Privacy Preserving In Location Based Services

Prof.Pragati Chandankhede[1], Mr.Bhavesh Bhanushali[2], Mr.Subhajit Charit[3], Mr.Dipesh Chaudhari[4]
[1, 2, 3, 4]K.C.C.O.E

Abstract- *At the present time, Preserving Privacy of individual in this Developing Modern World is still challenging. With the increase of Location-Enabled Mobile devices and the advances of wireless communication, use of Location Based Services(LBS) has increased which has attracted considerable interest recently. Aiming at this challenges, we have implemented a system, which will secure the Location and Preserve Privacy of User irrespective of Service Provider, who wants to track the user by sending notification messages. Before providing security, User's Location is accessed anonymously and transmitted through unsecured path to the Server. In this system, before sending the location directly to the server, our system will first encrypt the location using LBS Query algorithm and then Outsourced to the server so that the server will be unable to interpret the Location of User. Hence a Registered user can get accurate Services without revealing his/her location information to the LBS Provider and confidentiality of data is preserved.*

Keywords- LBS, Privacy, Service Provider

I. INTRODUCTION

In today's world, location-based services(LBS), such as a map, finding friend, or restaurant finder, can help people enjoy a convenient life and have recently attracted considerable interest. In fact, due to the increase of smart-phones and wireless communications, LBS has been superior in almost all social and business domains, according to the survey, more than 1 billion people have enjoyed LBS in 2013. For example, when a tourist is out of his/her comfort zone, locating some places of interest, such as hotels, restaurants, hospitals, schools, and shops, is much needed. To clearly illustrate the challenges in LBS systems, we consider the following application scenario, where a user may request LBS to find hospitals by exposing his/her location to the LBS provider. However, the LBS provider can infer user's healthy status according to user's information. Therefore, how to design a secure and efficient privacy-preserving query scheme for LBS systems has attracted considerable interest recently, and many research efforts have been dedicated to designing privacy-preserving schemes for LBS. To achieve low computational cost and a convenient data process, LBS providers often outsource their data to a cloud server, which will handle user's LBS queries. In general, since the data is sensitive and private, the LBS User wants to keep the LBS data secret from the cloud server. We are implementing a system to overcome this problems. To use our system first user need to register. Then our system will authenticate the user by verifying OTP which is unique number given to every user and it is send to its registered Emailid. After successful registration, user can use the Location Based Services (LBS).User then search for its query place and wait for reply. On other side Provider can View User Request, View Uploaded Places, Add New Places to the server by selecting from Map. On receiving reply user will connect to user System. User can perform various tasks such as view details of place, find direction to reach that destination.

II. METHODOLOGY

LBS User

In this system, the LBS user sends location-based queries to the LBS provider and receives location-based service from the provider. The user queries the location based service from the provider about the nearest points of interest on the basis of his current location. In general, the user needs to submit his location to the LBS provider which then finds out and returns to the user the requested services. This reveals the user's location to the LBS provider.

LBS Provider

In this system, the LBS provider provides location-based services to the user. LBS allows users to query a service provider in order to retrieve detailed information about points of interest (POIs) in their vicinity (e.g., restaurants,hospitals, etc.). The LBS provider processes queries on the basis of the location of the user. Location information collected from users, knowingly and unknowingly, can reveal far more than just a user's latitude and longitude.

