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

Mobile Privacy Preserving for Location Based Services in Wireless Network

Haritha .P
M.Tech Student ,
Department of CSE
Talla Padmavathi College of Engineering
Somidi, Tekulagudam Road, Kazipet, Warangal.

S. Rajesh
Assistant Professor
Department of CSE
Talla Padmavathi College of Engineering
Somidi, Tekulagudam Road, Kazipet, Warangal.

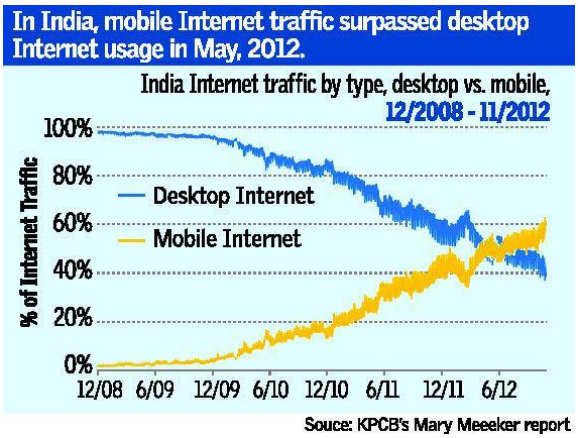
Abstract: ***Wireless enabled devices are having increasing presence in our day to day life. Wireless Enabled is a system normally on laptops which allows you to access the Internet via an existing Internet connection. For example; If you buy a laptop which is wireless enabled, and you wish to get on to the Internet then you can do if you have a wireless router. Now days PDAs, Smart Phones, Tablets and wearable gadgets are wireless enabled. This mobility has paved way to different location based services. Location-based services (LBS) are a general class of computer program-level services that use location data to control features. As such LBS is an information service and has a number of uses in social networking today as an entertainment service, which is accessible with mobile devices through the mobile network and which uses information on the geographical position of the mobile device. This has become more and more important with the expansion of the smartphone and tablet markets as well. Privacy is a major concern in such location based services. The rationale behind this work paper is to investigate the threats to privacy that come up while users not have a good judgment of privacy consciousness and apprehension when using location based services. In this paper we study and implement location based services to mobile users while protecting the privacy without using a third party trusted server.***

Keywords: ***Privacy Protection, Location-Based Services, Security, Mobile users, Wireless Networks***

Introduction:

A Smartphone is a mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded apps. Aided by affordability of cheap Smartphones and availability of 3G and 4G networks the number of Smartphone users is supposed to reach around 1.75 billion users. Although the growth rate of mobile phone users has reached a threshold in developing countries, the burgeoning increase of users in Asia Pacific, Middle East & Africa is supposed to drive the number of mobile phone users to 4.5 billion users.

In 2012 around 1.58 billion users used their mobile phones for internet, which is around 67% of internet users. The number of users using mobile phones for internet grew by 21% to 1.91 billion users, which is around 74% of internet users. This number is further expected to increase by 17% in 2014 to 2.23 billion users, which is around 79% of total internet users. India is ranked fifth in number of smartphone users and has shown one of the highest year-on-year growth rates (in smartphones). It, however, ranks second in the addition of new users to the Internet over the last five years.



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

With the tremendous growth of users in Wireless Technologies (WT), network size also increased. Providing security and privacy to these WT in network is most important factor. The most wireless technology here used is Mobile Technology (MT). Mobile technology is one of the progress factors on behalf of the people. People frequently require anonymity when they roam among the visited networks for their data. While roaming, preventing the resources from anonymous in network is a great issue and also identifying the anonymous in network after their attack requires more communication and computational cost, in recent computational capacity is limited under mobile terminology. To ensure connectivity for users roaming from one network to another, possibly provide roaming services in a secure and private manner.

Roaming service has to allow the MT users to use the WT services even when they take moves from one network to another i.e. home to foreign network. MT users may roam in different networks. Roaming service involves home server, foreign server and the MT user. MT users, who travel across different networks and access the home and foreign servers when their moves. For a harmless roaming service foreign server has to authenticate the user from the home server without knowing the data of the user. Foreign server just authenticate by only using the identity. Roaming services should be secure in location privacy, protect user data and provide strong user anonymity. This survey deals with the security and privacy of roaming networks.

Location Based Services:

LBS include services to identify a location of a person or object, such as discovering the nearest banking cash machine (a.k.a. ATM) or the whereabouts of a friend or employee. LBS include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. They include personalized weather services and even location-based games. They are an example of telecommunication convergence.

