Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (159-166), Month: January-April 2016, Available at: www.noveltyjournals.com

Enhancing Location Based Privacy Policies for Geospatial Applications

[1]N.Jayapratha, [2]J.Jayavel

[1,2] Information Technology Anna University Regional Campus CBE India

***Abstract*: Four Square is one of Geo spatial analysis in which lots of communities interrelate with their surrounding environment through their friends and recommendations. We must have to take care of our data and Location. But this is not possible every time sometimes because of busy time we can't take care of our data without sufficient location protection. However, these application can be easily misused. So, we proposed enhanced location privacy policies in Geo spatial networks. A technique that provides location secrecy without adding complexity into query results. Idea here is to secure user specific data and coordinate conversation to all location data shared with the database server. To provide privacy in server using Location index mapping and distance preserving coordinate transformation. The associates of a user share this user's secret key. This allows all spatial queries to be evaluated correctly by the server but privacy mechanisms guarantee that servers are unable to infer the actual location data from the transformed data and easily through the data access.**

Keywords: **Camera shake, Deconvolution, Fourier spectrum magnitude, Fourier burst accumulation.**

I. INTRODUCTION

A. Data Security:

Data security protects a data, such as database from destructive forces and the unwanted actions of unauthorized users. It refers to protective digital privacy measures are applied to prevent unauthorized access to computers, databases and websites. It also protects data from corruption. It is the practice of information from unauthorized access, use, disclosure, destruction. It is a general term can be used regardless of the form the data may take. Most of information is now collected processed and stored on the electronic computers transmitted across networks to other computers. The individual, it has a significant effect on privacy, which is viewed differently in different cultures. Data security is main priority for the organizations of every size. Data security also known as the information security or computer security. The field of data security has grown and evolved significantly in recent years.

B. Key Concepts:

Confidentiality:

Confidentiality refers to preventing the disclosure information to unauthorized individuals or systems. A credit card transaction on the internet requires credit card number to be transmitted from the buyer to the merchant to a transaction processing network. Confidentiality is necessary to maintaining the privacy of the people whose personal information is in the system.

Integrity:

Data integrity maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means the data cannot be modified an unauthorized or undetected manner. This is not the same as referential integrity in databases, although it can be viewed as special case of consistency understood in the classic ACID model of transaction process. Integrity is violated when a message is actively modified in transmit. Information security systems typically provide message integrity to data confidentiality.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (159-166), Month: January-April 2016, Available at: www.noveltyjournals.com

Authenticity:

In computing, e-Business and data security, it is necessary to ensure that the data, transactions, communications and documents are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some data security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and it is sent by someone possessing the proper signing key.

Non-Repudiation:

In law, non-repudiation implies ones intention to fulfil their obligations to a contract. It also implies that one party of a transaction cannot deny having receive a transaction nor the other party deny having sent a transaction. It is important to note that technology such as cryptographic systems can assist in nonrepudiation efforts, the concept is its core a legal concept transcending the realm of technology.

C. Cryptography:

Data security uses cryptography to transform usable information into a form that is unusable by anyone other than authorized user that process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back to its original usable form by an authorized user, who possesses the cryptography key, through the process of decryption. Fig 1.1 shows that the cryptography process using shared secret key between the sender and receiver. Cryptography is used information security to protect information from unauthorized or accidental disclosure while the information is transit and while information is in storage.

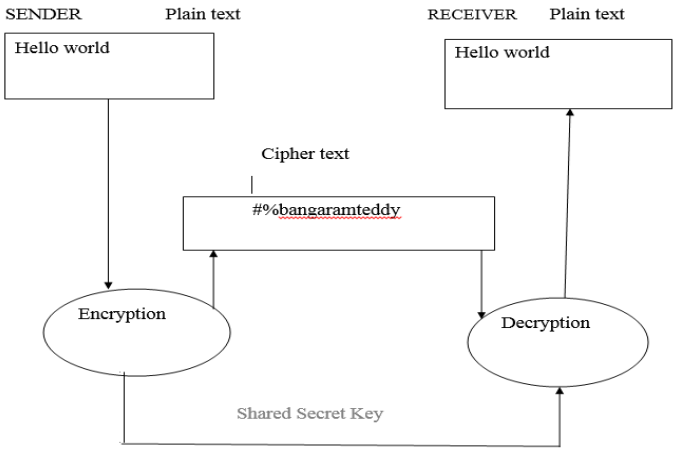

Fig. 1 Cryptography process

The keys used for encryption and decryption is to be protected to the same degree of rigors as any other confidential information. They must protected from unauthorized disclosure and destruction and they must be available when needed.

