iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** III **Month of publication:** March 2017

DOI: http://doi.org/10.22214/ijraset.2017.3088

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Location Based Privacy Preserving System for Smart Phones

R.Keerthana[1], S.N.Dharani[2], K.Vidhya[3], N.Rajganesh[4]
[1,2,3]UG Students, [4]Assistant Professor , Department of Information Technology
A.V.C College of Engineering, Tamilnadu, India

Abstract: This proposed system executed by efficiency privacy preserving based on location based service i.e., (LBS).The user identify specific location nearest user need to reach that location within time, accurate route etc. Location based provider collection all query latency of user specified location and send to cloud server with encrypt user privacy data. Cloud server search accurate result in location based on encrypted data and also response to provider .Finally, the server provider create password i.e. decrypted key and personal id number and send to user decryption key ,id and also accurate location details. This cloud services system and location based server provider is more security in user privacy prevention. Therefore, the LBS provider encrypts the LBS data, and outsources the encrypted data to the cloud.

Keywords: Location based service(LBS), query latency, Outsourced data, Accurate location.

I. INTRODUCTION

A. Location Based Service(LBS)

Location based mostly service (LBS) is rising as a killer application in mobile information services with the rapid development in wireless communication and site positioning technologies. Users with location-aware mobile devices will question their surroundings (e.g., finding all looking centers inside five miles or the closest 2 gas stations from my current location) anyplace and at any time. However, though this present computing paradigm brings great convenience for data access, the revealing of user locations to service suppliers raises a priority of intrusion on location privacy that has hampered the widespread use of LBS [1]. Thus, a way to fancy LBS with preservation of location privacy has been gaining increasing analysis attention recently. Within the literature, there are a unit mainly 2 classes of approaches to preserve location privacy for LBS the primary is through data access management. User locations area unit sent to the service suppliers as was common. It depends on the service suppliers to limit access to keep location information through rule-based polices. The second is to use a trustworthy middleware running between the clients and also the service suppliers. A user will specify for every location-based question the privacy demand with a minimum spatial space wants to hide the location. This information would be doubtless helpful if the phone's physical location information becomes additional reliable. It might yield a device's location to be known once its GPS setting is turned off manually.

B. Android Application Development

Android could be a software system stack for mobile devices like sensible phones and tablet PCs. it had been developed by the Open handset Alliance, an association of eighty hardware, software, and telecommunication firms LED by Google dedicated to advancing open standards for mobile devices [8]. Google purchased the initial developer of the software system, android INC., in 2005. Android includes associate software system, middleware, and key applications. The android SDK (Software Development Kit) provides the tools [6].Google discharged most of the android code underneath the Apache License, a free software license. Android is tightly integrated with Google Maps that provides a robust tool for location-based services.

C. Privacy-Preserving LBS Based on Spatial Cloaking

This kind of solutions combines anonymous communication and location obfuscation techniques together. To the LBS provider, a user cannot be identified from a set of users in a cloaking area, and the cloaking area instead of users' precise locations is sent to the LBS provider [4]. These techniques do not allow the cloud to search encrypted data. Therefore, they cannot be used for outsourced LBS where LBS data in the cloud are encrypted.

D. Cloud Services

The cloud has rich storage and computing resources. It stores based on code formation LBS data from the LBS provider, and provides query services for LBS users. So, the cloud has to search the encrypted POI records in local storage to find the ones matching the queries from LBS users.

II. RELATED WORK

This literature follows many related topics of those algorithm detailed in following below

A. Solutions Applicable to Outsourced LBS

1) *Privacy-Preserving Spatial Range Query Based on Coordinate Transformation:* In the answer supported coordinate transformation, the coordinates of queries and POIs in the original organization area unit reworked to new coordinates in an exceedingly new organization. When transforming, the distance information of any two points continued to be preserved. Coordinate transformation is incredibly economical, and the return results area unit correct. However, solutions designed primarily based on coordinate transformation would be susceptible to best-known sample attacks.
2) *Privacy-Preserving POI Query Based on PIR:* As so much as we all know, solely PIR-based solutions will shield the privacy in each public LBS and outsourced LBS. Private information retrieval (PIR) may be privacy primitive activity the retrieved information item's ID from the information server(s). As a result of the information things being retrieved area unit hidden from the information server(s), whether or not 2 queries' results area unit constant or not area unit undetectable. Therefore, PIR-based solutions area unit resilient to access-pattern attacks. PIR may be accustomed notice all the four forms of dish queries. However, PIR is extremely communicative and computationally pricey for the subsequent reasons. PIR needs linearly scanning all dish records as well as their location information (coordinates and radii) and non-location information. Moreover, to use PIR in LBS, Associate in Nursing LBS user should in addition access the LBS information base's index data during a privacy-preserving manner. PIR will retrieve records if given their IDs. To support spatial vary question, Associate in Nursing LBS user ought to acquire close POIs' record IDs from index information during a privacy-preserving manner. PIR or different techniques could also be accustomed acquire such IDs

