

I. INTRODUCTION

A spatial keyword query integrates location and text search. With the arrival of mobile computing, social networks have moderately become new model called MOSNS. Taking a location and a set of keywords as arguments, such queries return relevant spatial web objects that match the arguments. A moving top-k spatial keyword (MKSK) query which takes into account all the time moving query locality enables a mobile client to be always aware of the top-k spatial web items that best match a query with significance to location and text relevance, and it has numerous mobile uses. For example, a mobile user may activate a "cafe" query in organize to be alerted about nearby opportunities for a cup of coffee. With the MkSK query, a user always has a new result as the client moves. A easy solution to the MkSK query is to next to invoke an existing snapshot spatial keyword query processing method. However, this approach has the problem that even if snapshot queries are processed very frequently, which is costly and wasteful because consecutive results are likely to be very similar, there is no assurance that the user forever has the right, up-to-date result. Another feasible solution is to extend a buffering technique for spatial kNN query processing to top-k spatial keyword querying.

II. RELATED WORK

Obfuscation is an important technique for defending an individual's location privacy within a pervasive computing environment. This structure provides a computationally resourceful mechanism for balancing an individual's need for high-quality information services closest to that individual's need for location privacy. Negotiation is used to make sure that a location-based service provider receives only the information it requests to know in order to give a service of ample quality. The outcome of this work have implications for several applications of mobile and location-aware systems, as they give a innovative conceptual foundation for addressing the privacy concerns that are approved to be retarding the widespread recognition and use of location-based services. Recently, highly accurate positioning devices allow us to provide different types of location-based services. On the second hand, because such position data consist of deeply personal information, the security of location privacy is one of the most important problems in location-based services. we propose an anonymous announcement technique to protect the position privacy of the users of location-based services. In our future technique, such users generate a number of false position data (dummies) to initiate service providers with the exact location data of users. Because service providers cannot choose the correct position data, user location privacy is protected. We also describe a price reduction technique for communication between a client and a server.

III. METHODOLOGY

A direct additional solution to the MkSK query is to periodically call upon an existing snapshot spatial keyword query processing technique. a efficiently authenticate moving top-k spatial new authenticated data structure, the MIR-tree to, keyword query results, thus guaranteeing the soundness and completeness of both a top-k result and its corresponding safe zone The most important features of Longitude are that the location allocation provider only processes encrypted locations that it unable to decrypt, supports different granularities of locations for different receivers and low key management, computation and communication overheads. Depending on the spatiotemporal big data analysis the information will be processed and retrieved using the Hadoop framework. This study shows that sharing anonymized location data will likely lead to privacy risks and that, at a mini- mum, the data needs to be coarse in either the time domain or space domain. We propose two polynomial-time approximate inference algorithms and we extensively evaluate their performance on a real dataset.

IV. TECHNIQUES FOR LOCATION PRIVACY IN MOBILE SERVICE

In the implemented technique, Android and Cloud Computing are integrated. The modifications is made to have the privacy of the users location in which query is requested. Three Layers of High, Medium and Low are implemented for security purpose of location privacy. The wireless network is focused with the relational data and the spatial databases.

1. User Registration
2. User Authentication
3. User’s location identification
4. Safe Region Manipulation
5. Query request to the cloud server
6. Find the nearest location.

4.1. User Registration

In location query system the user have to be enrolled for his next query search. If the user is not enrolled then the user can’t access the clocking agent. For register the user should give his details such as name, locality, age, gender, etc. once a user is registered with his details he can access information from the server .Every single user will have separate user name and password.

4.2. User Authentication

If a client wants to raise a query, first the user must login with his username and password. After the user gets login he can raise a query to the server. This query will go to the clocking agent and send the query to the cloud server.

4.3. User’s location identification

The clocking agent will find the user location and then it will check the user is moving towards the location or moving outwards the location. The present location is obtained using GPS from the mobile phone user. The mobile user will carry with the GPS for fetching the longitude & latitude values. These values are obtained by means of satellite communication. So once the user sends the query to the clocking agent. The clocking agent will get the exact location of the user via GPS values of the user.

4.4. Safe Region manipulation

Every time a clocking agent receives a query from the client and then it will checks the query and find the safe region for the client. Safe region is intended from the exact user location. First we have to retrieve the direction of the user. If the direction of the user is towards ahead then the clocking agent will estimate the safe region with admiration to the main location. For example user sends a request from Enathur, user is moving towards kanchipuram, then the Safe region kanchipuram, if the user is moving in the opposite direction then the clocking agent wish to specify the safe region as Chennai .After finding the safe region the clocking agent ask the request to the Cloud server. The Cloud server will send the result for the safe region to the clocking agent and obtain the result from the Cloud server and find the nearby Location from the result and send the location to the client. The clocking agent and send the query to the cloud server.

4.5. Query Request to the Cloud Server

The Clocking agent handle the Safe region for the client and send the query to the Cloud server. The Cloud server analyze the Query and fetch the results according to the safe region and then send the result to the clocking agent. If the user is requested for ATM Bank from Enathur, first the query is sent to the Clocking Agent. Cloaking agent will manipulate the safe region as kanchipuram, and then the query is forwarded to the Cloud Server.

4.6. Find the Nearest Location

After getting the query result from the Cloud server, the clocking server will filter the results in accordance to the user exact location. The Cloud server will retrieve the bank information or ATM which location is nearest to the user in accordance to Enathur to the cloaking agent. But the cloaking agent knows user is in Enathur. So the cloaking agent will apply KNN Query Algorithm to fetch the nearest ATM or bank in accordance to Enathur. So user will be receiving the exact information, as requested but then the user's Location Privacy is still maintained, because the Cloud server will update in its table as the query is from Chennai not from Enathur. By this way we ensure Privacy in the user's location.

