International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-3, June 2015
ISSN: 2395-3470
www.ijseas.com

Secure mobile mining with location privacy control

V Vijay[1], P Saravanan M.E[2]
[1] PG Student, [2]Assistant Professor, Department of Computer Science and Engineering,
PTR College of Engineering and Technology, Tamilnadu, (India)

ABSTRACT

Now-a-days mobile technology rules the world and people consume everything with the mobile application. But the hidden fact is there is serious drawback of privacy breach on those geosocial applications. A well known geosocial application is foursquare in which huge amount of peoples communicates with their surrounding but there is a maximum possibility of misused such as tracking the user. In this paper we proposed a Location based methodology in concentrating the user's privacy such access from unauthorized users or tracking the user location. Generally user's forms a community and share their secrets as well as transformation, even though server track location by the queries our proposed application guarantee the privacy can't be shared by the unauthorized users. And it also shows the geo locations were the tracing is happening and secure transmission by means of cryptography in a most convenient manner as suitable for all mobile devices currently in used.

Keywords: Location-based social application, location transformation, location privacy, security, efficiency

INTRODUCTION

Technologies becomes trendy peoples use smart phones application offered by androids and i-phones for downloading as well as data transformation purposes. And mobile technology is the dominant technology with an emerging concept of geosocial application in developing GPS location services for enabling social network around the world. In which geo networking is a method of establishing network connection who is match with certain attributes like interest, local people, etc by means of IP based services. The enormous growth and usage is mainly due its advantages like by means of location they can easily find the nearby shopping mall or places as they required. In this analyze the location transformation needs to concern in an effective manner; by means of mobile network moving from one location to another it can make the possibility of unauthorized user to track the user information. The another major thing is to be discussed is security, due to the transparency of the technology the user sharing the secrets can possibly tracked by the hacker. Next thing is the location privacy it is still in developing stage how maintains the user location privacy in efficient manner.

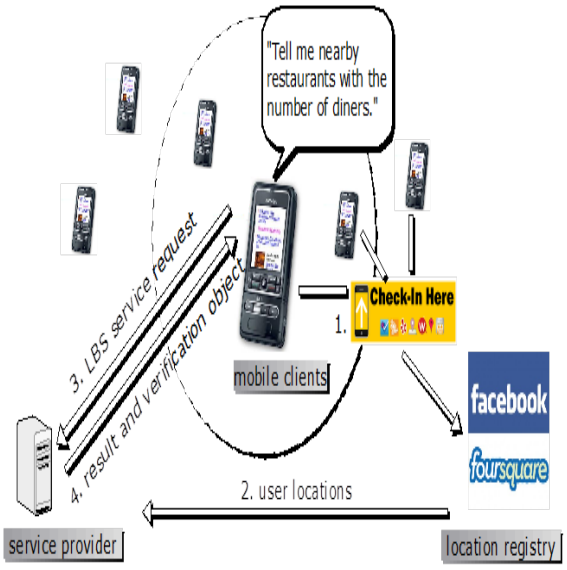

Fig 1 Location based service

In the fig1 shows generally how the location based services are generally processed. In this foursquare is famous application user for local search and discovery services for entertainment places in your area based on the mobile location. In which the user with their social network members are searching a centralized restaurant in their area. By means of the application location based service request is sent to the service provider and those providers sent the result with the verifications code. The increased usage of mobile application and major privacy drawback behind those technologies grabs the attention among the researchers in improving the security terms in a well manner. And the related works based on these fields were discussed in the below section.

RELATED WORKS:

On discussing about the location based services there are three categories on providing location privacy such as firstly spatial temporal and cloaking [1] [2] [3] [4] [5]. On these work instead of values an approximate location and time is communicated to the user. In these works the privacy is improved by hiding the user location among the anonymity but the simple mechanism is easily attacked by the unauthorized users on the spatial temporal. Then the cloaking can be achieved by the mechanism of Pseudonyms and silent times [6], [7] in which the device identifiers are frequently changed that does not supports frequent transmission for a long periods at regular intervals. The next category is location transformation in which the major issue is neighbor by user query enables to find the accurate user locations. According to Blind evaluation using Hilbert Curves [8] only approximate neighbors only can be possible. In addition to it the nearest neighbor queries and the trusted third parties influence in performing the location transformation between the server with the user were discussed on [9] [10]. The third category on this is work based on PIR in providing a strong location privacy by using special hardware's [11] [12]. Among these the resistant against attacks by means of monitoring continuous queries where discussed on [13] [14]. Some of the popular applications based on the location information's are social rendezvous [15], local friend recommendations for dining and shopping [16], [17] The networking services for games and explosive popularity of mobile social networks such as SCVNGR [18] [19] [20]. But the general fact on these applications are increased the risk on maintaining the personal privacy. An analysis on [21] [22] [23] shows on real world examinations the location information's were mainly misused for the purpose for economic gain, physical stalking and to gather legal evidence. Another challenging issue of data security was discussed by Persona [24] and Adeona [25] they are depends on encryption. The server stored all the user location in order to protect the data Persona in his work focused on privacy in online social networks, and Adeona deals the term of privacy by using the tracking device system by means of these is no data sharing among users. But these encryption techniques are successful among the user in retrieving own data, but not the data from her friends.