In this paper ***Section (2),***deals with the various other methods used for geospatial application for hide the data and location, ***Section(3),***focuses on the proposed method for secret key generation and providing user information to authorized users and ***Section(4),***explains the Analysis and Results of the proposed model which is been developed in java where is done.

II. LITERATURE SURVEY

[5] Today's geosocial applications raise security concerns because of use suppliers putting away a lot of data about clients (e.g., profile information) and locations. We tend to propose Zero square and foursquare, a privacy-friendly location hub encourages the event of privacy preserving geosocial applications. To utilize secure client particular, separation safeguarding direction changes to any otherwise all area learning imparted to the server. A unique approach to achieving user privacy where maintaining full accuracy in location-based social applications (LBSA).

[6] Location cloaking allows user privacy to be better protected. Unfortunately, this scheme can also reduce the quality of service provided by the location based service. Because the LBS does not have the most accurate information to provide

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (159-166), Month: January-April 2016, Available at: www.noveltyjournals.com

best service. Consider remote cab service that allows a subscriber to call for a cab nearby. If the subscriber reports her precise location, the service provider closest cab, and can tell the cab driver how to reach the customer. However, only vague location is given, it may take more time for a cab to reach the customer. By adjusting the accuracy of the location information sent to the service provider trade can be achieved between: (1) privacy of the user, and (2) quality of a service requested.

[7] Advances in sensing and tracking technology enable location-based applications but they also create significant privacy risks. Anonymity can provide high degree of privacy, save service users from dealing with service providers privacy policies and reduce the service providers requirements for safeguarding private information. The adaptive algorithms adjust the resolution of location information spatial or temporal dimensions to meet specified anonymity constraints based on the entities who using location services within a given area.

[9] The growth of the Internet has significantly reduced the cost of obtaining and sharing information about individual raise many concern about user privacy. Spatial queries pose an additional threat to privacy because the location of a query may sufficient to reveal sensitive information. K nearest neighbor (kNN) queries and define the notion of strong location privacy, which a query indistinguishable from any location in the data space. Hence, truly private services necessitate location privacy. The LBS should be oblivious of the query location.

[10] Geosocial networks provide a context-aware service that helps to associate location with users and content. The proliferation of Geosocial networks indicates that they're rapidly attracting users. Geosocial networks currently offer different types of services, photo sharing, and friend tracking. However, this ability to reveal users locations causes new privacy threats, which turn call for new privacy protection methods. The authors study four privacy aspects to social networks location, absence, colocation and identity privacy and describe possible means of protecting privacy in circumstances. In today's world, Smartphone applications become popular among the users enhancing computing platform.

III. PROPOSED METHOD

In the proposed system the users chat conversation can be stored in server and users location stored in server. They can be encrypted to store in proxy server. An unauthorized users cannot access the authorized user information and location. It can be accessed by authorized users by providing secret key.

Then the authorized user access the specified user information and location.

A. System Architecture:

The architecture for the proposed method is explained in the Fig 1.

