**PROTECTION OF PRIVACY FOR LOCATION IN GEO-SOCIAL THE USES.**

*1Madhamshetty Sravani, 2Kavati Manasa, 3Dameruppula Supraja, 4Vengala Ganesh, 5Mr.J.Raju*

*1,2,3,4Bachelor Degree,Cse,**Jayamukhi Institute Of Technological Sciences,Narsampet, Warangal*

*5Mr.J.Raju, Assistant Professor, Cse,**Jayamukhi Institute Of Technological Sciences,Narsampet, Warangal*

**ABSTRACT:**

Millions of individuals connect with their environment through their friends and suggestions using geo-social programmes like FourSquare. However, without sufficient privacy protection, these technologies are readily abused, for instance to follow users or pick them out for house invasion. In this study, we provide LocX, a unique substitute that dramatically enhances location privacy without introducing ambiguity into query results or depending on shaky server security assumptions. Our primary finding is that all location information communicated with the server should be transformed using safe, user-specific, distance-preserving coordinates. Friends of a user provide their insider information so that others might undergo the same metamorphosis. While our privacy procedures ensure that servers cannot view or deduce the real location data from the modified data or from the data access, this enables all location requests to be accurately evaluated by the server. We demonstrate that LocX offers privacy even in the face of a potent adversary scenario, and we demonstrate via prototype measurements that it does so with very low performance overhead, making it appropriate for modern mobile devices.

**INTRODUCTION:**

Smartphone programmes from Apple iTunes and Android are fast taking over as the user's primary computer device, with billions of installs and yearly revenue.

applications. New geo-social applications are taking full advantage of GPS location-based services in these markets to offer a "social" interface to the real world. Popular social apps include collaborative network services and games [4], [5], social rendezvous [1], local friend referrals for eating and shopping [2], and [3].

The fast growth of mobile social networks like FourSquare (3 million new members in a year) and SCVNGR [6] suggests that in the future, social suggestions will be our main source of local knowledge.

Unfortunately, this new functionality comes with significantly increased risks to personal privacy. Geo-social applications operate on fine-grain, time-stamped location information. For current services with minimal privacy mechanisms, this data can be used to infer a user’s detailed activities, or to track and predict the user’s daily movements. In fact, there are numerous real world examples where the unauthorized use of location information has been misused for economic gain [7], physical stalking [8], and to gather legal evidence [9]. Even more disturbing, it seems that less than a week after Facebook turned on their popular “Places” feature for tracking users’ locations, such location data was already used by thieves to plan home invasions [10]. . Clearly, the mobile social networks of the future need more robust privacy features than the opento-all rules present today.

In order to increase user privacy in geo-social systems, current technologies have mainly relied on three different strategies: (a) integrating uncertainty or error into location data [11], [12], [13], (b) depending on knew servers or intermediaries to apply the anonymization to user identities and personal data [14], [12], [15], and (c) relying on heavy-weight cryptographic or private information retrieval (PIR) techniques [16], [17], [18], [19].

However, none of them have achieved traction on today's app platforms.

Techniques based on the first approach fail due to the fact that they involve both users and application providers to incorporate uncertainty into their data, lowering the quality of application results delivered to the user. There is a basic tradeoff in this method between the amount of mistake brought into the time or location domain and the level of privacy offered to the user. Users detest losing accuracy in results, and application providers have a strong motivation for concealing user data from themselves, limiting their potential to monetize this information. The second method depends on the system's trusted proxies or servers to safeguard user privacy. This is a dangerous premise to make since malevolent administrators, as well as software defects and setup mistakes on trustworthy servers, might reveal sensitive information. Finally, it is prohibitively costly to implement heavy-weight cryptographic techniques on mobile devices [20], [21], or even on the servers for resolving queries like nearest-neighbor and range searches.

Therefore, the problem is to create procedures that effectively safeguard user privacy without compromising the system's correctness or making unfounded claims about the security or reliability of the application servers.

location data from a user's social network to worldwide exposure. We distinguish between nearest-neighbor (kNN) and point queries as the two primary types of queries required to enable the functionality of these geo-social apps. While kNN queries look for the k closest data within a given location coordinate's (or up to a defined radius) area, point queries look for location data at a specific point. Our objective is to provide both query types with effective support that is appropriate for modern mobile devices.

In this research, we propose LocX (short for location to index mapping), a unique method for achieving user privacy while preserving complete accuracy in location-based social apps (hereafter referred to as LBSAs), to overcome this difficulty.

