ISSN 2395-1621

Location Based Cloud EcoSystem Using Fog Computing

[#1]Piyanka B. Bachhav, [#2]Rani N. Pasalkar, [#3]Mayuri M. Shinde,
[#4]Snehal Y. Jagtap, [#5]Prof. Mrs. Nancy A. Peter

[1]priyankabachhav4@gmail.com,
[2]ranipasalkar95@gmail.com,
[3]mayurishinde0304@gmail.com,
[4]snehalyj2011@gmail.com,
[5]nancyambritta.peter@gmail.com

[#12345]Department of Computer Engineering,
SITS Narhe, Pune

ABSTRACT

Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. Fog computing, also known as fog networking, is a decentralized computing infrastructure in which computing resources and application services are distributed in the most logical, efficient place at any point along the continuum from the data source to the cloud. The goal of fog computing is to improve efficiency and reduce the amount of data that needs to be transported to the cloud for data processing, analysis and storage. This is often done for efficiency reasons, but it may also be carried out for security and compliance reasons [6]. We present a solution to one of the location-based query problems. This problem is defined as follows: (i) a user wants to query a database of location data, known as Points Of Interest (POIs), and does not want to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not want to simply distribute its data to all users. Owing to increasing demands from mobile users, Location-Based Services (LBSs) have received a lot of attention in recent years. Examples of queries for location-based services include "find the nearest gas station from my current location", "find all the cinemas within 1 km radius", "which buses will pass by me in the next 10 minutes?" and so on. While data objects in the first two examples are stationary, those in the last example are mobile. We focus on queries issued by mobile users on relatively static data objects, because they are the most common kind of queries in LBSs [3]. The movement of mobile clients presents many new research problems for location-dependent query processing. In which there are several technical issues involved with the implementation of an LBS, which include locating the position of a mobile user, tracking and predicting movements, processing queries efficiently, and bounding location errors.

Keywords-**Location Based System,. Location Based Services, Cloud computing Global Positioning System, Mobile Application User, Distributed Databases, Point Of Interest Algorithm, Honeypot**

ARTICLE INFO

Article History

Received: 19th December 2016

Received in revised form :

19th December 2016

Accepted: 22nd December 2016

Published online :

22nd December 2016

I. INTRODUCTION

Owing to increasing demands from mobile users, Location-Based Services (LBSs) [3] have received a lot of attention in recent years. Examples of queries for location-based services include "find the nearest gas station from my current location", "find all the cinemas within 1 km radius", "which buses will pass by me in the next 10 minutes?" and so on. While data objects in the first two examples are stationary, those in the last example are mobile. We focus on queries issued by mobile users on relatively static data objects, because they are the most common kind of queries in LBSs. The movement of mobile clients presents many new research problems for location-dependent query processing. In which there are several technical issues involved with the implementation of an LBS, which include locating the position of a mobile user, tracking and predicting movements, processing queries efficiently, and bounding location errors.

Consider a computing environment with a large number of location-aware mobile objects. We want to retrieve the mobile objects inside a set of user-defined spatial regions and continuously monitor the population of these windows over a time period. We refer to such continuous queries as range-monitoring queries. Efficient processing of range-monitoring queries could enable many useful applications. Similarly, we might want to track traffic condition pin some area and dispatch more police to the region if the number of vehicles inside exceeds a certain threshold. In such applications, it is highly desirable and sometime critical to provide accurate results and update them pin real time whenever mobile objects enter or exit the regions of interest. Unlike conventional range queries, a range-monitoring query is a continuous query. It stays active until it is terminated explicitly by the user. As objects continue to move, the query results change accordingly and require continuous updates. A simple strategy for computing range monitoring queries is to have each object report its position as it moves. The server uses this information to identify the affected queries, and updates their results accordingly. This simple approach requires excessive location updates, and obviously is not scalable. Each location update consists of two expenses - mobile communication cost and server processing cost. If a battery-powered object has to constantly report its location, the battery would be exhausted very quickly. It is well-known that sending a wireless message consumes substantially more energy than running simple procedures. For example, consider that the data objects are vacant cabs and the clients are pedestrians that wish to know their k closest free taxis until they hire one. As the reverse case, the queries may correspond to vacant cabs, and each free taxi driver wishes to be continuously informed about his/her k closest pedestrians. Several monitoring methods have been proposed, covering both range and k NN [3] queries.