EXISTING SYSTEM

In the existing system the privacy in geosocial system is maintained by the trusted servers based on applying the anonymization to user identities and private data, using PIR private information retrieval technique. However the design mechanism protects user privacy effectively by means of

cryptography it does not supports the system accuracy. It raises the trustworthiness among the server by means of assuming the intermediates that can be compromised and, therefore, are un-trusted. Generally there are two types of queries required for supporting the functionality of geosocial application such as point queries and nearest neighbor queries. In which the point query is for determining the user location and another one for locating the nearest. But in those existing systems there is no way in hiding the user location. In another aspect all the user locations and user networks locations are stored in the server database. There is maximum possibility in accessing of those databases by the hackers. In which the three categories providing location privacy in general LBSs that do not specifically targeted on social applications in an effective manner. Moreover the enhancement of security system by means of cryptography is not prominent to the real time scenario as it was easily predicted by the unauthorized user. There is no encryptions are available for latitude and longitude which make more simple in tracking the user location.

PROPOSED SYSTEM

As discussed above in order to solve the location privacy problem in the geosocial application, a mobile application is developed which encrypt the location of the user and stored in the service provider. Even though the hackers access the server the user location is preserved. In detail, an application is developed to be used within the organization. In which the user along with the network get authorized and able to share the information within the limit. If any other user outside the limit is entering by means connecting with server our proposed mechanism able to monitor them and their location is also can be traced in an effective manner. A fair thing with our proposed system is it can be applicable to most of all mobile application and simple to import as well as maintenance. To enable our proposed system more prominent, we introduced an enhanced encryption mechanism such as Advanced Encryption Standard (AES) to maintain the privacy in data storage. The AES mechanism is explained in implementation section.

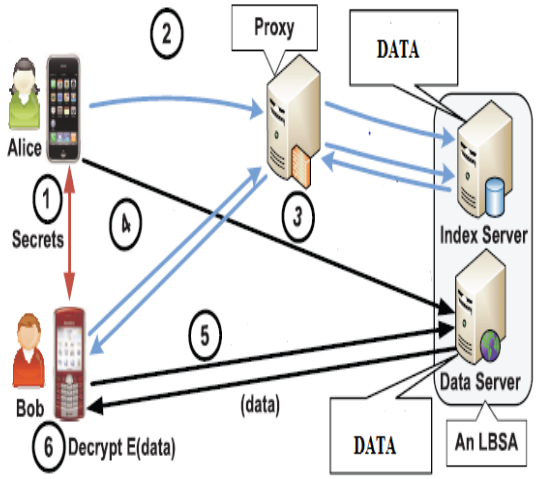

Fig 2: Data storage system using proposed methodology

As explain the fig 2 shows the user is connected with the network and those data's are stored in index server and shared by the data server in which the proxy is act as the mediator. The secrets between both the user can be shared by assuring their location in data server and the data is communicate to the other end user in encrypted form . By which the original data is decrypted by the authorized user who has the key which originally shared by the sender. This way ensures the location as well as data privacy in a secured manner within the network.

IMPLEMENTATION METHODOLOGY

In the section we discuss about the development of proposed application using net bean framework in a java platform along with the working methodology. Before starting the application is targeted to be based on education institution in sharing the staff progress and those activities were monitored by the admin.