Our discovery is that numerous apps only need to handle distance-based inquiries between friends who are interested in each other's locations and data, rather than between random pairs of users. As a result, we may divide location data according to the social groupings of users and subsequently alter the position coordinates before storing them on unreliable servers.

A user can turn her query onto the virtual location system that her peers use by knowing its conversion keys. Our coordinate transformations maintain distance measurements, enabling an application server to execute point and nearest-neighbor searches on changed data with accuracy. The transformation is safe, nevertheless, because it makes it difficult to link altered values to actual places without a secret that only those in the social group know. Finally, transformations are effective because they put less strain on the LBSAs.Because of this, LocX-based apps are portable and ideal for use with modern mobile devices.

**RELATED WORK:**

**Prior work on privacy in general location-based services:**

. In general, there are three sorts of location privacy approaches for LBSs that do not specifically target social applications. The first is spatial and temporal cloaking [11], [12], [13], [22], [15], in which a server receives a rough position and time rather than the exact values. The idea behind this is to promote privacy by preventing exact location tracking of the users or hiding the user among k other users (a concept known as k-anonymity [12], [13], [22]). precision, promptness, and most crucially, user privacy are still at risk due to a number of straightforward assaults on these methods [23], [24], [25], and [26]. Other methods of achieving cloaking, in which device IDs are regularly altered and data is not transferred for extended durations at regular intervals, include pseudonyms and quiet times [27], [14]. However, this substantially impairs functionality and alienates people. These methods differ significantly from ours in that they rely on trusted servers or intermediates and provide approximate real-world location information to the servers in plain-text.

On the plus side, although LocX primarily focuses on the newly developing geo-social applications, these methodologies are more broad and may thus be used to numerous location-based services.

The second class is location change, which protects user privacy by using altered location coordinates. Finding all of the actual neighbours with accuracy is one of the most subtle problems with this method of processing nearest-neighbor requests.

Unfortunately, blind assessment employing Hilbert contours [21] can only identify approximate neighbours.

Strong location privacy is provided by the third type of work, which uses Private Information Retrieval (PIR) [16]. It is currently unknown if this strategy can be used in actual LBSs because, even utilising specialised hardware to boost its performance [17], it still performs much worse than all the other ways.

Prior research on geo-social services privacy Some recent suggestions use pricey cryptographic approaches, such secure two side computation, to ensure proven location privacy for specific geo-social service types, including buddy tracking services to determine whether a friend is close. LocX, on the other hand, exclusively employs low-cost symmetric encryption and pseudorandom number generators. The project that comes the closest to LocX is Longitude [32], [33], which likewise changes coordinates to keep them from being revealed to the servers.

On the other hand, Longitude allows users to selectively share locations to pals by maintaining the transformational secrets between each pair of friends. . In other words, a person may utilise Longitude to let just a select group of her friends to know where she is. The amount of secrets that users must keep hidden is only one per user in LocX, which features a simplified threat model where all friends have access to a user's information. Location and user unlinkability are still achievable using LocX. In addition, LocX is capable of offering geo-social services that go beyond buddy monitoring like in the aforementioned earlier work, such as location-based social recommendations, reminders, and others.

So why isn't utilising Tor to anonymously transport data to LBSA servers adequate, one would wonder? This strategy appears to offer privacy because the server only sees location information and not the user's identity. Recent studies have found that protecting location privacy does not just depend on users' identities being concealed. Even when Tor is utilised, our privacy and unlinkability criteria might still be broken by an attacker who had access to the location information. For instance, it has been demonstrated that users' residences and workplaces, as well as their identities, may be determined using anonymized GPS data acquired by the servers [23], [24], [25], [26]. LocX protects against such assaults and satisfies all of our criteria.

Systems hosted on unreliable servers. Recent databases have advocated employing heavy-weight homomorphic [35] or asymmetric encryption [36] techniques to conduct database queries on encrypted data that is kept on untrusted servers.

These methods are appropriate for situations involving the outsourcing of geographical data or data mining where the data is static and held by a small group of users. However, they are less appropriate for LBSAs since the data there is dynamic and private and cannot be secured with a single secret key. Persona [37] and Adeana [38] similarly depended on encrypting all data kept on untrusted servers in the context of location and social apps to safeguard user privacy. Adeana focused on privacy in device monitoring systems where there is no user-to-user data exchange, whereas Persona focused on privacy in online social networks. If Persona's techniques were directly applied to LBSAs, all position coordinates would be encrypted, making it impossible for LBSAs to respond to nearest-neighbour requests.