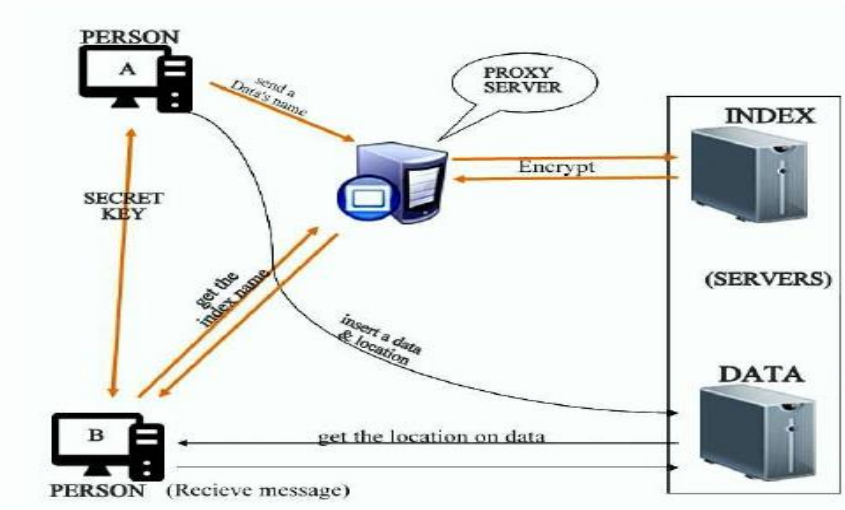

Fig. 2. Architecture diagram for the proposed system

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (159-166), Month: January-April 2016, Available at: www.noveltyjournals.com

In this architecture, fig 2 shows users are interested in querying public these objects are maintained by database on the server. Instead of providing exact location, the client submits a randomly generated cloak region data to the server. The server returns the set of points that are potentially a nearest person of some point in data. Finally, the user uses the exact location to find out its nearest person. The server only knows the region in which the user is located, but not knows the user exact location. A circle is used to represent an exact region. We adopt a simple yet model privacy measure. We can exact the send the location and also data.

The more uncertain is the user location should be shared. It is obviously that the encrypt is maximized when the probability of the client being at any location. Several techniques recently have been proposed for shares user locations with different privacy methods. All techniques perform location sharing in an isolated manner for each submitted query. They did not take into consideration the locality of user movement and hence, are vulnerable to trace your location analysis. The server can link the query trace and mobility pattern to shares the user location. For example, knowing the users maximum send the data, the server that share the friend location from the last region Data based on the location based social application.

B. Implementation:

The three techniques used in the project are location privacy technique, dummy based technique, transformation based technique and algorithm is to be used that is RSA algorithm.

Algorithm and techniques:

RSA is one of the Public-Key Cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring product of two large prime numbers, the factoring problem. RSA is made of the initial letters of the names of Ron Rivest, Adi Shamir, and Leonard Adleman.

Step 1: Choose two prime numbers and find the product

*prime1*prime2=ProductOfPrime1Prime2*

Step 2: Find the Totient of ProductOfPrime1Prime2

Totient= (Prime1-1)(Prime2-1)*

Step 3: Get list of possible integers that result in 1mod Totient

*(Totient*Any Integer)+1=1 mod Totient*

Step 4: Choose 1 mod Totient value exactly two prime factors: Encrypt Prime and Decrypt Prime.

Step 5: Encrypt

CipherText = PlainTextEncryptPrime mod Productofprime1prime2.

Step 6: Decrypt

PlainText = CipherTextDecryptPrime mod

Productofprime1prime2.

Location privacy technique:

Location privacy techniques that works in traditional client server architectures without any trusted components other than client's mobile device, such techniques have important advantage. First, they do not rely on any trusted third party components so they are relatively easy to implement. Second, they have potential for wide application the client server architecture remains dominant the web service. Third, their effectiveness is independent of the distribution of other users, unlike the k-anonymity approach.

Dummy based techniques:

Dummy based techniques hide the user's true location among fake locations, called dummies. In progressive retrieval, candidate results are retrieved iterative from the server, without disclosing the exact user location.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (159-166), Month: January-April 2016, Available at: www.noveltyjournals.com

Transformation based techniques:

Transformation based techniques employ cryptographic transformations so that the service provider is unable to decipher the exact user location. End by pointing out promising directions and open problems.

IV. ANALYSIS AND RESULTS

The result produced here is the output hide the user location from unauthorized user using the location privacy techniques and provide secret key by using RSA algorithm. The sample output of the location privacy in geospatial application obtained at the end of this experiment is also shown in this paper.