B. Solutions for Public LBS Only

1) *Privacy-Preserving LBS Based on Anonymous Communication:* In this quite solutions one or additional third parties relay messages between users and therefore the LBS supplier. This approach hides the linkage between user identities and messages from the LBS supplier. The question space would be exposed to the LBS supplier; however the user causing the question is hidden among a collection of users.
2) *Privacy-Preserving LBS Based on Location Obfuscation:* In this quite solution to forestall the LBS supplier from knowing users' precise locations, users submit low exactness locations or pretend locations alongside real locations. These solutions provide a weak level of privacy.
3) *Privacy-Preserving LBS Based on Spatial Cloaking:* This kind of solutions combines anonymous communication and placement obfuscation techniques along. To the LBS supplier, a user can't be known from a group of users in a very cloaking space, and also the cloaking space rather than users' precise locations is shipped to the LBS supplier [7]. All the on top of solutions will be applied to a large vary of LBS as well as dish question. However, their techniques don't permit the cloud to look encrypted knowledge. Therefore, they can't be used for outsourced LBS wherever LBS knowledge within the cloud are encrypted.

III. SYSTEM ANALYSIS

System Analysis is the process of analyzing the system and its component. Proposed systems are detailed below

A. Existing System

In existing system used to realize privacy-preserving POI query, though some of them are not designed for POI query. Privacy-Preserving LBS Based on Anonymous Communication: In this kind of solutions one or more third parties relay messages between users and the LBS provider. This approach hides the linkage between user identities and messages from the LBS provider. The query area would be exposed to the LBS provider, but the user sending the query is hidden among a set of users. Privacy-Preserving LBS Based on Location Obfuscation: In this kind of solutions to prevent the LBS provider from knowing users' precise

locations, users submit low precision locations or fake locations along with real locations. These solutions offer a weak level of privacy. Privacy-Preserving LBS Based on Spatial Cloaking: This kind of solutions combines anonymous communication and location obfuscation techniques together. To the LBS provider, a user cannot be identified from a set of users in a cloaking area, and the cloaking area instead of users' precise locations is sent to the LBS provider. These techniques do not allow the cloud to search encrypted data. Therefore, they cannot be used for outsourced LBS where LBS data in the cloud are encrypted.

1) *Disadvantage:* Fake location is courses, Difficult to secure user privacy.

B. Proposed System

LBS provider has abundant of LBS data, which are POI records. The LBS provider allows authorized users (i.e., LBS users) to utilize its data through location-based queries. Because of the financial and operational benefits of data outsourcing, the LBS provider offers the query services via the cloud. Therefore, the LBS provider encrypts the LBS data, and outsources the encrypted data to the cloud [5]. The cloud has rich storage and computing resources. It stores based on code formation LBS data from the LBS provider, and provides query services for LBS users. So, the cloud has to search the encrypted POI records in local storage to find the ones matching the queries from LBS users. LBS users have the information of their own locations, and query the identity records of nearby POIs in the cloud. Cryptographic or privacy-enhancing techniques are usually utilized to hide the location information in the queries sent to the cloud. To access user records received from the cloud, LBS users need to obtain the code from the LBS provider in advance.

1) *Advantages:* Accurate result of location based services, Efficiency performances and Security process of user preserving privacy.

C. System Description

System description deals with the modules what we are developing the modules for developing the project. It specifies the details of the system.

D. Modules Description

Modules means emphasizes separating the functionality of a program into a independent interchangeable, such that each contains everything necessary to execute only one aspect of the desired functionality. This is the stage of the project when the theoretical design is turned out in to a working system.

1) *Module 1: User Location Register:* The mobile user identifies particular location and to reach specified location using location based services. The mobile user first method is registration for privacy location between certain point call points of intersection (POI).
2) *Module 2: User Query Process:* The user sends location details and privacy information to the service provider. The services provider access user details based on query process for encrypted data.
3) *Module 3: Service Provider:* The process of query based encryption method to involve the generation of code during the location process. The mobile user accesses the current location for sources to destination accurately. The service provider enable service for location based but hidden the user privacy.
4) *Module 4: Verify the accurate location:* The mobile user verifies the correct process and also access the accurate result of query based encryption within surrounding of destination location. The service provider more secure outsources of user privacy.

E. System Architecture Diagram

A system architecture or systems architecture is the conceptual design that defines the structure and/or behavior of a system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system.

