AES Enabled Private Information Retrieval Scheme for Location Based Queries

Lothe Ashwini Bhaskar[1], **Apare Ravindra S**[2]

[1, 2]SPPU, Pune, Department of Information Technology, Smt. Kashibai Navale College of Engineering, Pune,India

Abstract: ***Various issues are embarrassing while using Location Base Search, Out of this preserving privacy and protecting content for Location Base queries is the in wireless concern. User fires question to get location base information but do not wish to expose his coordinate to the server and at the server will only send data to the validate user. For preserving privacy, user hides its coordinate through encryption and send to the server, information at a server is secured since a malicious user can only decrypt the block of data, accept by Private Information Retrieval (PIR) with the encryption key acquired in the previous stage. In earlier work ElGamal encryption scheme is used for encryption has some disadvantage like a need for randomness and its slower speed. Another potential problem of the ElGamal system is that message expansion by a factor of two takes place during encryption. To overcome problems as quoted earlier, Advanced Encryption Scheme (AES) is proposed here for the encryption of data. Recommended scheme is distinguished by using time and speed parameter.***

Keywords: Location Server, LBS, Oblivious Transform, PIR

1. Introduction

Due to rapid growth in wireless communication technologies and due to the internet enabled mobile devices peoples are focusing on Location Base Services. These wireless devices are quicker and easiest way for communication.

Location Base Services (LBS) are information Services which provide relevantly, precise information to the subscriber. When user search through LBS, it can give various services which provide Points of Interest (POIs) to the users depends upon the geographical area of their handheld devices. By querying the Points of Interest data from the server, the loyal user can gain multiple answers to multiple problems depend on location base data, which include but not fixed to search the ATM, petrol pump, or police station. [1]

Various Issues regarding privacy involve in Location Base Search In which privacy of the user is a primary concern. In this paper, user privacy is protected by hiding its location coordinate from the location server, and obtaining position information ongoing basis from the server by using Oblivious Transformation [2]. When Location system detects users coordinates ongoing basis it’s generate a tiny amount of potentially sensitive information. Location tracking feels user unsecured and usually avoid to use location search devices.

The user cannot restrict all access to be coordinate because various applications can want this information to provide useful services but user wants to be in control. Some aims are distinct mutually exclusive and cannot be concurrently obtained, for example, wanting to keep user's Location information secret and yet wanting colleagues to be able to locate the user. Despite this, there is still a scope of significant variations to be explored. The Location Server (LS), which give some LBS, utilize its resources to process data about different places. Hence, it is supposed that the LS would not uncover any information without the fee. Therefore the LBS have to guarantee that LS's data is gain only by the authorized user. During the process of transmission of information to the users, should not be allowed to get any data for which they have not charge. It is thus essential that solutions be devised that solve the privacy of the users issuing queries, but also secure peoples from obtaining information to which they do not have authorization.

2. Related Work

When location systems track users through GPS, they generate an enormous amount of potentially private information it is impossible to stop all path, but some constraint are involved. Privacy of location information is about controlling access to this information. It is not necessary to prevent all access because some applications can use this information to provide useful services. In [3], a privacy-protecting framework based on frequently changing pseudonyms is trained, so users avoid being identified by the locations they visit. This framework is further developed by introducing the concept of mix zones and showing how to map the problem of location privacy onto that of anonymous communication. It Grants us access to a growing body of theoretical tools from the information-hiding community. In this context, two metrics are developed for measuring location privacy, one based on anonymity sets and the other based on entropy. As the temporal and spatial resolution of the location data generated by this approach is high, location privacy is small, even with a moderately large mix zone.

Mix-zones acknowledged as an option and joint approach to spatial cloaking based approach to location privacy protection. Mix-zones break the continuity of location appearance by ensuring that users' movements that cannot be discovered while they reside in a mixing zone. [14] [4] illustrate a set of counter measures to make road network mix-zones attack resilient. The vulnerabilities of road network mix-zones identify into two classes: one expected to the road network components and user mobility, and the other due to the temporal, spatial and semantic correlations of area queries. For instance, the timing data of users' entry and exit into a mix-zone provides information to originate a timing attack. The non-uniformity in the changes taken at the road junction may lead to transition attack. They investigated the required number of users to satisfy the unlinkability property when there are repeated queries over an interval. It requires rigorous control of how many users contains within the mix-zone, which is hard to achieve in practice.