Fig. 3 Home page

Fig.3 shows that the home page for the enhancing location privacy policies for geospatial applications

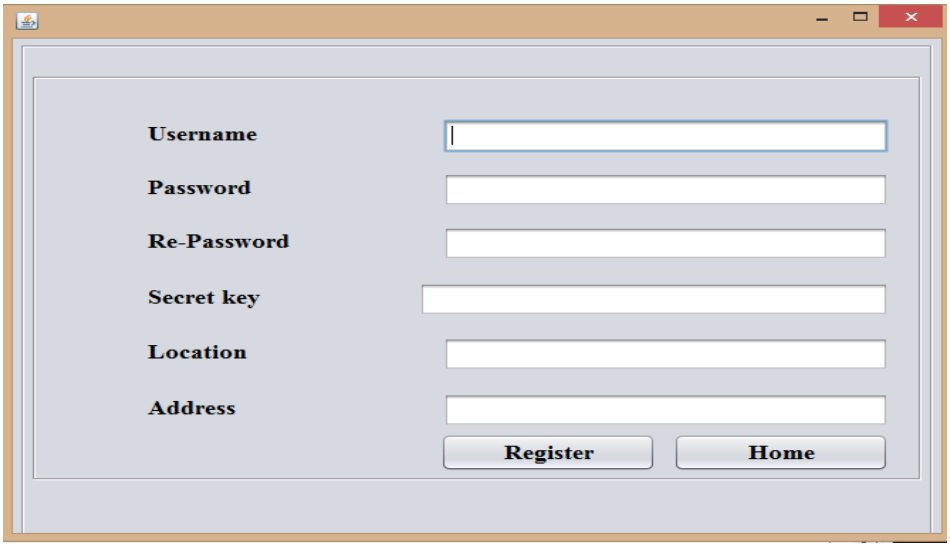

Fig. 4 Login page

Fig. 4 shows that the page allows the authorized users to login by giving user name, password otherwise go to home page.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (159-166), Month: January-April 2016, Available at: www.noveltyjournals.com

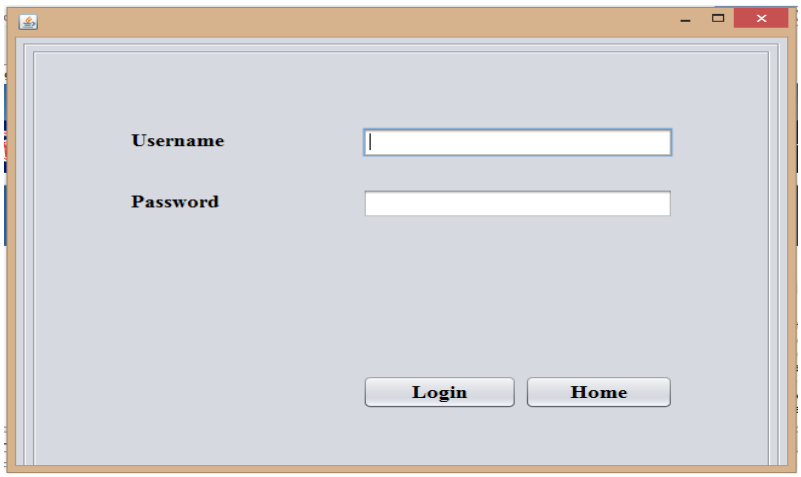

Fig. 5 User registration

Fig.5 shows that how the users to register by giving the following fields such as username, password, secret key, location, address.

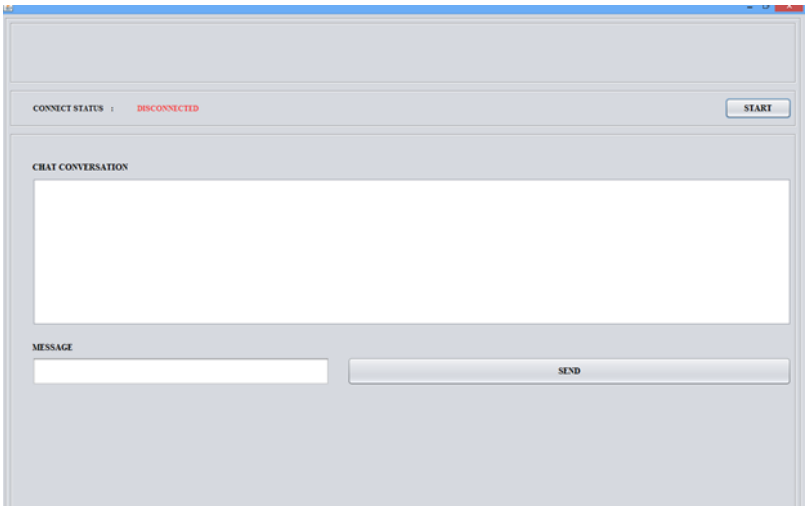

Fig. 6 Client page

Fig. 6 shows that the page client send message to server, shows that chat conversation and connect status with ip address.