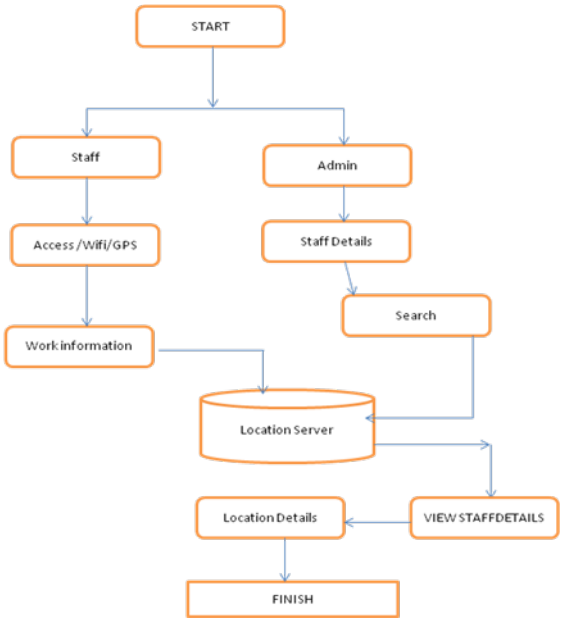

Fig 3: Proposed Framework design

Location Updater: The application is developed in such a manner it is connected to wifi and a network connection is established within the organization. The location updater in the application furnishes the user location at regular interval which was stored in the server in a encrypted form. If a request is sent to the location service it response by means of currently-available location providers such as WiFi and GPS. In this method certain rules are generated in order to restrict the unauthorized users and protect from violation behaviors attempt by the users.

Location transformation: By means the changing the user location the degree values can vary and fake location data is used. These fake locations are effective for those affecting the accuracy and frequency affected by the location permissions you've requested and the parameters you pass to Location Services with the request.

Security: In this mechanism the user who wants to share their location initially need to enter their No and the corresponding secret key for that user name. Then the server stores those details, so if anyone wants to access the other location only if the secret key match with the server otherwise the anonymous behavior is traced and tracked by the admin. In this we use AES algorithm for storing the transform location and it's a 128 bit block process the steps behind the algorithm is state's below;

- Initially the set of round keys were derive from the cipher key.
- The state array is initialized with the block data (plaintext).
- The initial round key is then added to the starting state array.
- A nine rounds of state manipulation is performed
- Next the tenth and final round of state manipulation is processed.
- Copy the final state array out as the encrypted data (cipher text)

RESULT AND DISCUSSION

International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-3, June 2015
ISSN: 2395-3470
www.ijseas.com