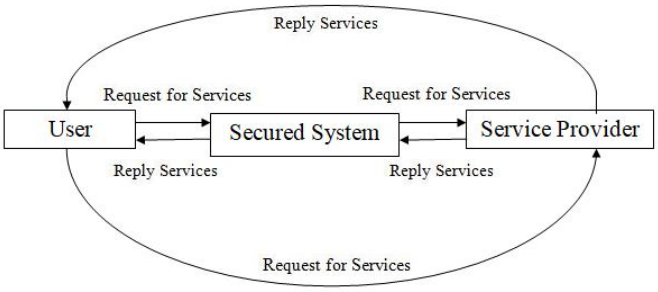

Fig 1: System Architecture

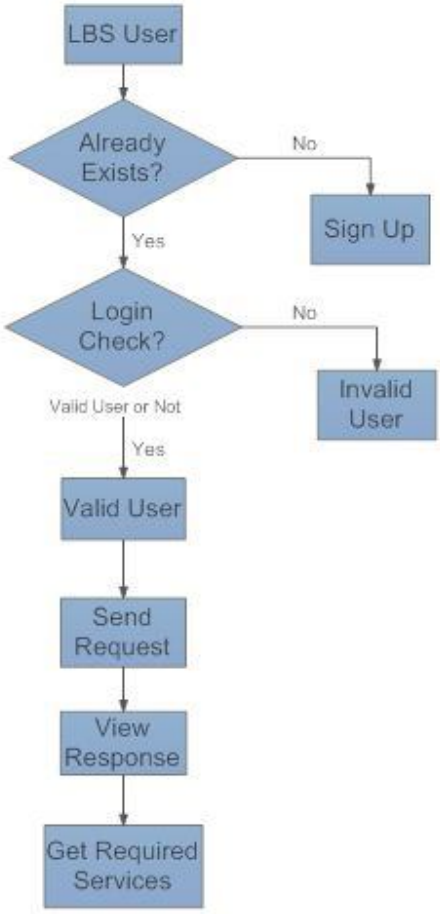

Fig 2.1: System Flowchart of LBS User

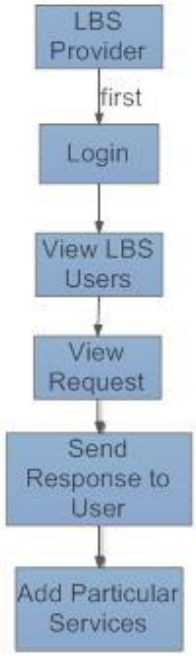

Fig 2.2: System Flowchart of LBS Provider

Module I: LBS User Registration and Authentication

- To use the LBS Services User first need to Register itself.
- LBS User Register itself by entering his/her details such as Name, Email, Contact Number, Location and creates an Username and Password which will be further needed when he/she will login to the system.
- The system assigns an unique User-id to each user which is used to identify each user and stores this User-id along with the user details in the database.
- LBS Provider by logging in to the system can view the information of all users who have registered and in order to authenticate the user, LBS Provider generates an OTP (One time password) which is send to the user's Email .
- If the OTP entered by the LBS User matches with the OTP send by the LBS Provider, then the LBS user gets authenticated and he can requests to the LBS Provider to access the location based services.

Module II: OTP Generate & Send

- OTP Generation is done from Provider Side.
- Provider will generate different 21 length OTP for different User's.
- On clicking generate key option provider calls a method named RandomString()
- This Method randomly select an AlphaNumeric Character (Upper case, Lower case, Number) iteratively 21 times and returns an String(OTP).

- After Successful OTP Generation, Provider send this OTP to the User's Registered Email.
- To Send Email, SMTP Protocol is used.
- Using SMTP & SSL, Provider Send OTP to the User Email through SMTP Authentication.

Module III: Addition of Location Based services by LBS Provider

- LBS Provider has the privilege to add LBS services.
- LBS Provider will select the location from the map and add description to it.
- This description along with the latitude and longitude of the place is stored in the database
- Now, user can request for this newly added service.

Module IV: LBS Query Algorithm

This algorithm is based on shuffling logic.

❖ Sequence Generation:

- Taking Key of Length 9 From user.
- Find ASCII value of each character of Key taken from User.
- Find Unique Digit For each character By Adding The Digits Of That Character and Taking Modulus 9 And Store in an Array "seq".
- If Answer of Step 3 is Already Present in "seq" then Increment It By 1 and Check Again For Same.
- If Character of Key is Repeated then Leave that Character For Future Processing.
- After Completion Of Processing We Fill The Digit Of Remaining Character By Unique Incremental Approach.

❖ Shuffling of actual Location:

- User's actual location is passed to the LBS Query algorithm.
- The sequence generated from the LBS Query algorithm is used to shuffle the location arranged in 9x9 grid.
- This shuffled location is then transferred to the provider.

Module V: LBS Request by User

- After successful login, user can request for LBS services.
- User will fill the required data such as username, Email, location, state, etc. and send the request.
- On receiving response from provider, user perform his desired task.

III. RESULT AND ANALYSIS

❖ Location Capture

- Provider views the user's location in latitude and longitude format in the database when user request for the services.

id	userid	username	mail	latitude	longitude	logindate
29	LBS_2849512	Bhavesh	collegemail4all@gmail.com	19.1799173	72.9801228	2018-03-19
30	LBS_2849512	Bhavesh	collegemail4all@gmail.com	19.1799425	72.9801276	2018-03-19

Fig 3: Location Capture

❖ OTP(One time password) Generation

- OTP is generated from Provider Side.
- Provider generates OTP for different User's.
- On clicking generate key option by provider, anOTP is generated and send to User's Registered Email.