Some of these methods assume that objects issue updates whenever they move, while others consider that data objects have some computational capabilities, so that they inform the server only when their movement influences some query.

II. LITERATURE SURVEY

Private Information Retrieval (PIR) is the fact that a client retrieves a certain record from a remote database managed by untrusted parties without letting them know which record has actually been requested, thus preserving the privacy of the client. Ostrovsky and Skeith showed in [1] that any homomorphic encryption can actually be used to achieve PIR. We use their protocol as basis to compare five well known homomorphic encryption schemes by providing simulation results.

In [2], two public key cryptosystems based on the multiplicative learning with errors (MLWE) problem. The cryptosystem 1 are semantically secure assuming the worst-case hardness of the decisional composite residuosity problem and the search (resp. decisional) LWE problem, which implies approximating the shortest vector problem in a lattice to small polynomial factors. In addition, the cryptosystem 2 has the additively homomorphic property.

[3], the author presents a solution to one of the location-based query problems. This problem is defined as follows: (i) a user wants to query a database of location data, known as Points Of Interest (POI), and does not want to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not want to simply distribute its data to all users. A location based query solution that employs two protocols that enables a user to privately determine and acquire location data. The first step is for a user to privately determine his/her location using oblivious transfer on a public grid. Oblivious Transfer used to achieve a more secure solution for both parties. The second step involves a private information retrieval interaction that retrieves the record with high communication efficiency.

In [4], private Information Retrieval is a technique that creates a common language between users and service provider so that external actors cannot understand most of the information being transferred. This includes introduces MaPIR, a mapping-based private information retrieval technique that uses mathematically generated mapping to create redundancy in order to provide multiple answers to a user within undistinguishable location. This technique is decentralized and focuses on Point of Interest Search-based application, not on tracking services. For performance evaluation, were compared in two scenarios MaPIR, a regular spatial query and the Dummy Query technique.

In [5], an ecosystem is the expansion of a software product line architecture to include systems outside the product which interact with the product. A cloud ecosystem includes interdependent and communicating components. Not only the cloud ecosystem itself keeps evolving, but it also affects the way in which we develop and deploy software. We model the architecture of a cloud ecosystem as a set of patterns, showing partial descriptions for some of them.

Sr. No.	Title of paper	Existing System	Parameters	Disadvantages	Advantages
1.	Performance Analysis of Private Information Retrieval Scheme based on homomorphic Encryption.	The privacy of the user is not preserved and the server providers tend to build user profiles to keep track of the behavior of the users in order to send them targeted ads	Private information retrieval- access for private information, homomorphic encryption, malleability, privacy, simulation.	Using internet services such as viewing a video or getting a record from a database in general can be very convenient for the end user. This convenience comes always with a huge downside: the privacy of the user is not preserved and the server providers tend to build user profiles to keep track of the behavior of the users in order to send them targeted ads.	used a generic protocol presented in [1] by Ostrovsky and Skeith that can achieve PIR using any homomorphic encryption scheme. This protocol is tested using five well known homomorphic encryption schemes for comparison.
2	Public Key Cryptosystems from the Multiplicative Learning with Errors	Due to public key cryptosystem, there are many the public key schemes which are mainly based on the hardness assumptions such as factoring, discrete logarithm or various lattice problems.	Multiplicative Learning with Errors; Public key Cryptography- two public-key Cryptosystems based on the hardness of multiplicative learning with error.; Lattice-based Cryptography; Decisional Composite Residuosity Assumption; Factoring Integer.	Due to the importance of public key cryptosystem, there are many the public key schemes which are mainly based on the hardness assumptions such as factoring, discrete logarithm or various lattice problems.	two MLWE-based public key cryptosystems whose securities are based on the standard cryptographic assumptions which are the decisional composite residuosity problem and the search/decisional LWE problem. These hard problems respectively come from the problem of computational number theory and the learning with errors problem, which implies the lattice problem.
3	Privacy-Preserving and Content-Protecting Location Based Queries	Location based query like user wants to query a database of location Data, known as Points Of Interest(POI), and does not want To reveal his/her location to the server due to privacy concerns.	Mobile nearest neighbor search (NN)-,k nearest neighbor search:- classification and regression, R-Tree algorithm, Grid index algorithm, Melkman's algo:- algorithms to solve queries .	Location based query like a user wants to query a database of location Data, known as Points Of Interest(POI), and does not want To reveal his/her location to the server due to privacy concerns.	A location based query Solution that employs two protocols that enables a user to Privately determine and acquire location data .The first step Is for a user to privately determine his/her location using Oblivious transfer on a public grid. The s