Solution to privacy protection problem provided in [5][14] involves a formal security structure device an announcement provides k-anonymity protection if the information for each person contained in the statement cannot classify from at least k-1 people whose data also seems in the release. It also checks re-identification attacks that can realize on releases that adhere to k-anonymity unless accompanying policies are respected. The k-anonymity protection model is significant because it forms the basis on which the real-world systems known as Data fly, μ-Argus and k-Similar provide guarantees of privacy protection.

Composite Residuosity Class Problem and its applications to public-key cryptography examined in [6] [14]. Trapdoor mechanism was introduced and from this mechanism, three encryption schemes such as a trapdoor permutation and two homomorphic probabilistic encryption schemes are proposed. This cryptosystem, based on usual modular arithmetic, are provably secure under appropriate assumptions in the standard model. But it does not provide any proof of security against chosen ciphertext attacks.

In [7] [14], a framework is proposed to support individual location-dependent queries, based on the theoretical work on Private Information Retrieval (PIR). It does not require trusted the third party since privacy achieved via cryptographic techniques. Compared with other methods, this approach produces stronger privacy for snaps of user locations; moreover, it is the first to present provable privacy guarantees against similarity attacks. This framework is used to implement approximate and exact algorithms for nearest-neighbor search. It optimizes query execution by employing data mining techniques, which redundant identity computations. Contrary to common belief, the experimental results suggest that PIR approaches incur reasonable overhead and are applicable in practice. This method requires the extension of this framework to different types of queries, such as spatial joins.

Hashem and Kulik presented a scheme [14] [8] whereby a group of trusted user's constructs graphs location server assigned to a single user. This idea is different from the previous works by the fact that there is no single point of defeat. If a user that is questioning the LS abruptly goes offline, then another candidate can be easily found. However, forming a trusted ad-hoc network in a real world scenario is not always possible.

Some methods have also been suggested to confuse and distort the location data, which include path and position confusion. Route confusion was done by Hoh and Gruteser [14][12]. The basic idea is to add dilemma to the position details of the users at the points the routes of the users cross, making it laborious to discover users based on new location data that was k-anonymized. Status confusion has also proposed as an approach to providing privacy [10] [11].

Contents enciphered document and delivered to whom those have key Document broadcasting based on access control policy, but in this approach scalability and optimization issue and also Need to implement fast linear algebra operation[9][14].

In [1], each coordinate of the location encrypts in the oblivious transfer by ElGamal Encryption scheme. Here, the first impediment to ElGamal encryption scheme is the need for randomness, and it is delayed speed. Slower Speed. Another potential limitation of the ElGamal system is that message expansion by a factor of two takes place during encryption. To overcome these obstacles, Advanced Encryption Scheme (AES) is proposed here for the encryption of data. The associated symmetric key for the block of information in the single grid. In the second stage, the user executes a communicational efficient PIR [5], to retrieve the appropriate block in the private network. This block is decrypted applying the symmetric key achieved in the previous stage. This protocol thus provides protection for both the user and the server. The user preserved because the server is unable to determine his/her location. Similarly, the server's data is protected by a malicious user can only decrypt the block of data concerned by PIR with the encryption key taken in the preceding stage. In other words, users cannot gain any more data than what they have paid for.

3. System Architecture

Three things outline in figure num.1 it includes service provider*(SP*), end users who search for location data and the one who give solutions that are location server LS. The user does not need to be bothered with the specifics of the communication.

In architecture are assuming that the mobile service provider *SP* is trusted to maintain the connection, consider only two possible opponents. One for each transmission command. Consider the case in which the user is the opponent and tries to obtain more than he/she is allowed. Next, we reconsider the case in which the location server *LS* is the opponent, and tries over connect uniquely a user with a grid coordinate.

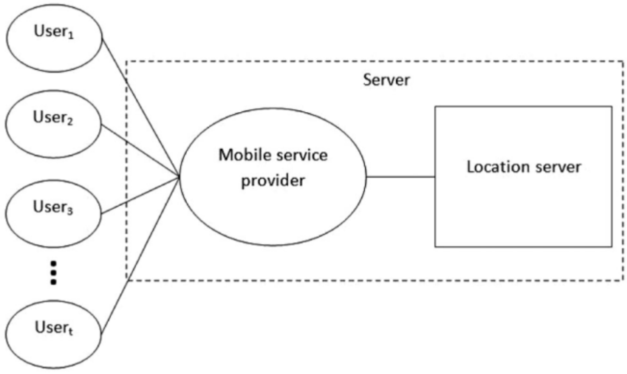


Figure 1: System model of base location search[1]

a) An AES enabled private information retrieval

In this work, a novel protocol for location-based queries that have significant performance improvements over the existing approaches is proposed. The protocol designed according to two stages. In the first phase, the user privately determines his/her location within a public grid, using the oblivious transfer. This data includes both the ID and associated symmetric key for the block of data in the own network. In the second stage, the user performs a communicational efficient PIR [1], to retrieve the appropriate block in the private network. This block is decrypted practicing the symmetric key recovered in the preceding stage.

This protocol thus gives protection for both the user and the server. The user keeps because the server is unable to resolve his/her location. Similarly, the server's data is protected by a malicious user can only decrypt the block of data received by PIR with the encryption key derived from the earlier stage. In other words, users cannot gain any more data than what they have been paid for.

In [1], each coordinate of the position encrypts in the oblivious transfer by ElGamal Encryption scheme. Here, the main flaw of ElGamal encryption design is the recognized for randomness, and it is slower speed. Another possible limitation of the ElGamal system is that message expansion by a factor of two takes place during encryption. To overcome these objections, Advanced Encryption Scheme (AES) is proposed here for the encryption of data as shown in figure no. 2.

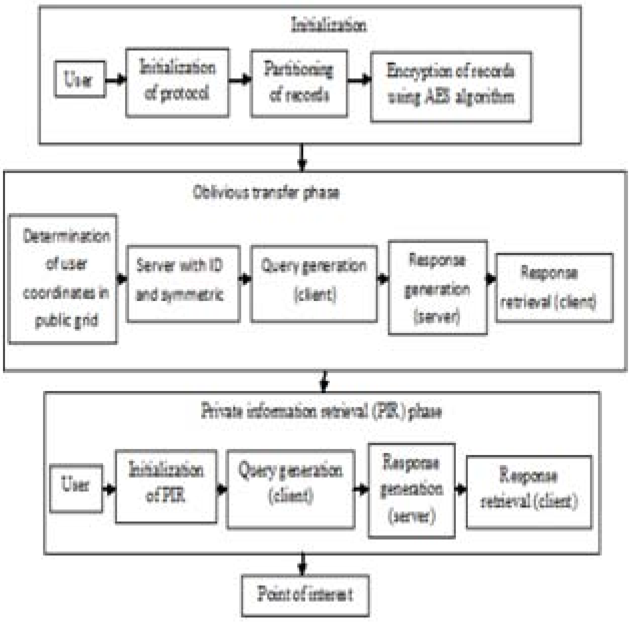

Initialization
User
Initialization of protocol
Partitioning of records
Encryption of records using AES algorithm
Oblivious transfer phase
Determination of user coordinates in public grid
Server with ID and symmetric
Query generation (client)
Response generation (server)
Response retrieval (client)
Private information retrieval (PIR) phase
User
Initialization of PIR
Query generation (client)
Response generation (server)
Response retrieval (client)
Point of interest

Figure 2: Block Diagram for AES enabled private information retrieval

b) Mathematical Formulation:

Let x ← y be the responsibility of the value of variable y to v variable x and $E \Leftarrow v$ be the directions of the variable v to entity E. g is a generator of group G, y is the public key of the form y = ,X and r are selected at random. It uses as a basis for constructing an adaptive oblivious transfer scheme [13]. The cyclic group G_0 is a multiplicative subgroup of the finite field F_p, where p is a large prime number and q are original that divides $(p - 1)$. Let g_0 be a generator of group G_0, with order q. Let G_1 be a multiplicative subgroup of finite field F_q, with many generators g_1 and g_2 where both have prime order $q'|(q - 1)$. Based on this definition, groups G_0 and G_1 can then be linked together and have the form $g_0{}^g{}_1{}^g{}_2$ where x and y are variable integers. Further will be used in our application to produce an Advanced Encryption Scheme instance in-groupG_1.$|p|$is denoted to be the bit length of p, $\oplus$ to be the exclusive OR operator, $a||b$to be the connection between a and b, and $\left|\langle g \rangle\right|$ to be the order of generator g. For security reasons, it is required that $|q'| = 1024$ and p has the form $p = 2q' + 1$. It is also necessary that the parametersG_0, g_0, G_1, g_1, g_2, p, q' be fixed for the term of around of our protocol and be made publicly accessible to every entity in our protocol.

4. Algoritham

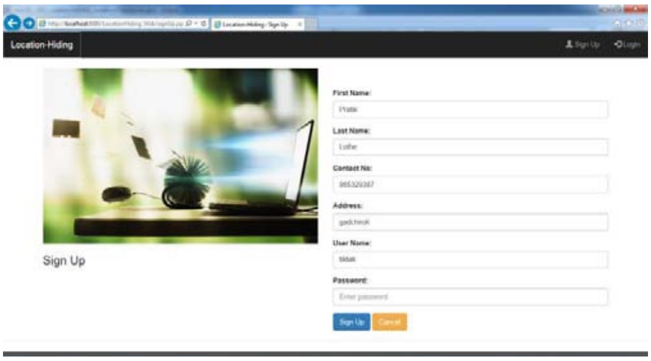
Proposed algorithm where existing system differentiated from base system

```
Input: X1,1, ..., Xm,n, where Xi,j = IDQi,j ||ki,j
Output: Y1,1, ..., Ym,n
Ki,j ← Ki,j = gRi ||gCj , for 1 ≤ i ≤ n and 1 ≤ j ≤ m,
where Ri and Cj are randomly chosen
Yi,j ← Xi,j ⊕ H(Ki,j ), for 1 ≤ i ≤ n and 1 ≤ j ≤ m,
where H is a fast secure hash function
return Y1,1, ..., Ym,n {Encryptions of X1,1, ..., Xm,n
using Ki,j}
```

In this algorithm contain Advance Encryption Standard for data hiding .

5. Result and Discussion

The proposed scheme will be implemented using JAVA programming, and the performance of the proposed scheme will be validated using comparison with state of the art. The progress of execution is displayed on the screen one by one. The press messages contain the following information. Task/process done figure 3 presents sign up a page for new customer .only validate customer can log into it.



Sign Up

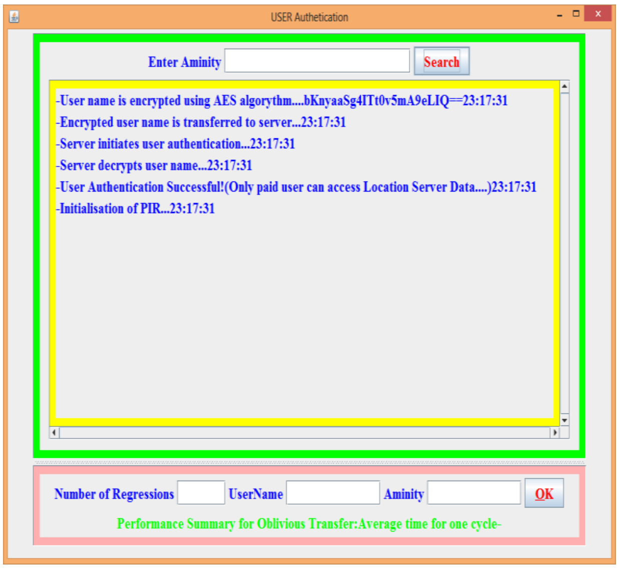
First Name: [illegible]
Last Name: [illegible]
Contact No: [illegible]
Address: [illegible]
User Name: [illegible]
Password: Enter password

Figure 3: Singn up Page for new Customer

Regression Steps:

To display the regression steps done, and results for the bulk number of iterations log maintain as shown below, an as the process is very fast and for a small number of regression cycles the results will be in milliseconds. It would be challenging the user to demonstrate the regression in milliseconds. So keep the iterations to 200 or above. Use the vertical scroll bar to peruse all the progress messages displayed on the screen. Progress results for the regression are given on the screen. The progress message has following information. Task/Activity done, Value/status in case some processing are done, and Timestamp. Messages displayed at the end of regression. Value/status, timestamp is shown in figure 4, 5 and 6.

In figure number 4 when user logged in he/she will enter their logging credentials that oblivious transformation takes place by encrypting user throw AES algorithm, then ittransferred username to server decrypt user name and checked for authentication



Enter Aminity

```
-User name is encrypted using AES algorythm....bKnyaaSg4ITt0v5mA9eLIQ==23:17:31
-Encrypted user name is transferred to server...23:17:31
-Server initiates user authentication...23:17:31
-Server decrypts user name...23:17:31
-User Authentication Successful!(Only paid user can access Location Server Data....)23:17:31
-Initialisation of PIR...23:17:31
```

Number of Regressions UserName Aminity

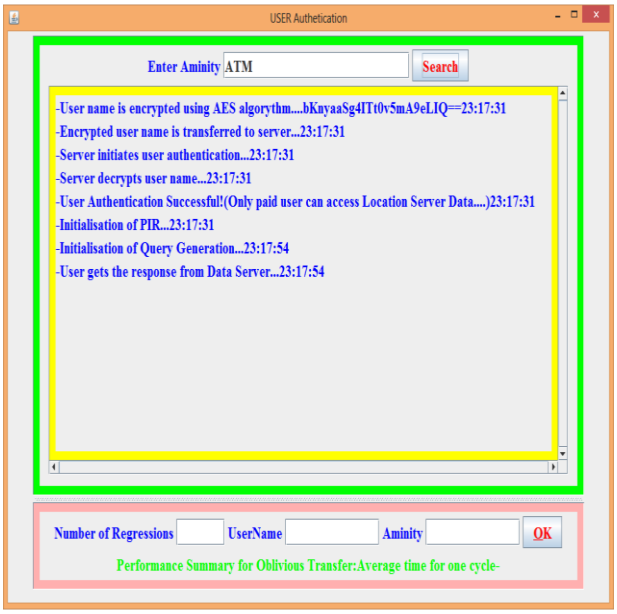
Performance Summary for Oblivious Transfer:Average time for one cycle-

Figure 4: User Authentication

Table 1: AES Enabled Oblivions Transform Experimental Result forDesktop

Component	AvrageTime (millisecond) for Desktop
Query Generation	-
Response Generation	23

After successful Authentication server asks for amenity he wants and initialization of Private Information Retrieval Phase Takes Place. Result from server reply is specified in graph



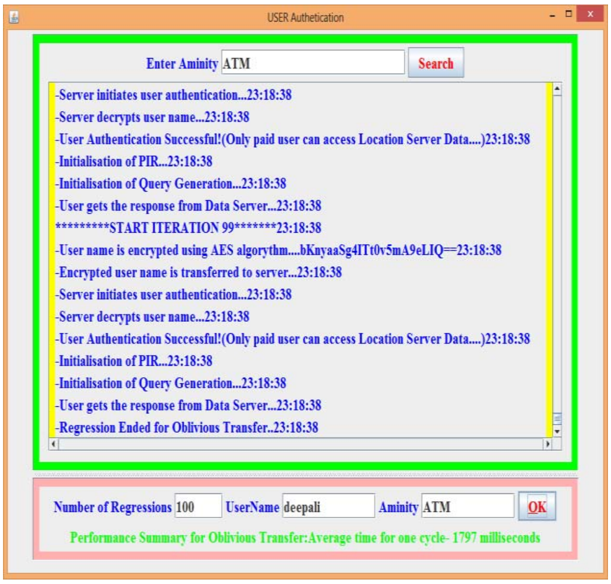
Enter Aminity ATM

```
-User name is encrypted using AES algorythm....bKnyaaSg4ITt0v5mA9eLIQ==23:17:31
-Encrypted user name is transferred to server...23:17:31
-Server initiates user authentication...23:17:31
-Server decrypts user name...23:17:31
-User Authentication Successful!(Only paid user can access Location Server Data....)23:17:31
-Initialisation of PIR...23:17:31
-Initialisation of Query Generation...23:17:54
-User gets the response from Data Server...23:17:54
```

Number of Regressions UserName Aminity

Performance Summary for Oblivious Transfer:Average time for one cycle-

Figure 5: Execution flow Until Oblivious Transform



Enter Aminity ATM

```
-Server initiates user authentication...23:18:38
-Server decrypts user name...23:18:38
-User Authentication Successful!(Only paid user can access Location Server Data....)23:18:38
-Initialisation of PIR...23:18:38
-Initialisation of Query Generation...23:18:38
-User gets the response from Data Server...23:18:38
*********START ITERATION 99*******23:18:38
-User name is encrypted using AES algorythm....bKnyaaSg4ITt0v5mA9eLIQ==23:18:38
-Encrypted user name is transferred to server...23:18:38
-Server initiates user authentication...23:18:38
-Server decrypts user name...23:18:38
-User Authentication Successful!(Only paid user can access Location Server Data....)23:18:38
-Initialisation of PIR...23:18:38
-Initialisation of Query Generation...23:18:38
-User gets the response from Data Server...23:18:38
-Regression Ended for Oblivious Transfer..23:18:38
```

Number of Regressions 100 UserName deepali Aminity ATM

Performance Summary for Oblivious Transfer:Average time for one cycle- 1797 milliseconds

Figure 6: logiging log

Respected graph illustrated in figure shows, the difference between each query execution Summary of regression output displayed on the screen as shown in above figure no.5 in average Milliseconds.F

Table 2: AES Enabled Private Information RetrivalExperimental Result forDesktop

Component	AvrageTime (millisecond) for Desktop
Query Generation	-
Response Generation	850

Figure 7: Execution Flow

An output of user point of interest within millisecond is mentioned in below diagram, shows securing users privacy and by protecting the content of users. Figure no 8 shows the desired result.

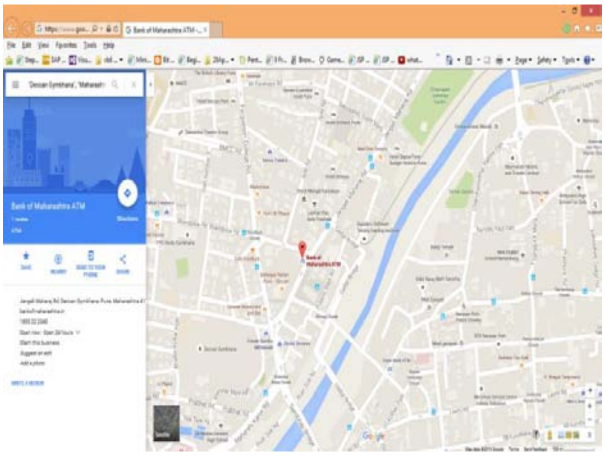


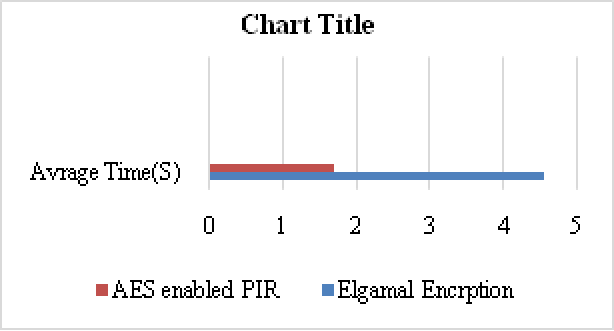
Figure 8: Create profile

Comparative Result between ElGamal encryption for preserving privacy and content at location base search and AES enabled PIR for location base Query as shown in Table No. 3

Table 3: Comparative Result between Base and Proposed work

Component	AvrageTime(second) for Desktop	
	El Gamal (Based system)	AES Enabled PIR(Proposed System)
Query Generation	-	-
Response Generation	4.57	1.79

Resultant graph showing deference between existing and proposed system



6. Conclusion and Future Scope

This work device an AES enabled scheme for location-based queries, and that has significant performance improvements on the ElGamale encryption system. This solution works on a desktop machine and a mobile device to assess the efficiency of our protocol. Also, introduce a security model and analyze the security in the context of our protocol. Results are measured by using time and speed, and both parameters have significance changes over previous work. Finally, this paper highlights a security weakness of earlier work and present a solution to overcome it. Future work includes reducing some overhead in PIR Phase. Also, we can use MD5 instead of AES scheme.

References

[1] Russell Paulet, Md. Golam Kaosar, Xun Yi, and Elisa Bertino, "Privacy-Preserving and Content-Protecting Location Based Queries", IEEE Knowledge and Data computing., vol. 26, no. 5, pp. 1200–1210, May 2014.

[2] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," in Proc. CRYPTO, vol. 1666, Santa Barbara , CA , USA, ,1999 ,pp.79

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

[4] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," in Proc. ICDE, Hannover, Germany, 2011, pp. 494–505.

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

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

[7] 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.

[8] T. Hashem and L. Kulik, "Safeguarding location privacy in wireless ad-hoc networks," in Proc. 9th Int. Conf. UbiComp, Innsbruck, Austria, 2007, pp. 372–390.

[9] Ning shang Mohamed Nabeel, Federica paci, Elisa Bertino ," A privacy preserving Approch to policy –Based Content Dissemination" in IEEE Purdue university ,west Lafayette, Indiana, USA-2010

[10] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services withoutcompromising privacy," in Proc. VLDB, Seoul, Korea, 2006, pp. 763–774

[11] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventinglocation-based identity inference in anonymous spatial queries,"IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733,Dec. 2007

[12] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in Proc. 1st Int. Conf. SecureComm, 2005,pp 194–205.

[13] 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.

[14] AshwiniB.Lothe,R.S.Apare"Survey on Securing Privacyand Protecting Content of Location Based Queries" International Engineering Research Journal (IERJ) Volume 1 Issue 11 Page 1606-1609, 2016, ISSN 2395-1621.