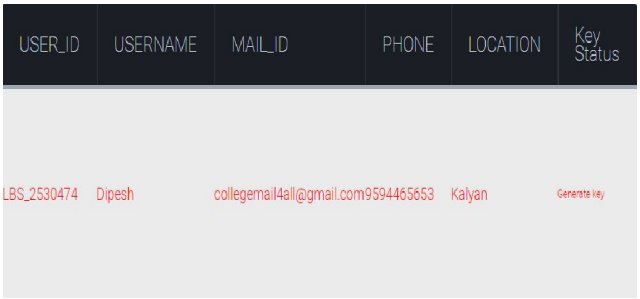

Fig 4: OTP Generation

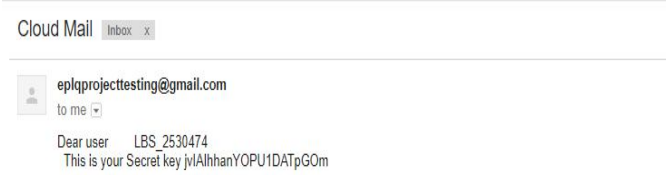

Fig 5: OTP Received

❖ Key Authentication

- In order to authenticate the user, LBS Provider generates an OTP which is send to the user's Email.
- If the OTP entered by the LBS User matches with the OTP send by the LBS Provider, then the LBS user gets authenticated.

Fig 6: Authentication of User

❖ Location Tracking

- Provider tracks the user's location by viewing in the google map.

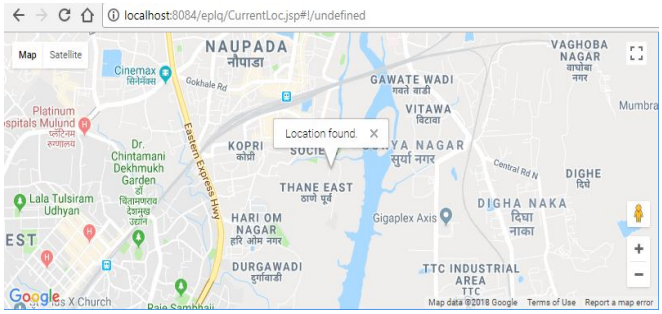

Fig 7: Location Tracking

❖ Location Blocking

- Manipulate user actual location tracked but shuffled location (fake location) stored.

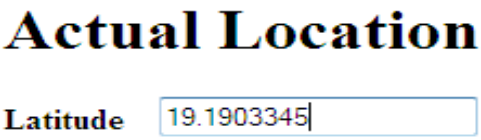

Fig 8: Actual Location

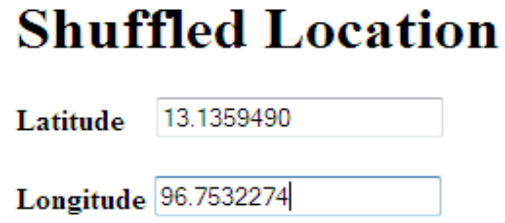

Fig 9: Shuffled Location

IV. FUTURE SCOPE

- Key provided by user is limited to Length 9 only.
- User defined Service Request Generation can be misplaced if Location Information is required and at times System may fail to detect.
- Security based Companies can provide us with Security concerns on our Logic.
- Currently not designed for Location Based Service Provider.
- Currently for Systems who access User Location without any need.

V. CONCLUSION

Through an analysis it is observed that 60% applications that access user location against a particular service provision do not require the exact state of user location. This paper focuses on safeguarding user privacy information like personal location from third party service provider. This secured information is later transmitted to few money making agencies like Advertising agency that use our location for providing their services. In this system, we have successfully safeguarded user location from this third party service provider without blocking the required services. We have used one own shuffling technique LBS Query Algorithm that capably provided the expected results.

REFERENCES

[1] A. Gutscher, "Coordinate transformation—A solution for the privacy problem of location based services?" in Proc. 20th Int. Parallel Distrib. Process.Symp. (IPDPS'06), Rhodes Island, Greece, Apr. 25–29, 2006, p. 424.

[2] W. K. Wong, D. W.-l. Cheung, B. Kao, and N.Mamoulis, "Secure kNN computation on encrypted databases," in Proc. SIGMOD, 2009, pp. 139–152.

[3] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L.Tan,"Private queries in location based services: Anonymizers are not necessary," in Proc. SIGMOD, 2008, pp. 121–132.

[4] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, "Practical k nearest neighbor queries with location privacy," in Proc. 30th Int. Conf. Data Eng. (ICDE), 2014, pp. 640–651.

[5] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," J. ACM, vol. 45, no. 6, pp. 965–981, 1998.

[6] F. Olumofin and I. Goldberg, "Revisiting the computational practicality of private information retrieval," in Financial Cryptography and Data Security. New York, NY: Springer, 2012, pp. 158–172

[7] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proc. 27th Ann. Int. Conf. Theory Appl. Cryptograph. Tech. Adv. Cryptol. (EUROCRYPT '08), Istanbul, Turkey, Apr. 13–17, 2008, pp. 146–162.
[8] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. 4th Theory Cryptograph. Conf. (TCC'07), Amsterdam, The Netherlands, Feb. 21–24, 2007, pp. 535–554.