A NOVEL TECHNIQUE FOR CONTENT PROTECTION ON LOCATION BASED QUERIES USING MD5

A.Srinivasa Rao[1], K.Vivek[2]
1M.Tech Scholar, Department of Computer science, Vignan’s Lara Institute of Technology and science, Vadlamudi, India.
2M.Tech, Assistant Professor, Department of Computer science, Vignan’s Lara Institute of Technology and science, Vadlamudi, India.

ABSTRACT
In today’s modern world, it is very easy for a person to know his/her location with the help of devices having GPS facility. When user’s location is provided to LBS, it is possible to user to know all location dependent information like location of friends or Nearest Restaurant, whether or traffic conditions. The massive use of mobile devices pave the way for the creation of wireless networks that can be used to exchange information based on locations. When the exchange of location information is done amongst entrusted parties, the privacy of the user could be in harm. Existing protocol doesn’t work on many different mobile devices and another issue is that, Location Server (LS) should provide misleading data to user. So we are working on enhancement of this privacy protocol.

Keywords: Location server, overhead, private information retrieval, reputation technique, privacy.

I. INTRODUCTION
Location based service can offer many services to the users based on the geographical position of their mobile device. The services provided by LBS are typically based on a point of interest database. By retrieving the Points Of Interest (POIs) from the database server, the user can get answers to various location based queries, which include but are not limited to - discovering the nearest ATM machine, gas station, hospital, or police station. Private Information Retrieval (PIR) protocols allow a client to retrieve one bit from a database, without the server inferring any information about the queried bit. Private information retrieval (PIR) is a way for a client to look up information in an online database without letting the database servers learns the query terms or responses. The goal of PIR is to transmit less data while still protecting the privacy of the query. These protocols are too costly in practice because they invoke complex arithmetic operations for every bit of the database. Here a major enhancement introduced into two stage approach, where the first stage is based on Oblivious Transfer and the second stage is based on Private Information Retrieval (PIR), to achieve a secure solution for both parties. Here introduce a successful privacy preserving Location Based Services (LBS) must be secure and provide accurate query results. Privacy preserving Location Based Services is deal with the privacy and the accuracy issues of privacy preserving LBS. As LBS is a developing technology, users might not be aware of the risks that it poses. New types of smart mobile devices enabled the emergence of Location Based Services (LBS). A user of the service carries a mobile device that obtains its location via GPS or a Wireless Local Area Network (WLAN). In location based services (LBS), users with location were mobile devices can query their surroundings anywhere and at any time. While this ubiquitous computing paradigm brings great convenience for information access, it raises a concern of potential intrusion on user’s location privacy, which has hampered the widespread use of LBS. Users of mobile devices tend to frequently have a need to find Points Of Interest (POIs), such as restaurants, hotels, or gas stations, in close proximity to their current locations. Collections of these POIs are typically stored in databases administered by Location Based Service (LBS) providers such as Google, Yahoo!, and Microsoft, and are accessed by the company’s own mobile client applications or are licensed to third party independent software vendors. A user first establishes his or her current position on a smartphone such as a RIM BlackBerry, Apple iPhone, or Google Android device through a positioning technology such as GPS (Global Positioning System) or cell tower triangulation, and uses it as the origin for the search. The problem is that if the user’s actual location is provided as the origin to the LBS, which performs the lookup of the POIs, then the LBS will learn that location.

II. RELATED WORK
M. blearer and S. cicala [2]. They are proposed an client and fair agreement for protected two-party computation in the assured model, in which a partially credible 3rd party T is available, but not in velvet in normal beheading of protocol. T is required only if there exist interruption in communication or if one Of the two celebration denies or trespass. This contract ensures that even if one party terminates the contract at
any of the time, the calculation is still fair for the second party. Communication is over an all chronic network. All agreement we are using are based on application proofs of knowledge and affect no general zero-knowledge to ols as transitional steps we describe e¿cien tveriÔ-able oblivious transfer. A. bereaved and F. satan[3] they are expected an As location-aware function begin to track our change in the name of accessibility, how can we protect our racy? This article announce the mix zone-a new manufacture inspired by anonymous connection approach-together with metrics for assessing invisibility of an user which is based on alias which are frequently changing. C. batting, X.