In the Fig.1 shows the mobile user identifies explicit location and to succeed in specified location using location primarily based services. The mobile user initial technique is registration for privacy location between certain purpose decision points of intersection (POI). The user sends location details and privacy information to the service supplier. The services supplier access user details based on query process of question primarily based encoding method to involve the generation of code throughout the situation process. The mobile user accesses the present location for sources to destination accurately. The service supplier enable service for location primarily based however hidden the user privacy. The mobile user verifies the proper method and

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

conjointly access the correct results of query primarily based encoding within encompassing of destination location.

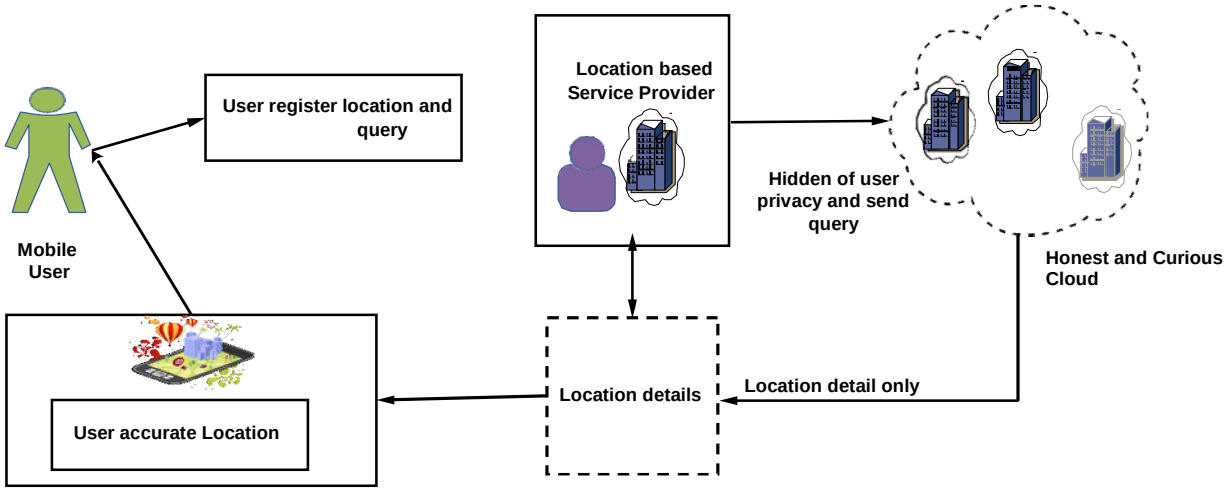


Fig. 1 Architecture Diagram of our Proposed Work

1) *Transfer Phase:* QueryGeneration1 (Client)(QG1): Takes as input indices i, j, and the dimensions of the key matrix m, n, and outputs a query Q1 and secret s1, denoted as (Q1, *s*1) = *QG*1(*i*, *j*, *m*, *n*).
2) *ResponseGeneration*1(*Server*)(RG1): Takes as input the key matrix K*m*×*n*, and the query Q1, and outputs a response R1, denoted as (R1) = RG1(Km×n, Q1).
3) *ResponseRetrieval*1 (*Client*)(RR1): Takes as input indices i , j the dimensions of the key matrix m, n , the Query Q1 and the secret s1, and the response R1 and outputs a cell key K*i*,*j* and cell-Id*i*,*j* denoted as *(Ki,j, Idi,j)= RR1*(*i* ,*j*, *m*, *n*, (Q1,S1), R1)

IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed solution in terms of computational cost, storage cost, and accuracy.

A. Computational Cost at User Side

To generate a question, AN LBS user must cypher 2 predicate vectors, which needs 2n standard exponentiations, regarding 2n2 multiplications, and regarding 2n2 additions. The n is that the length of encoded vectors to examine whether or not the process price is suitable for mobile LBS users or not [2], we have a tendency to measure the question generation latency. We have a tendency to let the humanoid phone in our workplace generate one thousand queries, and therefore the average latency per question generated.

B. Accuracy

Reduces the scale of public parameter however introduces some false positives. This may not hurt the accuracy of resolution. The false positive rate is (τ2 − τ1 + 1)/|Hash()|, that is concerning five.42 × 10−12. O(logN + R) tree nodes square measure scanned throughout a question [3]. This variety is at the most many a whole lot. Then, the chance that a question result contains false positive(s) is at the most many hundred times of five.42 × 10−12, which is negligible.