Today the question about LBS (Location Based Services) is not, "what they are inside of," but rather, "what they are not an active part of," and the answer is, "very little". They are a part of virtually all control and policy systems which work in computers today. They have evolved from simple synchronization based service models to authenticated and complex tools for implementing virtually any location based service model or facility.

LBS is the ability to open and close specific data objects based on the use of location and/or time as (controls and triggers) or as part of complex cryptographic key or hashing systems and the data they provide access to. Location based services today are a part of everything from control systems to smart weapons. They are actively used trillions of times a day and may be one of the most heavily used application-layer decision framework in computing today.

Some examples of location-based services are:

- Recommending social events in a city
- Requesting the nearest business or service, such as an ATM, restaurant or a retail store
- Turn by turn navigation to any address
- Assistive Healthcare Systems
- Locating people on a map displayed on the mobile phone
- Receiving alerts, such as notification of a sale on gas or warning of a traffic jam
- Location-based mobile advertising
- Asset recovery combined with active RF to find, for example, stolen assets in containers where GPS would not work

Related Work:

Hyo Jin Jo et al, studied the existing three-party roaming protocol mechanisms and analyze the required assistance of the home servers, and also studied the twoparty roaming protocols have weak security , weak anonymity, insecurity in the CK model,

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

backward linkability, and leakage of the session key or inefficient operations. They were the problem in high authentication and revocation costs. Hence in two-party roaming protocols requires the revocation lists to revoke invalid users. A revocation list includes the revocation information associated with each Revoked User (RU). It uses group signature algorithms to authenticate users anonymously. However, these algorithms generally involve a high revocation cost, depending on the number of RU.

Preserving privacy under personal location is one of the greatest issues in wireless network. 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. Many approaches were implemented, which failed to prevent the internal data misuse and privacy preserving policy.

Yan Sun, Thomas F. La Porta and Parviz Kermani proposed a Location-Based Services System (LBSs) for location sharing in social networks. LBS system is used to secure the privacy of the user locations. It secures a user identity and locality within basic mobile communication services. This paper focuses on following aspects: User should be control the access to location information at different levels of granularity and with different levels of user control, user has to define the group of entities that are allowed to access its location information and the main goal of location information is to provide intelligent services to the other users and servers. LBS support location privacy control by the user. It supports user control and scalability. It provides Instant Messaging service for server and clients.

Yan Sun et al approaches is based on offering members of the location information group keys (GKs) that enables them to decrypt the location information. For this GK management this paper proposes a Rebalancing algorithm to maintain rekeying performance with GK management. This article supports the free coupling through a network, thus permit third-party control. This paper provides a protocol like suitable key distribution, Multimedia Internet Keying (MIKEY), and Logical Key Hierarchy (LKH) protocol. These protocols are used to maintain hierarchical location information dissemination for flexible location privacy control for effective message delivery and group management complexity. Hence it does not support the multicast communication. And they were computational cost is also high. They were user anonymity problem from this approach.

Monitoring personal location under untrusted server may cause the privacy problem for the user in wireless sensor network. For this issue Chi-Yin Chow, Mohamed F. Mokbel, and Tian propose a preservingprivacy location monitoring system to provide better security to the user. Chi-Yin Chow et al propose a two innetwork algorithm, which are resource and quality-aware algorithms used to protect the location information of the user [4]. Both these algorithms are well established in kanonymity privacy model to indistinguishable among k person's aggregate locations. Each aggregate location is a cloaked area. This approach provides a high quality for monitoring services for the locations of system user. Hence this approach provides a high quality location monitoring.

The resource-aware algorithm is one which is used to reduce communication and computational cost, while the quality-aware algorithm is used to reduce the size of cloaked areas in order to generate more accurate aggregate locations. Here they use spatial Histogram model to analyze the aggregate locations from sensor node to estimate the monitored objects. Hence this approach reduces the quality of monitoring services; it requires high quality services for larger areas and less privacy protection.

Chunlin Jiang , Weijia Jia and Ke Gu proposed a anonymous authentication protocol based on anonymous proxy signature for wireless communication systems. With the rising number of

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

wireless network with numerous users requires anonymous authentication while roaming among different areas in different networks. Roaming user does not like to identify and tracker their own information to other user, they also want to secure their information while roaming from home network to foreign network.