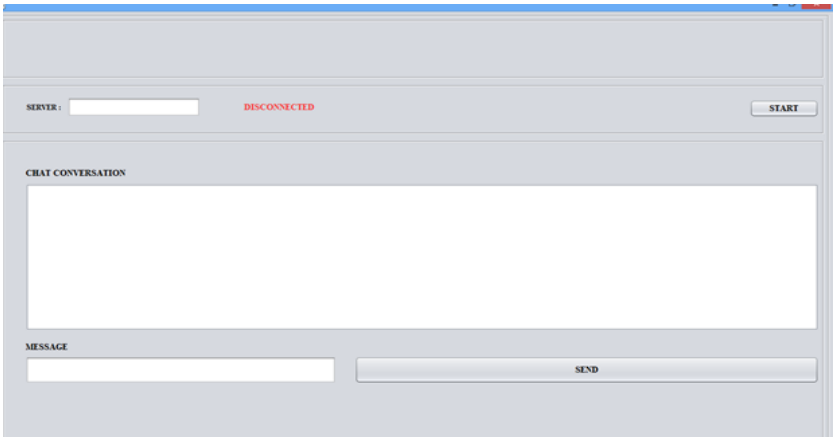

Fig. 7 Server page

Fig.7 shows that the page server send message to client and shows that chat conversation.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (159-166), Month: January-April 2016, Available at: www.noveltyjournals.com

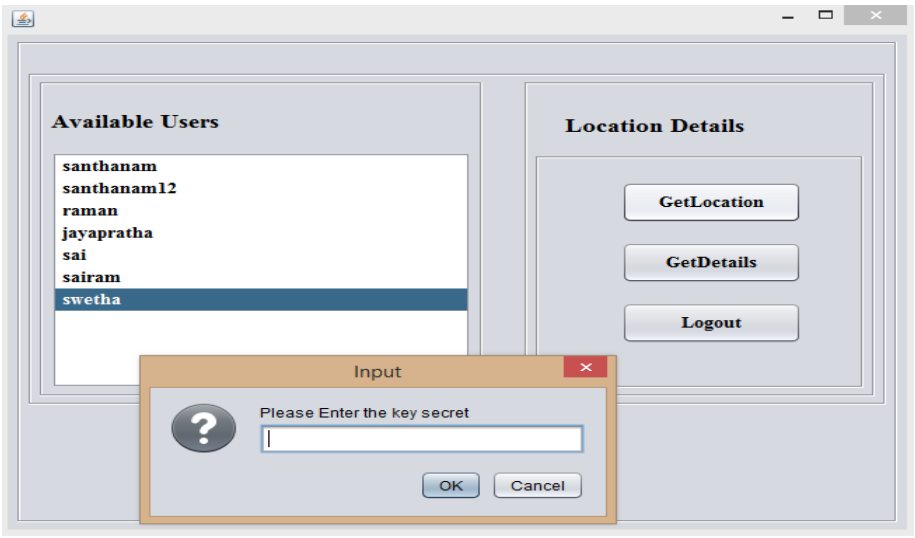

Fig. 8 Users list

Fig.8 shows that the available users list and get the location details by entering secret key.