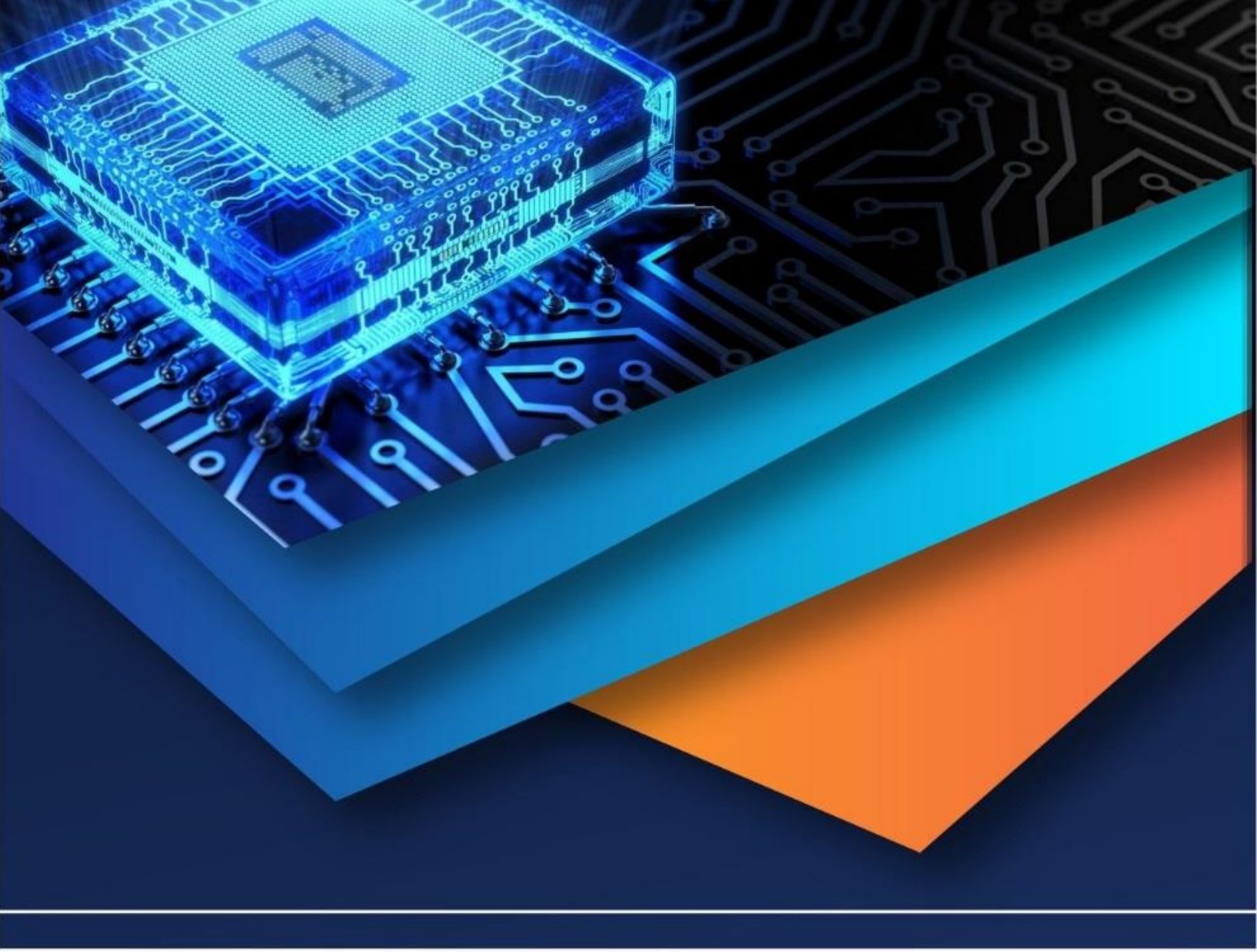
V. CONCLUSION

A location based query solution that employs two protocols that enables a user to privately determine and acquire location data efficiency had been evaluated the detailed analysis shows its security against known-sample attacks and cipher text-only attacks. Our techniques have potential usages in confidentiality.

REFERENCES

[1] JochenSchiller,AgnèsVoisard, 2004, Location-Based Services 1st Edition.
[2] F. Olumofin and I. Goldberg,2012, Revisiting the computational practicality of private information retrieval. [3] B. Yao, F. Li, and X. Xiao, 2013, Secure

nearest neighbor revisited
[3] Emekc. F¸ Agrawal D, Abbadi A. E, ndGulbeden A. ICDE, 2006, privacy preserving query using third parties.
[4]]Lichun Li, RongxingLu , IEEE internet of things journal, 2016, EPLQ:Efficient privacy-preserving location based query over outsourced encrypted data. [6] [Online] http://www.vogella.com/tutorials/AndroidLocationAPI/article.html ,2016vogella GmbH.
[5] AditiGupta 1, Vibhor Harit2.IEEE DOI 10.1109/CICT.2016.141 201, Child safety & tracking management system by using GPS, Geo-Fencing & Androi application.
[6] BhuvanaSekar and Jiang B.Liu .IEEE (ICIEA),2014, Location Based Mobile Apps Development on Android Platform.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY