International Conference on Advances in Materials, Computing and Communication Technologies
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

GPS Based Online Medicine Identification System

Nithish K[1], Rahul R G[1], Bindhu A[2]
[1]Department of CSE, Marthandam College of Engineering and Technology, Tamil Nadu, India
[2]Assistant Professor, Department of CSE, Marthandam College of Engineering and Technology, Tamil Nadu, India

ABSTRACT

Online medicine identification system is an application that is dependent on the location of a mobile device. This application is part of the larger service viz. the location based services (LBS). This system uses the location based services to help user to find shops from their current place and to find medicine from their location which saves his/her time by making him the facility of fast access of products. Instead of searching throughout the shops manually, one can use the gps enabled mobile device to identify the medicine. A GPS tracking unit is a navigation device normally carried by a moving vehicle or person, that uses the (GPS) to track the product available shops and determine its location. The proposed framework includes three user-facing components: 1) an energy-aware application for end users to recognize their locations and access the services available to them 2) the application, which enables end users to search medicine available on their current location and 3)the application for shops to specify the availability of medicines on shops and in which areas. In order to protect query privacy of the user, the existing state-of-the-art schemes either reduce the accuracy of LBS or insert a trusted third party (TTP) between the vehicle user and the location server hosting the LBS scheme. In order to address the security and privacy issues, an efficient privacy-preserving mechanism is proposed for protecting the query privacy of the user, information content of the location server, and location privacy-preserving of the vehicle in the LBS scheme. The query privacy of the user and content privacy of the location server is preserved in the exchange.

Keywords: LBS, GPS, VANET, V2I, Location Based Services, Medicine Identification

I. INTRODUCTION

In VANETs, vehicles get information regarding traffic conditions, infotainment vehicle to infrastructure (V2I), I2V, V2V communication. Infotainment messages can provide news, environment, social interaction, and network services to the drivers to improve the experience of driving. LBS provides information and utility service to the drivers based on their geographical position. A fee is charged for the service by the location server providing the LBS. To get utility services and information, the driver selects query content and sends it to the location server. The location server retrieves all the query specific POIs from the database server and sends it to the driver. The driver extracts information from POIs, such as

the nearest hospital, ATM, gas station, police station or restaurant, etc. However, this process may reveal the vehicle's location. Revealing the exact location of the vehicle allows a location server to predict and track the vehicle's daily movement and identity, which may result in economic loss, physical stalking, etc. Therefore, there is a need to preserve the privacy of the vehicle. The location server which provides LBS needs resources to maintain database server and gather information about POIs. Therefore, for this commercial venture, the location server levies a charge to distribute the queried data to the drivers. The vehicle user must get only queried data other data must remain hidden from it. Hence, the privacy of both, the driver, and services not paid for, must be preserved in the LBS scheme. Different types of privacy-preserving LBS schemes for location privacy have been proposed. In LBS, privacy-preserving services can be divided into two parts location privacy and query content privacy. In case of location privacy, the current location of LBS user is protected from the malicious server, while in case of query content privacy, content-specific information requested by the driver to location server is protected from a malicious server. For query content protection, mainly two types of schemes have been proposed dummy query construction and query content obfuscation

II. RELATED WORK

C. Peikert et al., proposes lowbandwidth reconciliation technique that allows two parties who "approximately agree" on a secret value to reach exact agreement, a setting common to essentially all lattice-based encryption schemes.

Liang Cheng, Yue Jiang et al., proposes redundant POI records to protect privacy against LBS provider but employs a semi-trusted third party, called proxy, to filter out redundant POI records. To protect privacy against proxy, we design a novel filtering protocol, Blind filter, to allow the proxy to filter out redundant encrypted POI records in a blind way. In comparison with existing solutions, our framework is not only resilient to dual identity attack, but also incurs lower communication and computation overhead.

H. Zhu, F. Liu et al., proposes an efficient special polygons spatial query (SPSQ) algorithm over ciphertext is constructed, based on an improved homomorphic encryption technology over composite order group. With SPSQ, Polaris can search outsourced encrypted LBS data in CS by the encrypted request, and respond the encrypted polygons spatial query results accurately.

R. Schlegel, C.-Y. Chow et al., proposes a user-defined privacy grid system called dynamic grid system (DGS); the first holistic system that fulfills four essential requirements for privacy-preserving snapshot and continuous LBS. (1) The system only requires a semi-trusted third party, responsible for carrying out simple matching operations correctly. This semi-trusted third party does not have any information about a user's location. (2) Secure snapshot and continuous location privacy is guaranteed under our defined adversary models. (3) The communication cost for the user does not depend on the user's desired privacy level, it only depends on the number of relevant points of interest in the vicinity of the user. (4) Although we only focus on range and k-nearest-neighbor queries in this work.

B. Niu, Q. Li et al., proposes Dummy-Location Selection (DLS) algorithm to achieve k-anonymity for users in LBS. Different from existing approaches, the DLS algorithm carefully selects dummy locations considering that side information may be exploited by adversaries. We first choose these dummy locations based on the entropy metric, and then propose an enhanced-DLS algorithm, to make sure that the selected dummy locations are spread as far as possible

III. ARCHITECTURAL DESIGN

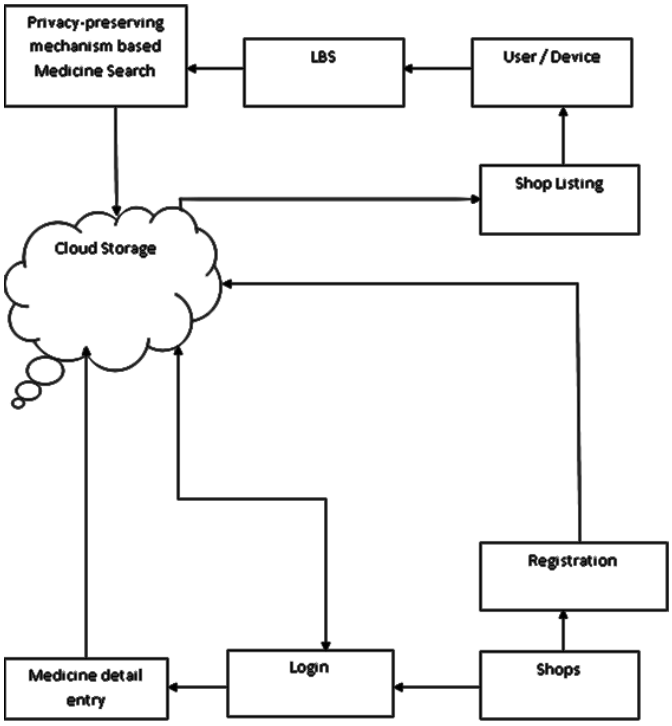

Fig 1: Architectural Design

IV. METHODOLOGY

The proposed system includes the following modules.

- Login
- Products details
- LBS and querying
- Shop listing

Login

The shops have to register with the system with their current location and contact no's. The registered shops can obtain the validation process using their username and password. The authorized shops are provided with services. The services are denied for the unauthorized users.

Products details

The shop's have to enter the medicine details periodically. It have the following responsiblities:

- Adding new Medicines, amount details
- Updations
- Deletion

LBS and querying

A location-based service (LBS) is used to utilize the geographic data to provide services or information to users. In the proposed system LBS is used to identify thecurrent location to purchase the required medicine. Querying section is used to search the required medicines on the current location.

Shop listing

This module is used to list the shops to the users. The system will perform a search over the data based on the acquired location and display the shop details where ever the products available based on the location. It also supports the shop wise search.

V. CONCLUSION

Initially mobile phones were developed only for voice communication but now days the scenario has changed, voice communication is just one aspect of a mobile phone. Two such major factors are web browser and GPS services. The Online product identification application will help user to find medicine in a short time and the user would be able to buy products from the given list of shops. While traveling on the road, vehicle users want to avail services available in their vicinity. An LBS server provides this service. However, there are caveats from both entities. The vehicle does not wish to reveal the specific service it wants and the LBS server wishes to provide information of those services only to the vehicle user for which it is paid for. On a stretch of road, LBS provider must be able to handle of a large number of queries efficiently. The proposed LBS scheme for VANET endeavors to achieve these seemingly contradictory objectives efficiently. The LBS scheme uses the OT extension protocol, which provides the required privacy to the vehicle user by protecting its needs, privacy to LBS server by protecting its basket of services and scalability when large number of users query for service simultaneously. The proposed LBS scheme was found

to be quite efficient in terms of computational and communication needs. The OT extension protocol outperformed existing protocols with respect to running time. The OT protocol also had slightly lower communication overhead. Moreover, the number ofcommunication rounds was also significantly less with smaller message sizes.

VI. REFERENCES

[1]. C. Peikert, "Lattice cryptography for the internet," in international workshop on post-quantum cryptography. Springer, 2014, pp. 197–219

[2]. H. Zhu, F. Liu, and H. Li, "Efficient and privacy-preserving polygons spatial query framework for location-based services," IEEE Internet of Things Journal, vol. 4, no. 2, pp. 536–545, 2016.

[3]. R. Schlegel, C.-Y. Chow, Q. Huang, and D. S. Wong, "User-defined privacy grid system for continuous location-based services," IEEE Transactions on Mobile Computing, vol. 14, no. 10, pp. 2158–2172, 2015

[4]. B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in IEEE INFOCOM 2014-IEEE Conference on Computer Communications. IEEE, 2014, pp. 754–762

[5]. H. Zhu, F. Liu, and H. Li, "Efficient and privacy-preserving polygons spatial query framework for location-based services," IEEE Internet of Things Journal, vol. 4, no. 2, pp. 536–545, 2016.

[6]. S. Zhang, Q. Liu, and Y. Lin, "Anonymizing popularity in online social networks with full utility," Future Generation Computer Systems, vol. 72, pp. 227–238, 2017

[7]. G. Asharov, Y. Lindell, T. Schneider, and M. Zohner, "More efficient oblivious transfer extensions with security for malicious adversaries," in Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2015, pp. 673–701.

[8]. Beaver, "Correlated pseudorandomness and the complexity of private computations," in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM, 1996, pp. 479–488.