Wang, and S. jacked[4] They proposed an article & we present a solution to one of the location affirm query quandaries. This difficulty is defined as follows: (i) a utilized wants to query a database of location data, appreciate as Points Of Interest (POIs) and does not extract to reveal his/her location to the server due to privacy burden; (ii) the owner of the district data, that is, the location server, does not extract to simply administer its data to all the users. Here the location server wishes to have some authority over its data, since the data is its asset. We advocate a major improvement upon anterior solutions by announce a two stage accession, where the first step is predicated on inattentive Transfer and the second step is declare on Private Information bettorem (PIR), so as to accomplish a secured solution for both the celebration. The solution which we present is quite adequate and more practical in many of the scheme. We then appliance our solution onto a desktop machine and a mobile artifice to assess the efficiency of our contract. We additionally introduce a security model and analyze the security in the context of our protocol. Finally, we highlight a security impotency of our antecedent work and present a solution to surmount it.

X. Chen and J. Pang[5] They proposed an Vehicular networks are envisioned to play an important role in the building of intelligent transportation systems. However, the dangers of the wireless transmission of potentially exploitable information such as detailed locations are often overlooked or only inadequately addressed in field operational tests or efforts of standardization. The main reasons for this is that the concept of privacy is difficult to quantify. While vehicular network algorithms are usually evaluated by means of simulation, it is a non-trivial task to assess the performance of a privacy protection mechanism. In this paper we discuss the principles, all the challenges, and also the necessary steps in terms of privacy assenment in vehicular N/W s. We also identify all useful and the practical metrics that allow the comparison and evaluation of privacy protection algorithms. We hereby present a very systematic literature review that sheds light on the current state of the art and give recommendations for future research directions in the field. B. Chor, E. Kushilevitz, O.

Goldreich, and M. Sudan[6] the proposed a survey the notion of Single-Database Private Information Retrieval (PIR). The first Single-Database PIR was constructed in 1997 by Kushile vitz and Ostrovsky and since then Single-Database PIR has emerged as an important primitives of cryptography. For ex., Single-Dbase PIR turned out to be intimately connected to collision resistant hash functions, the oblivious transfer and also public-key encryptions with some additional properties. Here in this survey, we state an overview of many of the constructions for Single-Database PIR (including an abstract construction based upon homomorphic encryption) and describe some of the connections of PIR to other primitives. T. ElGamal[9] proposed A new signature scheme, together with the implementation of the Diffie-Hellman public key distribution scheme that achieves a public key cryptosystems. The secureness of the both systems relies on the difficulty of computing discrete logarithms over finite fields. B. Gedik and L. Liu[10] they are proposed a solution to one of the location predicated query quandaries. This quandary is defined as follows: (i) a utilizer wants to query a database of location data, kennd as Points Of Interest (POIs) and does not opt 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 opt to simply distribute its data to all the users. Here the location server wishes to have some control over its data, since the data is its asset. We recommend a major enhancement upon anterior solutions by introducing a two stage approach, where the first step is predicated on Oblivious Transfer and the second step is predicated on Private Information Retrieval, so as to achieve a very secure solution for both the parties. The solution which we present is too efficient and practical in most of the scenarios. We then implement our solution to/on a desktop machine and a mobile contrivance to assess the efficiency of our protocol. We additionally introduce a security model and analyze the security in the context of our protocol. Finally, we highlight a security impotency of our antecedent work and present a solution to surmount it.