4	MaPIR: Mapping-Based Private Information Retrieval for Location Privacy in LBISs	location privacy is one of the most critical concern for ensuring users' right to protection. the fact that one of the best ways to protect the location information is not to reveal it.	Location obfuscation:- protect location of user; privacy; point of interest:- specific location which user wants to find; geographical query; LBIS:- connect information pieces to position in outdoor and indoor spaces.	location privacy has become one of the most critical concerns for ensuring users' right to protection. the fact that one of the best ways to protect the location information is not to reveal it	The MaPIR technique is a private information retrieval–based privacy protection technique, which enforces location privacy and allows querying PoIs with great accuracy, in an efficient manner, and without revealing the actual location of the users

III. PROPOSED SYSTEM

Product Perspective:

System having a novel protocol for location based queries that has major performance improvements and like such protocol, our protocol is organized according to two stages. In the first stage, the user privately determines his/her location within a public grid, using oblivious transfer. This data contains both the ID and associated symmetric key for the block of data in the private grid. In the second stage, the user executes a communicational efficient PIR [], to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage.

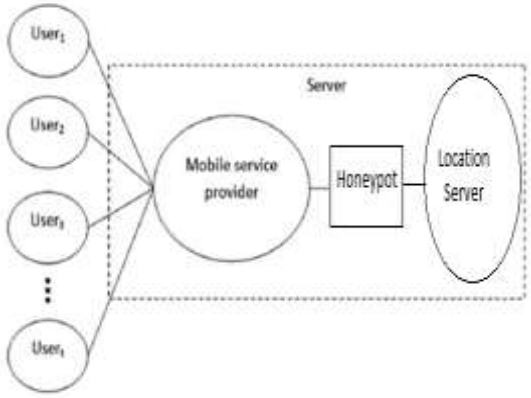

Figure 1: System Architecture

Product Functions

Protocol provides protection for both the user and the server. The user is protected because the server is unable to determine his/her location. Similarly, the server's data is protected since a malicious user can only decrypt the block of data obtained by PIR with the encryption key acquired in the previous stage[2]. In other words, users cannot gain any more data than what they have paid for.

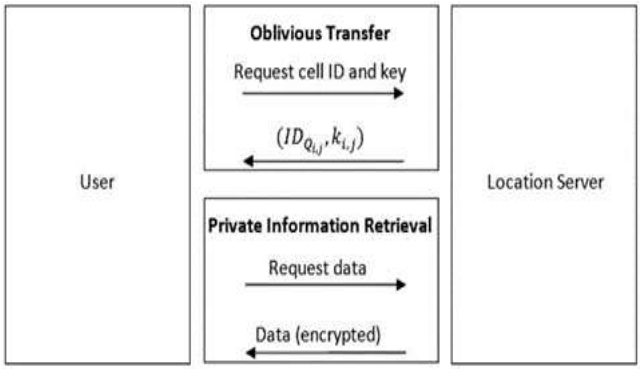

Figure 2:Function Architecture

A first-time user of the mobile application should see the log-in page when he/she opens the application, see Figure 2. If the user has not registered, he/she should be able to do that on the log-in page. If the user is not a first-time user, he/she should be able to see the search page directly when the application is opened, see Figure 3. Here the user chooses the type of search he/she wants to conduct. Every user should have a profile page where they can edit their e-mail address, phone number and password, see Figure 4. Also, the user can set the mobile application to his/her preferred language. The "P" icon shows where the user can click to navigate to his/her profile page

Figure 2 - Login page

Figure 3 – Search page

Figure 4 – Profile page

Equations:
Let 'S' be the solution set of the problem statement of the project.
S = {S, E, I, O, DD, NDD, Fs, A, Success, Failure,}

Where,
S- {Start state: User login}
E- {End state: Location Found.}

I-Set of input to the system {I1, I2, I3}
Where,
I1=Login details: username and password,
I2=current location,
I3=Destination.

O-Output of system{O1,O2}
Where
O1=Successful Login,
O2=Location Found,

DD- Deterministic data
{username, password, location, privacy of device}

NDD- Non-Deterministic data
{ unsuccessful login, location is not tracked, privacy of device is not maintained }

$\mathbf{F_s}$-{Function and used in the system}={f1,f2,f3,f4}
Where,
f1={ successful user login.}
f2={ used to specify the location to find.}
f3={ used to give relevant location as resultant.}
f4={used to hide the privacy of user device.}
A-{Algorithms used to achieve the goals}={key generation ,encryption, decryption, etc.}

Success-{Specified Location is effectively found and also users device privacy is maintained
using effective algorithm and specified protocol.}

Failure-{ Failed to track specified location.}

IV. CONCLUSION

In this paper we have presented a location based query solution that employs two protocols that enables a user to privately determine and acquire location data. The first step is for a user to privately determine his/her location using oblivious transfer on a public grid. The second step involves a private information retrieval interaction that retrieves the record with high communication efficiency.

A private information retrieval based privacy protection technique, which enforces location privacy and allows querying PoIs with great accuracy, in an efficient manner, and without revealing the actual location of the users.

It is able to protect the location information of the user by generating redundant information to hide the original source of the query, obtaining similar protection results compared to the Dummy Query technique. In addition, this redundancy is used to generate no overhead of the server side, and even, the mapping function, the preprocessing and the nature of the queries performed, shows better processing time than the regular geographical queries.

REFERENCES

[1] Yacine Ichibane ,Youssef Gahi ,Mouhcine Guennoun ,Zouhair Guennoun Laboratoire Electronic Communications. "Performance Analysis of Private Information Retrieval Scheme based on Homomorphic Encryption" School of Electrical Engineering and Computer Science University of Ottawa 800 King Edward Ave., Ottawa, ON, Canada.

[2] Gu Chunsheng School of Computer Engineering Jiangsu Teachers University of Technology Changzhou, China, 213001 guchunsheng@gmail.com "Public Key Cryptosystems from the Multiplicative Learning with Errors", 2010 International Conference on Multimedia Information Networking and Security

[3] Anandababu A, S.Brintha Rajakumari, Dr.C.Nalini, P.G. Student, Department of Computer Science and Engineering, Bharath University, Chennai, India " Privacy-Preserving and Content-Protecting Location Based Queries" International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 3, March 2015

[4] P. M. Wightman, M. Zurbarán, M. Rodríguez Departamento de Ingeniería de Sistemas Universidad del Norte Barranquilla, Colombia "MaPIR: Mapping-Based Private Information Retrieval for Location Privacy in LBISs" 8th IEEE Workshop on Network Security 2013.

[5] Madiha H. Syed, Eduardo B. Fernandez, Dept. of Comp. and Elect.Eng.and Computer Science Florida Atlantic University, Boca Raton, FL, USA, msyed2014@fau.edu , ed@cse.fau.edu "Cloud Ecosystems support for Internet of Things and DevOps using Patterns" 2016 IEEE First International Conference on Internet-of-Things Design and Implementation.

