ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Seclusion Security and Data Protecting Position Based Search

Yellinedi Hari Krishna
M.Tech Student
Department of CSE
PNC & VIJAI Institute of Engineering and Technology,
Guntur, AP, India.

M.Aparna
Assistant Professor
Department of CSE
PNC & VIJAI Institute of Engineering and Technology,
Guntur, AP, India.

Abstract:

Location based services (LBS) is a utility services accessible by various devices and are part that virtually controls systems which work in computer Typically a GPS coordinates are sent as an input to the location servers and based on the GPS coordinate the point of interests can be served back to the client from the location server Proposed solution can be implemented on a desktop pcs laptops and mobile phones to assess the efficiency of implemented protocol. Proposed method also introduces a security model and analyzes the security in the context of implemented protocol. Finally this solution highlights a security weakness of previous systems work and presents a novel solution to overcome the disadvantages of previous work We suggest a foremost enhancement providing AES Algorithm security on user security and server security The solution many of us existing is actually successful and functional in most situations Privacy concerns are expected to rise as LBSs become more common. Location privacy means data privacy

Index Terms: ***Private Information Retrieval, Centroid, databases, location based queries, Privacy preserving.***

1. INTRODUCTION

There are increasing mobile phone users worldwide. So location technologies can be currently used by wireless carrier operators to provide a good forecast of the user location number of users are use location based services which can provide location-aware information.[1] The Location Based Service Location based service is a service accessible with mobile phones pocket PC's, GPS devices. It is like Google maps, map request. Mobile devices with positioning capabilities facilities access to location based services that provide information relevant to the user's geospatial context. Number of users uses these services for retrieving Points Of Interest from their current location.[2] LBS can be query based and provides the end user with useful information the normal. Area protection implies information security.[3] So here security certification is measure issue. On the other area server has their own particular database in which, number of purpose of interest records are found the server transform the solicitation and sends back the inquiry result to the client. So server needs to keep database access from unapproved client furthermore clients who have not pay for that administration [4].

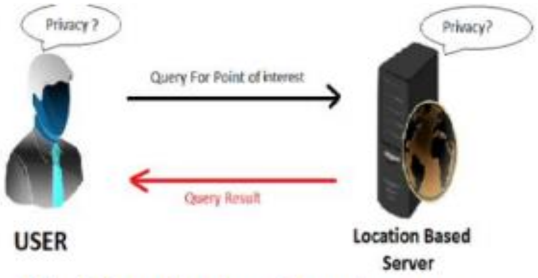
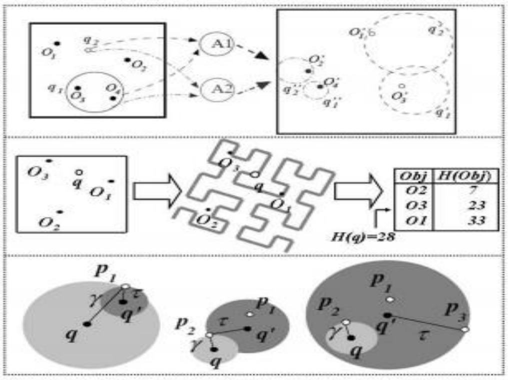


Fig.1 Location based service process

2. Related Work

It can be shown that, due to the nature of the data being exchanged between the user and the server, the frequent changing of the user's name provides little protection for the user's privacy. A more recent investigation of the mix-zone approach has been applied to road networks [11] They investigated the required number of users to satisfy the unlink ability property when there are repeated queries over an interval. This requires careful control of how many users are contained within the mixzone which is difficult to achieve in practice.[5] The concept of k-anonymity was introduced as a method for preserving privacy when releasing sensitive records [6] This is achieved by generalization and suppression algorithms to ensure that a record could not be distinguished from (k − 1) other records. The solutions for LBS use a trusted anonymiser to provide anonymity for the location data, such that the location data of a user cannot be distinguished from (k − 1) other users Preserving privacy under personal location is one of the greatest issues in wireless network. [7] They where many approach proposed for the privacy preserving policy under personal location. In many research articles they focus only on anonymization of location techniques but failed to preserve privacy under the network. Some privacy policy may cause data leakage problem because of inefficient algorithms the agents serve as intermediaries and do not store user information since their only responsibility is to transform information received from other users or the server. To preserve privacy, users randomly choose the agent to perform the transformation [8].