Chunlin Jiang et al proposed five properties for strong anonymity they were (a) Server Authentication: a user is confident on their identity of the visited server. (b) Subscription Validation: Visited server validates the identity of the home server of the user. (c) Key Establishment: Random session key is established by the user and the visited server which the key is only known to them. In this case, the home server should not acquire the session key. (d) User Anonymity: By this anonymity no one can tell the identity of the user (e) User Untraceability: no one is able to identify any previous protocol runs which have the same user involved including the visited server. So it is hard to tackle these issues because of limited computation and limited storages.

Privacy Issues:

The European Union also provides a legal framework for data protection that may be applied for location-based services, and more particularly several European directives such as: (1) Personal data: Directive 95/46/EC; (2) Personal data in electronic communications: Directive 2002/58/EC; (3) Data Retention: Directive 2006/24/EC. However the applicability of legal provisions to varying forms of LBS and of processing location data is unclear.

One implication of this technology is that data about a subscriber's location and historical movements is owned and controlled by the network operators, including mobile carriers and mobile content providers. Mobile content providers and app developers are a concern. Indeed, a recent MIT study by de Montjoye et al. showed that 4 spatio-temporal points, approximate places and times, are enough to uniquely identify 95% of 1.5M people in a mobility database. The study further shows that these constraints hold even when the resolution of the dataset is low. Therefore, even coarse or blurred datasets provide little anonymity.

Beside the legal framework there exist several technical approaches to protect privacy using privacy-enhancing technologies (PETs). Such PETs range from simplistic on/off switches to sophisticated PETs using anonymization techniques, e.g., related to k-anonymity. Only few LBS offer such PETs, e.g., Google Latitude offered an on/off switch and allows to stick one's position to a free definable location. Additionally, it is an open question how users perceive and trust in different PETs. The only study that addresses user perception of state of the art PETs is. Another set of techniques included in the PETs are the Location obfuscation techniques, which slightly alter the location of the users in order to hide their real location while still being able to represent their position and receive services from their LBS provider.

Privacy protection is especially meaningful and challenging in such an environment. Privacy protection for the roaming user is one of the increasing factors for people that care about their privacy. A roaming user's privacy is like a movement model, extracting information, network usage habit, etc. should be protected from possible enemy intend to break users' privacy. Protecting the privacy of the roaming user in wireless network have to solve the following problems have to protect the user identity, user data, user location information and user likability between the home and foreign server.

a. User Identity

Each user has a unique Identity (ID) for the transferring the information through wireless communication. It is maintained by the ID proxy server. It is an independent service provider this manages the service of the user using separate user ID. Communication device can directly communicate with the proxy server using HTTP protocol. It contains two components i.e. mobile device identification: it helps

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

to check the original user by identifying their name, address, phone no and the home server ID. Then the second component is checking the accessing of the data to that mobile user. So only the users have secure data in wireless communication.

b.Data privacy

Data privacy protections aims privacy of the user data which is collected by a network and queries posted to a network to allot privacy to the user data [10]. Data privacy is under two scenario (i) External adversary and (ii) internal adversary. External adversary: protect the network eavesdrops communication and where in internal adversary protect the access to encryption keys of the two servers (i.e. Home & Foreign server). For data privacy in roaming networks they were used ciphertext anonymity in many research articles. Ciphertext anonymity in one which does not contains identity of both the sender and the receiver information. Here we use Signcryption scheme to provide a better privacy with the ciphertext anonymity property for the user under that two servers (Home & Foreign).

c. Location privacy

Location privacy is especially important in Wireless Network. Location event or the location information is one of the primary concerns from the adversary. Location privacy is under two adversaries: (i) Local adversary and (ii) Global adversary. Local adversary: is able to monitor traffic under limited area of the network at a time. Where as in Global adversary: able to monitor whole network at a time. Accessing Location privacy must be controlled by the user so only they can securely travel in one to another server in network. User must characterize a set of entity to allow access to its location information this provides intelligent services to the attackers.

Existing System:

In Existing System, it was established in a static network with *n* nodes, there has been tremendous interest in the networking research community to understand the fundamental achievable capacity in wireless ad hoc networks. How to improve the network performance, in terms of the capacity and delay, has been a central issue.

Heterogeneous networks with multicast traffic pattern were studied by existing system. Wired base stations are used and their transmission range can cover the whole network. One of the work in existing system studied a dense network with fixed unit area. The helping nodes in their work are wireless, but have higher power and only act as relays instead of sources or destinations. Other Existing works all study static networks.

Disadvantages of Existing System:

- × Limiting factors
- × Low redundancy.

Proposed System:

In Proposed System, assume that at each time slot, bits can be transmitted in a successful transmission. Mobility time scales: Two time scales of mobility are considered in this paper:

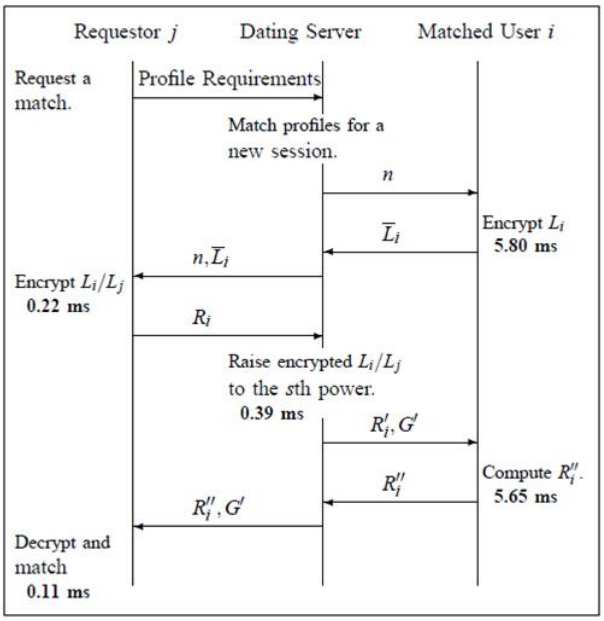
Fast mobility: The mobility of nodes is at the same time scale as the transmission of packets, i.e., in each time-slot, only one transmission is allowed.
Slow mobility: The mobility of nodes is much slower than the transmission of packets, i.e., multiple transmissions may happen within one time-slot.

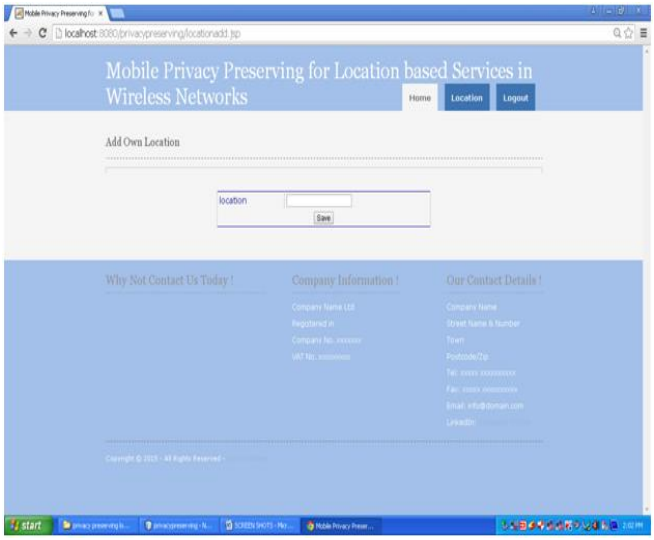
Advantages of Proposed System:

- ✓ The advantage of dimensional mobility lies in the fact that it is simple and easily predictable, thus increasing the inter contact rate.
- ✓ Though nodes are limited to only moving horizontally or vertically, the mobility range on their orbit lines is not restricted.

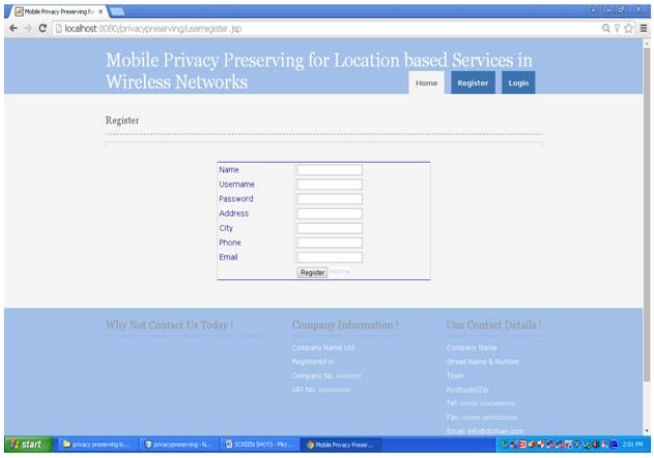
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