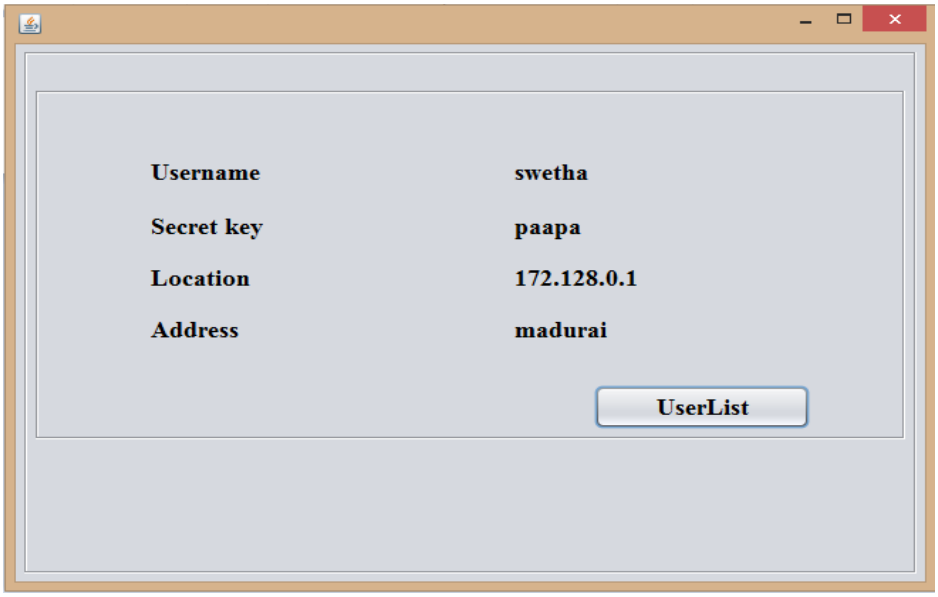

Fig. 9 Details of User

Fig. 9 is the sample output which would be obtained at the last of the project. The user details can be displayed to authorized users.

V. CONCLUSION

The proposed method designed to providing the security, privacy and increasing the performance of the location based social network system. The users efficiently transform all their locations shared with the server and encrypt all location data stored on the server using inexpensive Secret keys. Only friends with the right keys can query and decrypt a user data. To achieve both privacy and efficiency in this process, and analyze their privacy policies.

Secure by a data sharing and its confidentiality & database store in cloud is to. After share data on cloud secured all the records about user who have used the data as a future work. Also bundling of the data with its information and can easily accessing that data or sharing location by getting that secret key & through that we can secure our location is the process of the system.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (159-166), Month: January-April 2016, Available at: www.noveltyjournals.com

REFERENCES

[1] Krishna P.N Puttaswamy, Shiyuvan wang, Troy Steinbauer,, Divyakant Agrawal, and Ben Y.Zhao, "Preserving Location Privacy in Geosocial Applications," IEEE transactions on mobile computing, vol.13, no.1, pp.159-173, 2014.

[2] B.Schilit, J.Hong, and M.Grutester, "Wireless Location Privacy Protection," computer, vol.36, no.12, pp.135-137, 2003.

[3] B.Hoh, M.Gruteser, H.xiong, and A.Alrabady, "Enhancing Security and Privacy in Traffic-Monitoring Systems," IEEE pervasive computing magazine, vol.5, no.4, pp.38-46, Oct 2006.

[4] C.Y.Chow and M.F.Mokbel, "Enabling private continuous queries for revealed user locations," proc.10th int'1 conf.advances spatial temporal databases, pp.258-275, 2007.

[5] P.Chinna Masumanna, G.Vijay Subramanyam, B.Sharath Kumar Reddy, and I.S.Raghuram, " A Locx Unique Approach for Location based Social Applications," international journal of computer engineering in research trends,vol.1, pp.188-194, oct 2014.

[6] R.Cheng, Y.Zhang, E.Bertino, and S.Prabhakar, "Preserving User Location Privacy in me data management infrastructures," in proc.of the 6th workshop on privacy enhancing technologies, pp.393-412, 2006.

[7] M.Gruteser and D.Grunwald, "Anonymous usage of location based services through spatial and temporal cloaking," in proc.of mobisys'03, pp.31-42, 2003.

[8] P.Kalnis, G.Ghinita, K.Mouratidis, and D.Papadias, "Preventing Location based Identity Inference in Anonymous Spatial Queries," IEEE transactions on knowledge data engineering, vol.19, no.12, pp.1719-1733, Dec 2007.

[9] S.Papadopoulous, S.Bakiras and D.Papadias, "Nearest Neighbour Search with Strong Location Privacy," proc VLDB Endowment, vol.3, no.1/2, pp.619-629, 2010.

[10] Prudhvi V, Mahendra Reddy Y, "Safe Guarding spot privacy with geosocial applications," international journal of computer science and mobile computing, vol.4, pp.188-200, 2015.

[11] L. Huang, H.Yamano, K.Matsura, and K.Sezaki, "Silent Cascade: Enhancing location privacy without communication qos degradation," in proc.SPC'06, pp.165-180, 2006.