3. Background Orations

We introduce the system model, which defines the major entities and their roles The description of the protocol model begins with the notations and system parameters of our solution privacy-aware query processor. In order to enable location privacy, the anon miser maintains the current locations of all subscribed users.[9] Instead of sending the location query to the LBS, the user contacts the anon miser which generates a cloaked region enclosing the user as well as k – 1 other users in her vicinity There are various methodologies in the writing to take care of the issues of security insurance with area based administrations which incorporates shrouding, era of shams and private information retrieval (PIR). A correlative system to the mix zone methodology is in light of k-anonymity [2]. The idea of k-anonymity was presented as a system for protecting security when discharging delicate records [3]. This is accomplished by speculation and concealment algorithms to guarantee that a record couldn't be recognized from (K – 1) different record [10].There raised number of approaches in order to protect data and provide privacy to user during querying. New methods introduced and more challenges were faced for improvement by reconsidering known privacy metrics. There all approaches tried solve problem of privacy protect in their own way. Methods including: Cloaking; Generation of dummies; Private information retrieval [11].

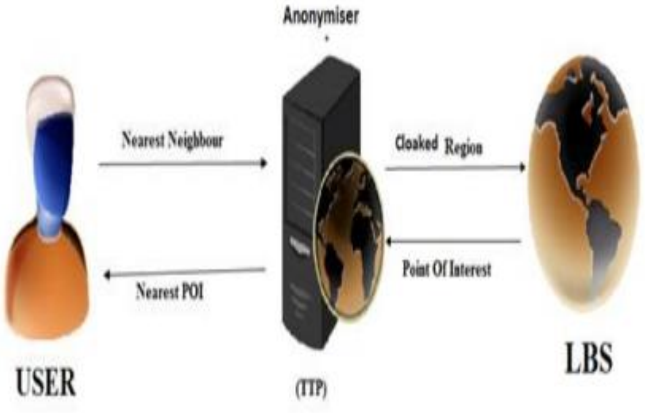
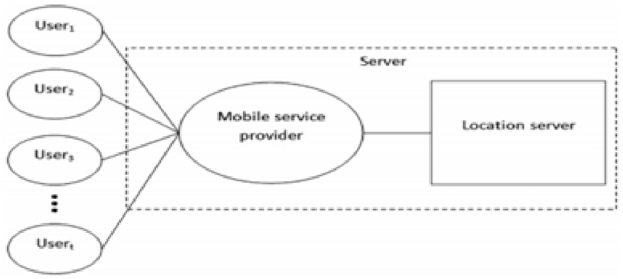


Fig 3- Location Based Service using TTP

The basic idea is to employ PIR [12] to enable the user to query the location database without compromising the privacy of user .Existing system requires clocked region and a TTP, but it doesn't need of anon miser[2] and privacy is achieve through cryptographic techniques. Here server forms the region regarding to POI and while answering to query, server first send regions to user

A. Preserving Techniques & Methods

There was work proposed in year 1999 that enable a user to access k replicated copies of a database and privately retrieve information stored in the database [6]. This means that each individual server (holding a replicated copy of the database) gets no information on the identity of the item retrieved by the user. This schemes and similar works, proposed very earlier use the replication to gain full real saving with multi-server. In particular, it's presenting a two-server scheme with less communication complexity. [13] Then as work progress, there was application of the anonymity set technique to location data collected. The anonymity set measurements gives information that pseudonymity technique cannot give users adequate location privacy.



B. PROBLEM STATEMENT

Existing system involve two protocols namely oblivious transfer and private information retrieval [8]. But these protocol doesn't work on different mobile devices and additional problem will arise that location server LS should supply misleading data to client is also interesting. Compared to previous work, we have to achieve reasonable communication and CPU cost. It's better to use ATTP free protocol for location privacy in location based services [14].

C. Security Analysis:

User Security:

The user does not want to disclose the cell Pi,j which contains his/her location to the server. Two assumptions must be maintained in order to effectively render location private. The server must not be able to determine which cell the user is querying in the oblivious transfer protocol, and the server must not be able to determine which cell the user is querying in the private information retrieval protocol [15]

Server's security:

The server's security is based on keeping the boundaries of its records private. Since disclosing this information may enable the user to infer more information about the database than he/she is allowed. In our solution this information is protected by the oblivious transfer protocol. The user is forced to retrieve one and only one record from the public grid Pi,j All other times, the result will be indistinguishable from random. [16] Under the discrete logarithm problem assumption, it is computationally intractable to determine any exponent from the cipher text.