C. Gentry and Z. Ramzan[11] the are proposed an location with the help of devices having GPS facility. When user’s location is provided to LBS, it is possible to user to know all location dependent information like location of friends or Nearest Restaurant, whether or traffic conditions. The massive use of mobile devices pave the way for the creation of wireless networks that can be used to exchange information based on
locations of users. When we get done with exchange of location information amongst entrusted parties, the privacy of the user could be in harm. Existing protocol doesn’t work on many different mobile devices and another issue is that, Location Server (LS) should provide misleading data to user. So we are working on enhancement of this protocol. Mobile devices with global positioning capabilities allow users to retrieve points of interest (POI) in their proximity area. To protect the user privacy, its important not to disclose exact user coordinates to un-trusted entities that provide location-based services. Currently, there are two main approaches to protect the location privacy of users: (i) hiding locations inside cloaking regions (CRs) and (ii) encrypting location data using private information retrieval (PIR) protocols. Our previous work mainly focused on discovering good trade-offs between privacy and user protection techniques performances, but it disregarded the most important issues of protecting the POI dataset D. For the instance, location cloaking requires large-sized CRs, leading to excessive disclosure of POIs (\(O(D)\) in its worst case). PIR (private information retrieval), on the other hand, minimizes this bound to \(O(\sqrt{D})\), but at the expense of high processing and the communication overhead. We therefore proposed a hybrid, two-step approaches for private location-based queries which provide protection for both the users and also the database. In the very first step, user locations are hence generalized to coarse-grained CRs which provide strongest privacy. Next: a PIR protocol is applied with respect to the obtained query CR. To protect against excessive disclosure of POI(point of interest) locations, we devise two cryptography protocols which privately evaluate whether a point is enclosed inside a rectangular region or a convex polygon. We also state algorithms to efficiently support PIR on dynamic POI.

III. PROPOSED SYSTEM

In this system we involve testing the protocol on several different mobile devices. The mobile result we offer may be completely different than alternative mobile devices and computer code environments. Also, we'd like to cut back the overhead of the property take a look at utilized in the personal info retrieval based protocol. in addition, the matter regarding the L.S supply deceptive information to the consumer is additionally attention-grabbing. Privacy protective name techniques appear a suitable approach to deal with such drawback. A possible solution may integrate strategies. Once appropriate strong solutions exist for the overall case, they'll be simply integrated into our approach. This algorithm uses the location indexes of the users and multiple parallel threads to search and select quickly all the candidate anonymous sets with more users and their location information with more uniform distribution to accelerate the execution of the temporal-spatial anonymous operations, and it allows the users to configure their custom-made privacy-preserving location query requests.
MD5 works
Preparing the input
The MD5 algorithm first divides the input in blocks of 512 bits each. 64 Bits are inserted at the end of the last block. These 64 bits are used to record the length of the original input. If the last block is less than 512 bits, some extra bits are 'padded' to the end.
Next, each block is divided into 16 words of 32 bits each. These are denoted as $M_0$ ... $M_{15}$.

MD5 functions
The buffer
MD5 uses a buffer that is made up of four words that are each 32 bits long. These words are denoted as A, B, C and D. They are initialized as:
- word A: 01 23 45 67
- word B: 89 ab cd ef
- word C: fe dc ba 98
- word D: 76 54 32 10

The table
MD5 further uses a table K that has 64 elements. Element number i is indicated as $K_i$. The table is computed beforehand to speed up the computations. The elements are computed using the mathematical sin function:
$$K_i = \text{abs} \left( \sin (i + 1) \right) \times 2^{32}$$

Four auxiliary functions
In addition MD5 uses four auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word. They apply the logical operators and, or, not and xor to the input bits.
- $F(X,Y,Z) = (X \text{ and } Y) \text{ or } (\neg X \text{ and } Z)$
- $G(X,Y,Z) = (X \text{ and } Z) \text{ or } (Y \text{ and } \neg Z)$
- $H(X,Y,Z) = X \text{ xor } Y \text{ xor } Z$
- $I(X,Y,Z) = Y \text{ xor } (X \text{ or } \neg Z)$

Processing the blocks
The contents of the four buffers (A, B, C and D) are now mixed with the words of the input, using the four auxiliary functions (F, G, H and I). There are four rounds, each involves 16 basic operations. One operation is illustrated in the figure below.

The figure shows how the auxiliary function $F$ is applied to the four buffers (A, B, C and D), using message word $M_i$ and constant $K_i$. The item "<<<s" denotes a binary left shift by s bits.

IV. CONCLUSION
Conclusion and Future Work In this paper we’ve got given a location based mostly question solution that employs 2 protocols that permits a user to in private verify and acquire location information. The first step is for a user to in private verify his/her location using oblivious transfer on a public grid. The second step involves a non-public info retrieval interaction that retrieves the record with high communication potency. We analyzed the performance of our protocol and located it to be each computationally and communicational a lot of efficient than the answer by Ghinita et al., that is that the most recent resolution. we tend to enforced a software system epitome using a desktop machine and a mobile device. The software system prototype demonstrates that our protocol is among sensible limits.

REFERENCES