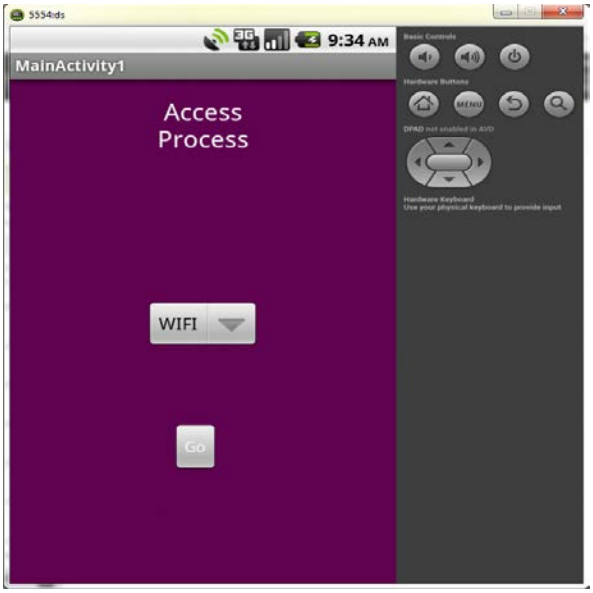

Fig 4: Connection establishing

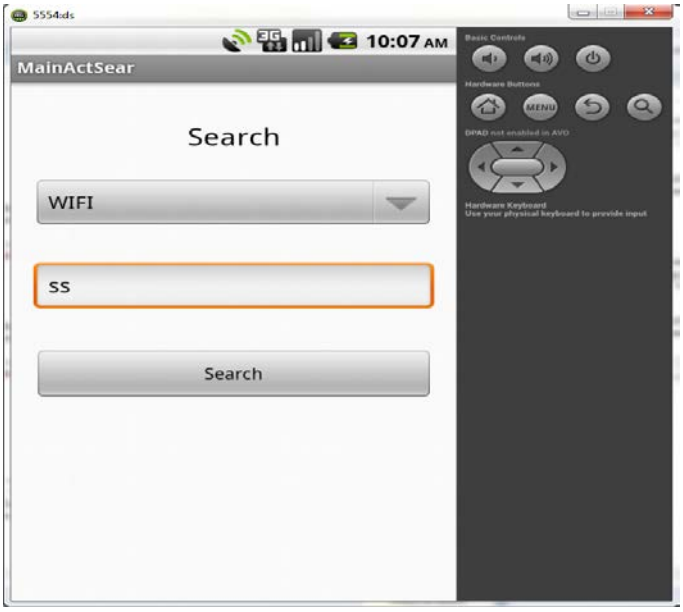

Fig 6: Searching by staff ID

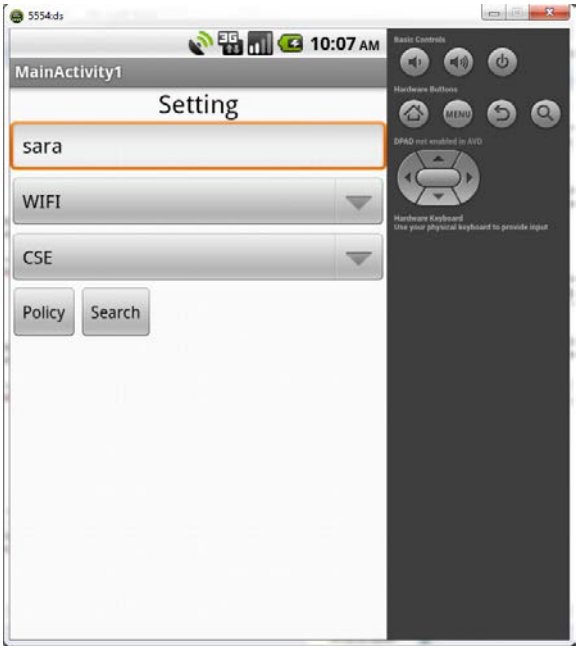

Fig 5: User information with policy

Fig 7: Admin Process

From fig 4 & 5 it shows the application is started and the initial stage of user entering their details with accepting the policy. Here choosing the service provide WIFI which is shown on the result. The user information contains details about staff, their college etc. Then those data were updated to the process.

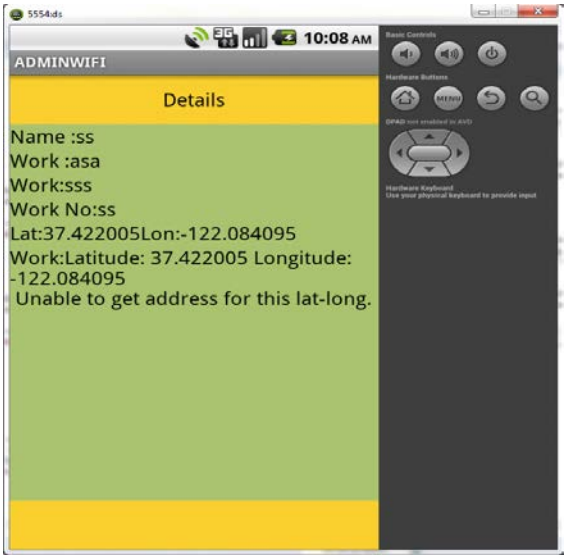

Fig 8: Shared result

Once all the staff details are enters a well formed network is connected by means of wifi. If a user wants to access the location of another user within the range he can select the user by giving the ID as shown in fig 6. Meanwhile the admin undergoes checking the secret key and validate the user. If the key matches the original data is decrypted and shared to the requested user as shown in fig 8. Otherwise the admin monitor the unauthorized user and its location is tracked, preventive measures were taken by the admin. Thus achieving the security along with location privacy with accurate and location frequencies.

CONCLUSION

In this paper the drawback of location based system using existing approach were discussed and those are overcome by our propose design along with prototype implementation. The achieved results justifies the preserving the location privacy of the user in location based social application on trusted server with effective encryption mechanism suitable multiple mobiles. The location transform creates a fake location which makes the unauthorized user to difficult in convincing the policy and the encryption enables in tracking those unauthorized user from accessing the stored data in the server. The simple mechanism and overall performance states the proposed system is more suitable for both synthetic and real-world LBSA traces when compared to the existing methods.