4. PROPOSED WORK

We propose a novel convention for area based inquiries that have significant execution changes concerning the methodology and [8] such convention; our convention is sorted out as per two stages. In the first stage the client secretly decides his area inside of an open lattice [17].

1. System Model

The framework model comprises of three sorts of elements the arrangement of clients who wish to get to area information, a portable mobile service provider SP, and an location server LS. From the perspective of a client, the SP and LS will form a server, which will serve both capacities [18] The client does not should be worried with the correspondence's specifics. The clients in our model utilize some area based administration gave by the location server LS. For instance The base measurements of general society lattice are characterized by the server and are made

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

accessible to all clients of the framework.[19] This open framework superimposes over the secretly apportioned network produced by the area server's POI records, such that for every cell Qi,j in the server's allotment there is no less than one Pi,j cell from general society matrix. Since PIR does not oblige that a client is compelled to acquire stand out bit/hinder, the area server needs to execute some insurance for its records [20].

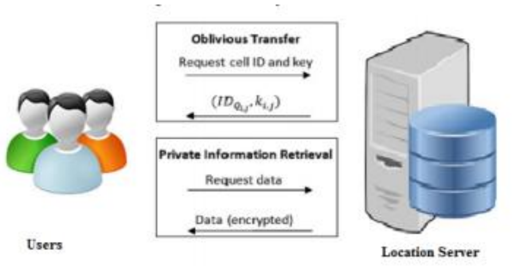
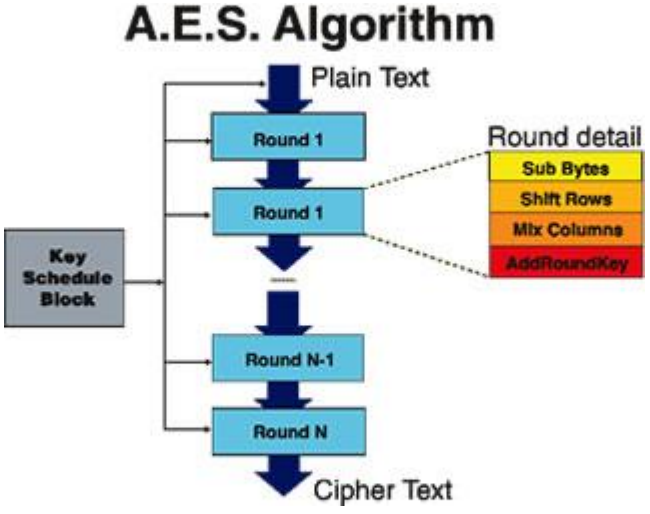
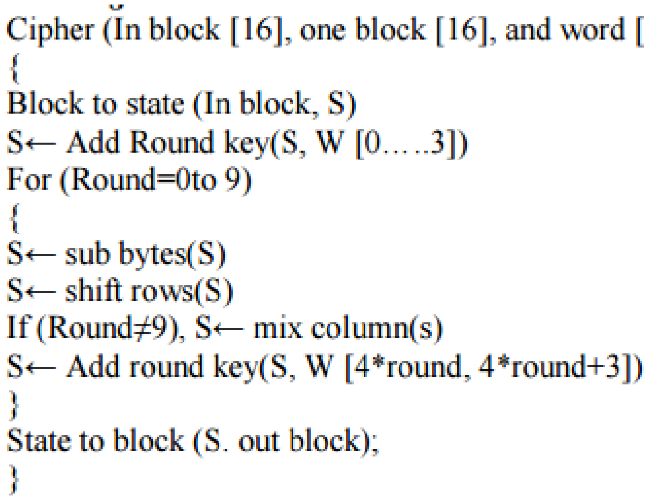