V. ARCHITECTURE OF LOCATION SHARING MOSNS

Mobile users gradually report on their co-locations with other users, in addition to revealing their locations to online services. For instance, they tag the names of the associates they are with, in the messages and in the pictures they post on public networking websites.

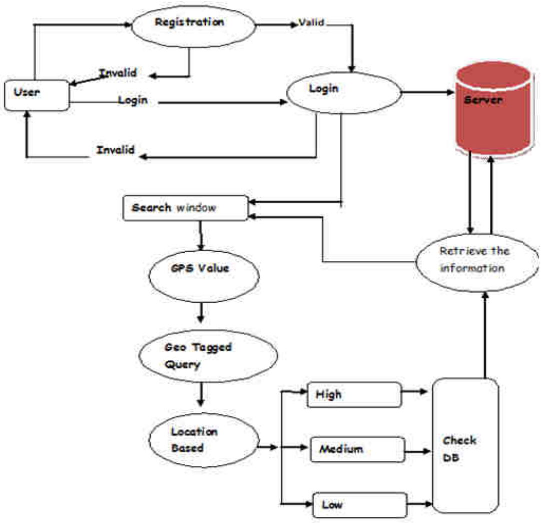
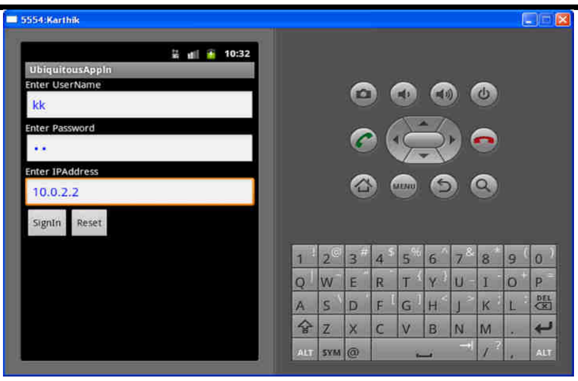


Fig.1:.Location sharing schemes in mobile

VI. RESULT

This work proved to provide a clear review of methods by which privacy protection may take place at levels of technology and management. so a better perceptive of how a complete approach to privacy protection may take place. It is hoped that this effort will result in a clearer understanding of ways in which privacy protection efforts should address the related concepts of technology and practice to effectively minimize the risk of privacy harm.


5554:Karthik

UbiquitousAppIn

Enter UserName: kk

Enter Password: ••

Enter IPAddress: 10.0.2.2

Fig.2: *privacy protection for user's location.*

Combined with (possibly obfuscated) location information, such co-locations can be used to look up the inference of the users' locations, thus further threatening their location privacy, as co-location information is taken into account, not only a user's reported locations and mobility patterns can be used to localize the user locations.

VII. CONCLUSION

In this paper work it proposes a new authenticated data structure, the MIR-tree, to efficiently authenticate moving top-k spatial keywords query results, thus guaranteeing the soundness and completeness of both a top-k result and its corresponding safe zone. A verification object for authenticating the top-k results and safe zones of MkSK queries is designed. Algorithms for constructing and using verification objects for verifying the top-k results and safe zones are developed. An enhancement of the MIR-tree, the MIR_-tree, is proposed to further reduce the communication cost. Extensive empirical studies on real data sets demonstrate that the proposed approaches are capable of outperforming two baseline algorithms that utilize existing techniques by orders of magnitude. It gives a new preserving location sharing privacy called Longitude. The most important features of Longitude are that the location sharing provider only processes encrypted locations that it unable to decrypt, supports unusual granularities of locations for different receivers, and low key management, computation and communication overheads. One type of privacy policy which has proven to be useful in location sharing services is discriminating location-based policies.

REFERENCES

[1] Jin Li, Hongyang Yan, Zheli Liu, Xiaofeng Chen, Xinyi Huang and Duncan S.Wong.

[2] Z. Liu, D. Luo, J. Li, X. Chen, and C. Jia, "N-Mobishare: New privacy preserving Location-sharing

system for mobile online social networks," Int. J. Comput. Math., 2014.

[3] W. Cheng and K.-L. Tan, "Query assurance verification for outsourced multi-dimensional databases," J. Compute. Security, vol. 17, no. 1, pp. 101–126, 2009.

[4] R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in Information Theoretic Security, ser. ser. Lecture Notes in Computer Science, A. Smith, Ed. Berlin Germany: Springer-Verlag,2012, vol. 7412, pp. 37–61.

[5] C.K.Gomathy and S.Rajalakshmi "A Business intelligence Network design for service oriented architecture," International journal of engineering trends and technology, vol. 9, no. 3, pp. 151–154, march 2014.

[6] G. Cong, C. S. Jensen, and D. Wu , "Efficient retrieval of the top-k most relevant spatial web objects," Proc. VLDB Endowment, vol. 2, no. 1, pp. 337–348, 2009.

[7] A. Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy," in Proc.SSTD, 2007, pp. 239–257.

[8] Y.-Y. Chen, T. Suel, and A. Markowitz, "Efficient query processing in geographic web search engines," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2006, pp. 277–288.

[9] H. Kido, Y. Yanagisawa, and T. Satoh, "Protection of location privacy using dummies for location-based services," in Proc. 21st Int. Conf. DataEng. Workshops, 2005, p. 1248.

[10] T.Brinkhoff, "A framework for generating network-based moving objects," Geoinformatica, vol. 6, no. 2, pp. 153–180, 2002.