REFERENCE

1) M. Gruteser and D. Grunwald, “Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking,” Proc. First Int’l Conf. Mobile Systems, Applications Services, 2003.
2) M.F. Mokbel, C.-Y. Chow, and W.G. Aref, “The New Casper: A Privacy-Aware Location-Based Database Server,” Proc. IEEE 23rd Int’l Conf. Data Eng., 2007.
3) B. Gedik and L. Liu, “Location Privacy in Mobile Systems: A Personalized Anonymization Model,” Proc. IEEE 25th Int’l Conf. Distributed Computing Systems, 2005.
4) P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing Location-Based Identity Inference in Anonymous Spatial Queries,” IEEE Trans. Knowledge Data Eng., vol. 19, no. 12, pp. 1719-1733, Dec. 2007.
5) G. Ghinita, P. Kalnis, and S. Skiadopoulos, “PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems,” Proc. 16th Int’l Conf. World Wide Web, 2007.
6) A. Beresford and F. Stajano, “Mix Zones: User Privacy in Location-Aware Services,” Proc. IEEE Second Ann. Conf. Pervasive Computing Comm. Workshop, 2004.

7) T. Jiang, H.J. Wang, and Y.-C. Hu, "Preserving Location Privacy in Wireless Lans," Proc. Fifth Int'l Conf. Mobile Systems, Applications Services, 2007.
8) A. Khoshgozaran and C. Shahabi, "Blind Evaluation of Nearest Neighbor Queries Using Space Transformation to Preserve Location Privacy," Proc. 10th Int'l Conf. Advances Spatial Temporal Databases, 2007.
9) M.L. Yiu, C.S. Jensen, X. Huang, and H. Lu, "Spacetwist: Managing the Trade-Offs among Location Privacy Query Performance and Query Accuracy in Mobile Services," Proc. IEEE 24th Int'l Conf. Data Eng., 2008.
10) D. Lin, E. Bertino, R. Cheng, and S. Prabhakar, "Position Transformation: A Location Privacy Protection Method for Moving Objects," Proc. Int'l Workshop Security Privacy GIS LBS, 2008.
11) G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private Queries in Location Based Services: Anonymizers Are Not Necessary," Proc. ACM SIGMOD Int'l Conf. Management Data, 2008.
12) S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest Neighbor Search with Strong Location Privacy," Proc. VLDB Endowment, vol. 3, nos. 1/2, pp. 619-629, Sept. 2010.
13) C.-Y. Chow and M.F. Mokbel, "Enabling Private Continuous Queries for Revealed User Locations," Proc. 10th Int'l Conf. Advances Spatial Temporal Databases, pp. 258-275, 2007.
14) E.O. Turgay, T.B. Pedersen, Y. Saygin, E. Savas, and A. Levi, "Disclosure Risks of Distance Preserving Data Transformations," Proc. 20th Int'l Conf. Scientific Statistical Database Management, 2008.
15) M. Motani, V. Srinivasan, and P.S. Nuggehalli, "PeopleNet: Engineering a Wireless Virtual Social Network," Proc. ACM MobiCom, 2005.
16) M. Hendrickson, "The State of Location-Based Social Networking on the iPhone," http://techcrunch.com/2008/09/28/the-state-oflocation- based-social-networking-on-the-iphone, 2008.
17) P. Mohan, V.N. Padmanabhan, and R. Ramjee, "Nericell: Rich Monitoring of Road and Traffic Conditions Using Mobile Smartphones," Proc. Sixth ACM Conf. Embedded Network Sensor Systems, 2008.
18) G. Ananthanarayanan, V.N. Padmanabhan, L. Ravindranath, and C.A. Thekkath, "Combine: Leveraging the Power of Wireless Peers through Collaborative Downloading," Proc. Fifth Int'l Conf. Mobile Systems, Applications Services, 2007.
19) M. Siegler, "Foodspotting is a Location-Based Game that Will Make Your Mouth Water," http://techcrunch.com/2010/03/04/ foodspotting, 2013.
20) B. Schilit, J. Hong, and M. Gruteser, "Wireless Location Privacy Protection," Computer, vol. 36, no. 12, pp. 135-137, Dec. 2003.
21) F. Grace, "Stalker Victims Should Check for GPS," http:// www.cbsnews. com, Feb. 2003.
22) A. Gendar and A. Lisberg, "How Cell Phone Helped Cops Nail Key Murder Suspect. Secret 'Pings' that Gave Bouncer Away," New York Daily News, Mar. 2006.

23) "SCVNGR," http://www.scvngr.com, 2013.
24) R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: An Online Social Network with User Defined Privacy," Proc. ACM SIGCOMM Conf. Data Comm., 2009.
25) T. Ristenpart, G. Maganis, A. Krishnamurthy, and T. Kohno, "Privacy-Preserving Location Tracking of Lost or Stolen Devices: Cryptographic Techniques and Replacing Trusted Third Parties with DHTs," Proc. 17th Conf. Security Symp. (SS '08), 2008.