Fig.3 High Level Overview of the Protocol

2. AES Algorithm



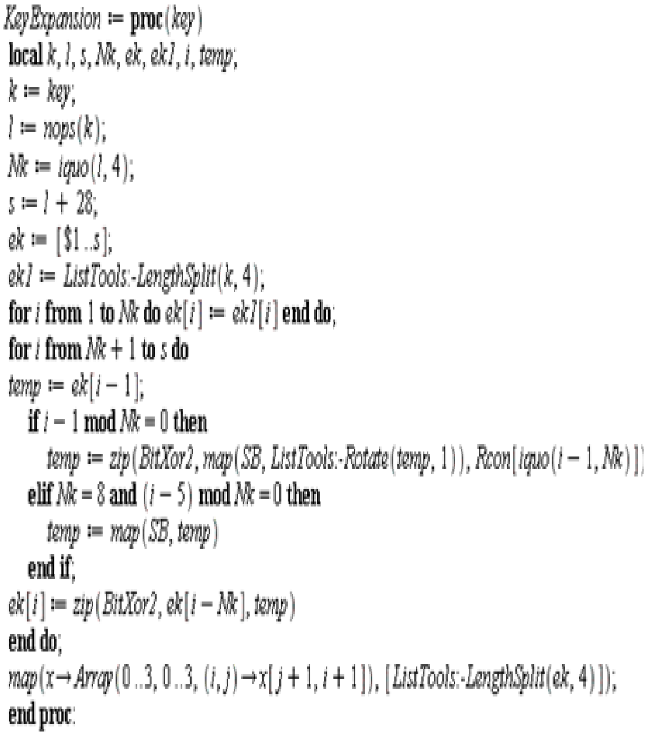
The source node might want to send information for the destination around then we perform the security achievement sending the information to the destination the source node can impart the security key to the assistance of AES algorithm subsequent to sharing the key the source node can scramble the information by utilizing cryptographic[7] algorithm. Encoded information exchanged from source to destination, amidst transmission the assailants through middle of the road nodes need to get to the information there will be no impact on the information, because of scrambling the information, the first information as it is send to its destination node



```
Cipher (In block [16], one block [16], and word [
{
Block to state (In block, S)
S← Add Round key(S, W [0.….3])
For (Round=0to 9)
{
S← sub bytes(S)
S← shift rows(S)
If (Round≠9), S← mix column(s)
S← Add round key(S, W [4*round, 4*round+3])
}
State to block (S. out block);
}
```

3. Key Expansion

Round keys are derivative from the cipher key To create round keys for each round AES algorithm uses a key expansion process. If the number of rounds is Nr the key-expansion routine creates Nr + 1 128-bit round keys from one single 128-bit cipher key [11].



```
KeyExpansion := proc(key)
local k, l, s, Nk, ek, ek1, i, temp;
k := key;
l := nops(k);
Nk := iquo(l, 4);
s := l + 28;
ek := [$1 ..s];
ek1 := ListTools:-LengthSplit(k, 4);
for i from 1 to Nk do ek[i] := ek1[i] end do;
for i from Nk + 1 to s do
temp := ek[i − 1];
    if i − 1 mod Nk = 0 then
        temp := zip(BitXor2, map(SB, ListTools:-Rotate(temp, 1)), Rcon[iquo(i − 1, Nk)])
    elif Nk = 8 and (i − 5) mod Nk = 0 then
        temp := map(SB, temp)
    end if;
ek[i] := zip(BitXor2, ek[i − Nk], temp)
end do;
map(x→Array(0 ..3, 0 ..3, (i, j)→x[j + 1, i + 1]), [ListTools:-LengthSplit(ek, 4)]);
end proc:
```

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

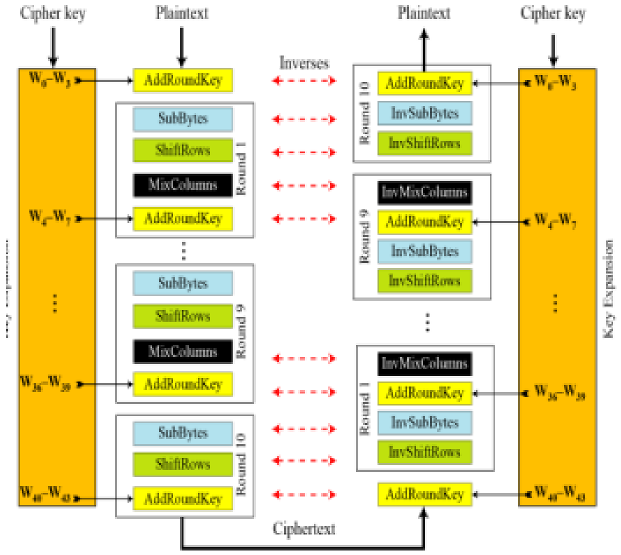


Fig.4 Architecture of AES

5. Conclusion:

We have presented a location based query solution that employs two protocols that enables a user to privately determine and acquire location data more efficient than the solution the most recent solution. Authors implemented a software prototype using a desktop machine and a mobile device. The software prototype demonstrates that protocol is within practical limits The proper maintenance of privacy and the detection of the query that violate privacy is the aim to look upon in process of transfer and retrieval of data between user and server. Working on PIR and related work proved adaptive method different ways a framework that while ensuring perfect privacy, can very efficiently respond to various spatial queries dealing with both static and dynamic objects is still an open problem and far from what the existing approaches offer there is need to reduce the overhead of the primarily test used in the private information retrieval based protocol and security.

6. Future Work

Future work could be done in efficient way and faster in much more real time. This could be contribution to the system further Any opinions, findings, and conclusions recommendations expressed in this material are those of the author do not necessarily reflect the views of the National Science Foundation We investigations the presentation of our convention and observed it to be both computationally and communicational more which the latest arrangement is. We executed a product model utilizing a desktop machine. The program prototype demonstrates that our project is at useful restrictions

7. REFERENCES

[1] (2011, Jul. 7) Openssl [Online]. Available:

[2] M. Bellare and S. Micali, “Non-interactive oblivious transfer and applications,” in Proc. CRYPTO, 1990, pp. 547–557

[3]G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, “Approximate and exact hybrid algorithms for private nearest neighbour queries with database protection

[4]B. Palanisamy and L. Liu, “MobiMix: Protecting location privacy with mix-zones over road networks,”

[5] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, ”Private queries in location based services: Anonymizers are not necessary”, in Proc. ACM SIGMOD, Vancouver, BC, Canada, 2008, pp. 121-132.

[6] M. Naor and B. Pinkas,”Oblivious transfer with adaptive queries”, in Proc. CRYPTO, vol. 1666, Santa Barbara, CA, USA, 1999, pp. 791-791.

[7] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in Proc. EUROCRYPT, vol. 1592, Prague, Czech Republic, 1999, pp. 223–238.

[8] M. Duckham and L. Kulik, “A formal model of obfuscation and negotiation for location privacy,” in Proc. 3rd Int. Conf. Pervasive Comput., H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, pp. 243– 251, LNCS 3468.

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

[10] R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino, "Privacypreserving and content-protecting location based queries," in Proc. ICDE, Washington, DC, USA, 2012, pp. 44–53.

[11] G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacypreserving matching of spatial datasets with protection against background knowledge," in Proc. 18th SIGSPATIAL Int. Conf. GIS, 2010, pp. 3–12

[12] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," in Proc. CRYPTO, vol. 1666, Santa Barbara, CA, USA, 1999, pp. 791–791

[13] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection," GeoInformatica, vol. 15, no. 14, pp. 1–28, 2010

[14] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in Proc. Int. Conf. ICPS, 2005, pp. 88–97.

[15] J. Krumm, "A survey of computational location privacy," Pers. Ubiquitous Comput., vol. 13, no. 6, pp. 391–399, Aug. 2009

[16] Deepika Nair, Bhuvaneswari Raju "Privacy Preserving in Participatory Sensing" in IJSR,Volume 3 Issue 5, May 2014

[17] R.Paulet, M.GolamKaosar, X.Yi,andE.Bertino,"Privacypreserving and content-protecting location based queries," in Proc. ICDE, Washington, DC, USA, 2012, pp. 44–53

[18] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," inProc. 3rd Int. Conf. Pervasive Comput., H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, pp. 243–251, LNCS 3468.

[19] L. Sweeney, "k-Anonymity: A model for protecting privacy," Int. J. Uncertain. Fuzziness Knowl. Based Syst., vol. 10, no. 5, pp. 557–570, Oct. 2002

[20] A. Beresford and F. Stajano, "Location privacy in pervasive com-puting,"IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar.2003.

Author Details

Yellinedi Hari Krishna was born in Sattenapalli, Guntur Dt, AP. He received B.Tech in IT from Nalanda Institute of Engineering & Technology, JNTU Kakinada in the year 2011. Presently he is pursuing M.TECH in CSE from P.N.C & VIJAI Institute of Engineering & Technology, Phirangipuram, Guntur Dt, Andhrapradesh, India. He attended various National Workshops on Data Mining.

M.Aparna Received B.Tech degree from BVC College of Engineering and Technology, Amalapuram affiliated in JNTUK University and M.Tech Degree from EVM College Of Engineering and Technology, Narasaraopet. Currently she is working as Asst. Professor in CSE department from PNC&VIJAI Institute of Engineering and technology, Guntur. She has 4 years of experience in teaching. Her Interested papers are Computer Networks, Data Warehousing and Data mining and Web Technologies.