However, attacks employing the previously described anonymized GPS traces can succeed if location is not encrypted, rendering Persona inadequate to guarantee location privacy.

Similar to this, a person can access her own info from Adeana but not that of her friends. Our contributions strengthen these frameworks.

Some of the methods in these articles, such as Persona's strategy for fine-grained grouping of data shared with friends and Adeana’s hardware-assisted approaches for accelerating crypto processing, can benefit LocX as well.

**EXISTING SYSTEM:**

Existing systems have mainly taken three approaches to improving user privacy in geosocial systems:

· Introducing uncertainty or error into location data.

· Relying on trusted servers or intermediaries to apply anonymization to user identities and private data.

· Relying on heavy-weight cryptographic or private information retrieval (PIR) techniques.

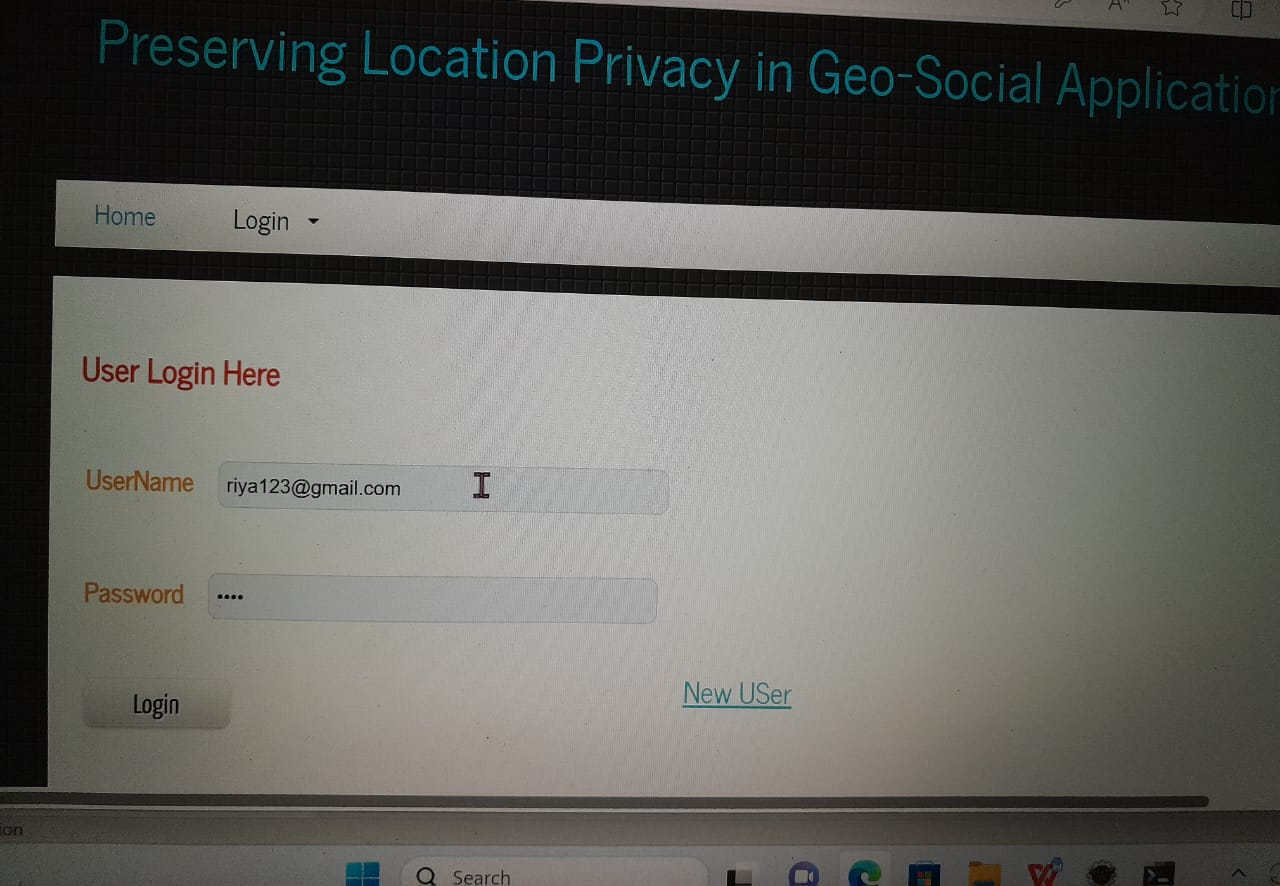
None of them, however, have proven successful on current application platforms. Techniques using the first approach fall short because they require both users and application providers to introduce uncertainty into their data, which degrades the quality of application results returned to the user. In this approach, there is a fundamental tradeoff between the amount of error introduced into the time or location domain, and the amount of privacy granted to the user. Users dislike the loss of accuracy in results, and application providers have a natural disincentive to hide user data from themselves, which reduces their ability to monetize the data. The second approach relies on the trusted proxies or servers in the system to protect user privacy. This is a risky assumption, since private data can be exposed by either software bugs and configuration errors at the trusted servers or by malicious administrators. Finally, relying on heavy-weight cryptographic mechanisms to obtain provable privacy guarantees are too expensive to deploy on mobile devices and even on the servers in answering queries such as nearest neighbour and range queries.