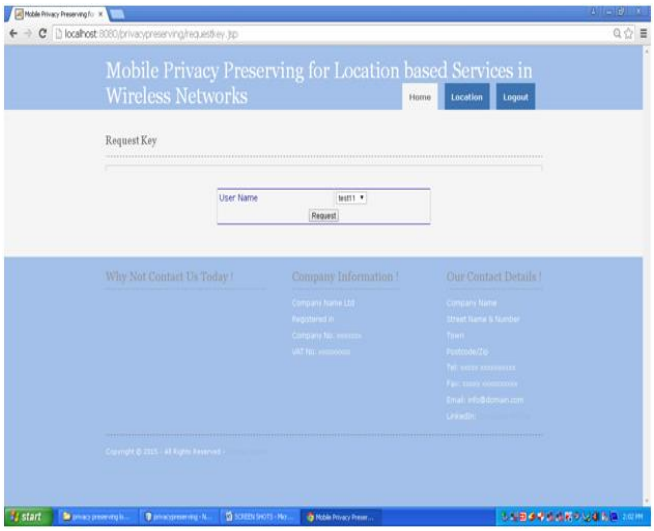
Implementation:

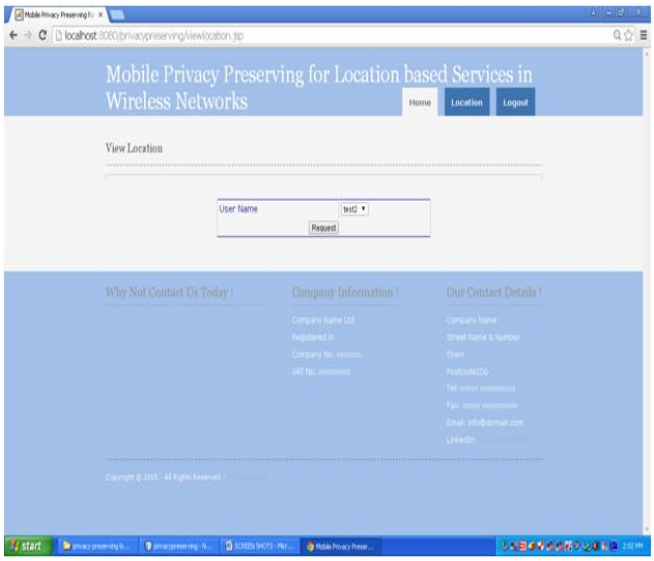




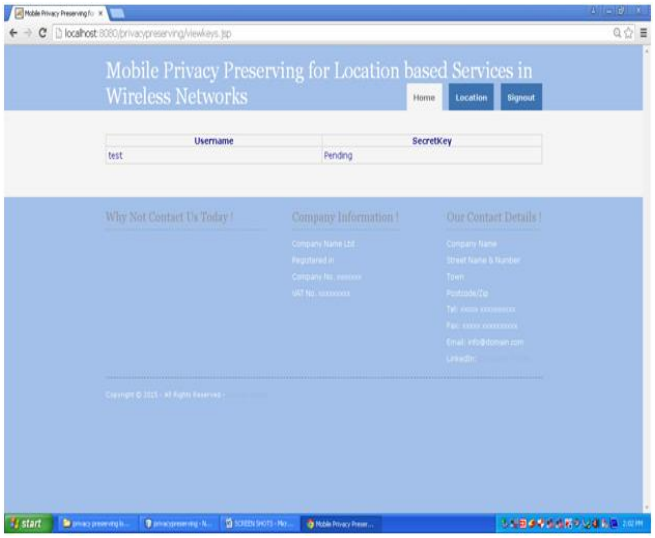
Simulation Screen Shots:

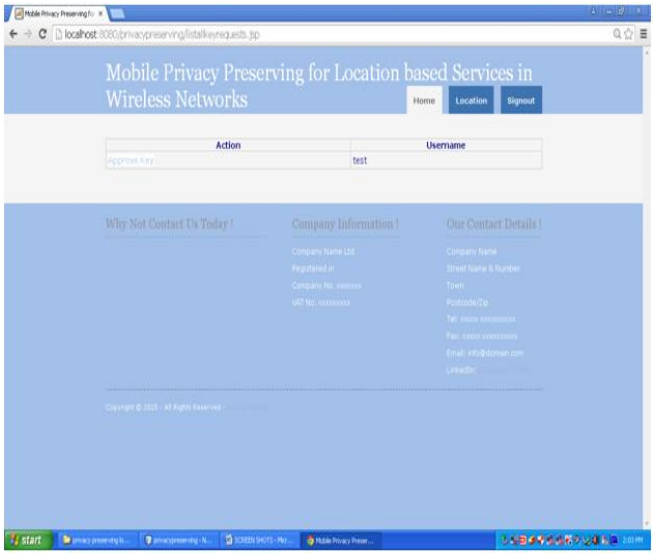


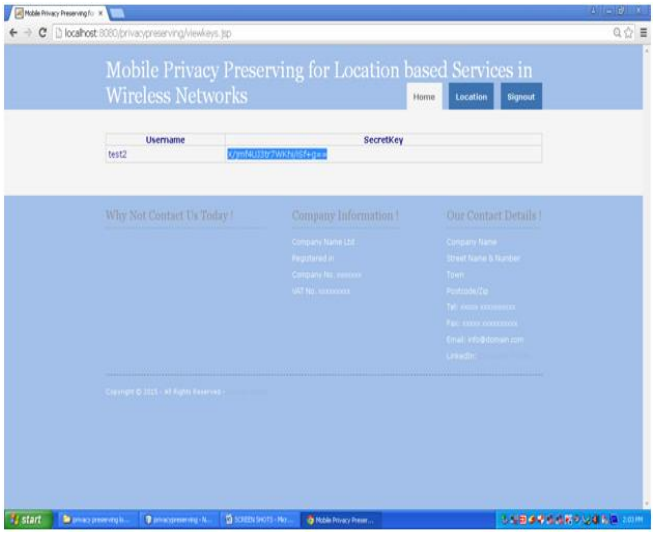




ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal







Conclusion:

Even with many advantages to Location-Based Services, Privacy issues are of a major concern. A weak point of a location based service is the service itself, far before the other components of the localisation and communication that e.g. can be rendered secure by using direct signals instead of radio-based localisation or blind signature. However, a safe location based service implies the use of a trustful server. But still, there are many other undesirable effects to trustful server. In this paper we implemented protocols for the mentioned scenarios, in order to prevent from location information disclosure. We implemented a protocol that enables the user to decide which entity can retrieve the user location and for the secondly we implemented a protocol that accomplishes the desired computations without revealing the users' location. We have tested our system for a number of practical applications and found that the protocols are suitable for personal mobile devices, in order to protect users' privacy.

References:

[1] Sheng Zhong, Li (Erran) Li, Yanbin Grace Liu, Yang Richard Yang, Privacy-Preserving Location-based Services for Mobile Users in Wireless Networks, Yale Computer Science Technical Report YALEU/DCS/TR-1297, 2004

[2] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. IEEE Pervasive Computing, 1:46–55, 2003

[3] Marripally Sathish & P.A Hima Kiran, Preserving Data and Identity Privacy in an Un trusted Cloud Environment Where Membership of the Group Is Changing and Dynamic in Nature, http://www.ijmetmr.com/olapril2015/MarripallySathish-PAHimaKiran-39.pdf , Volume No: 2 (2015), Issue No: 4 (April)

[4] L. Barkuus and A. Dey, "Location-Based Services for Mobile Telephony: A Study of Users' Privacy Concerns," 9th IFIP TC13 International Conference on Human-Computer Interaction, 9 July 2003, pp. 1-5.

[5] D. Ashbrook and T. Starner, "Using GPS to Learn Significant Locations and Predict Movement across Multiple Users," Personal and Ubiquitous Computing, Vol. 7, No. 5, 2003, pp. 275-286. doi:10. 1007/s00779-003-0240-0

[6] S. Dhar and U. Varshney, "Challenges and Business Models for Mobile Location-Based Services and Advertising," Communications of the ACM, Vol. 54, No. 5, 2011, pp. 121-128

[7] M. Abo-Zahhad, S. M. Ahmed and M. Mourad, "Future Location Prediction of Mobile Subscriber over Mobile Network Using Intra Cell Movement Pattern Algorithm," International Conference on Communications, Signal Processing, and Their Applications, Sharjah, December 14 2012, pp. 1-6.

[8] H. Federrath, A. Jerichow, and A. Pfitzmann. MIXes in mobile communication systems: Location management with privacy. In Information Hiding, pages 121–135, 1996.

[9] Marco Gruteser and Dirk Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In Proceedings of The First International Conference on Mobile Systems, Applications, and Services (MobiSys), June 2003.

[10] Q. He, D. Wu, and P. Khosla. Quest for personal control over mobile location privacy. IEEE Communications Magazine, 42(5):130–136, May 2004.