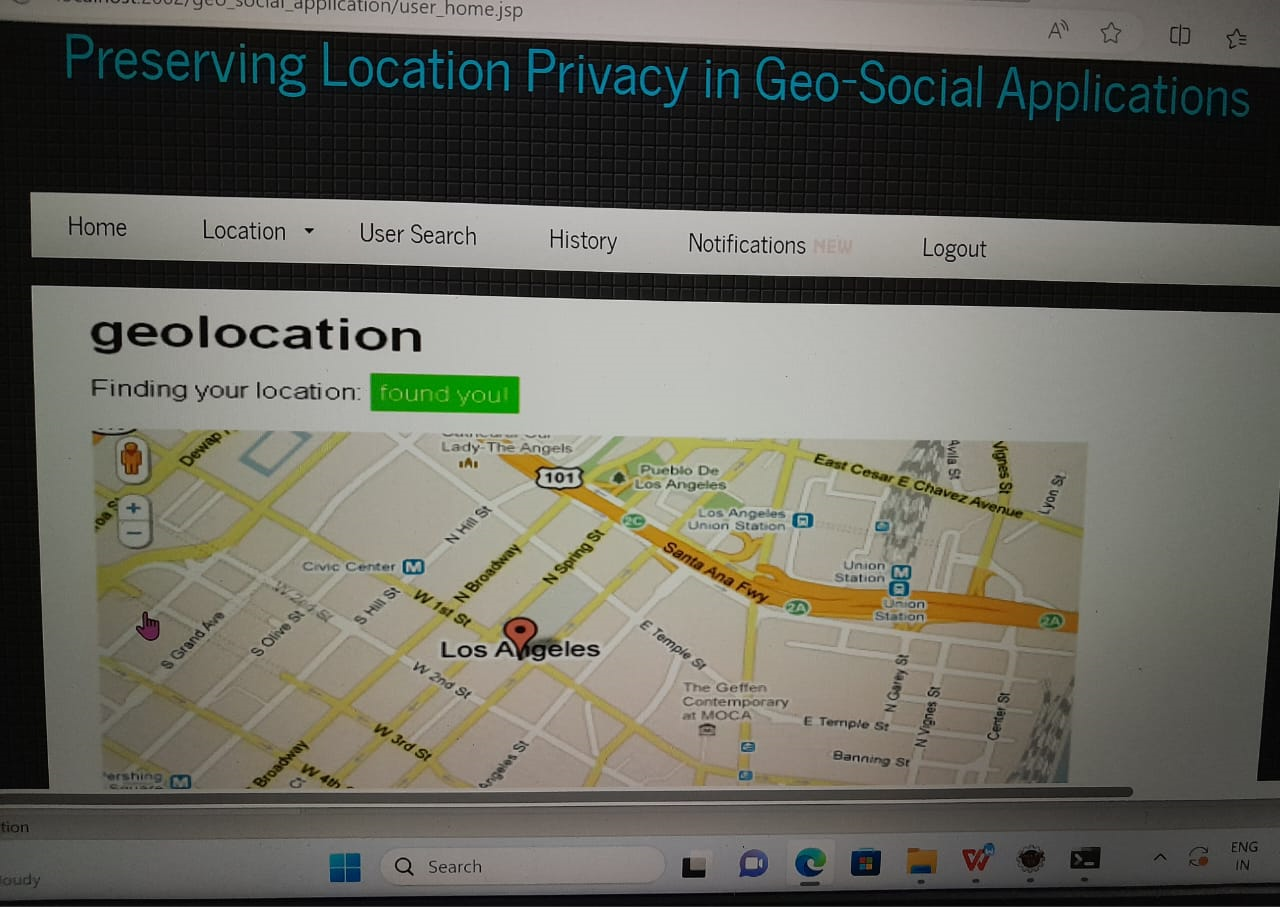
**PROPOSED SYSTEM:**

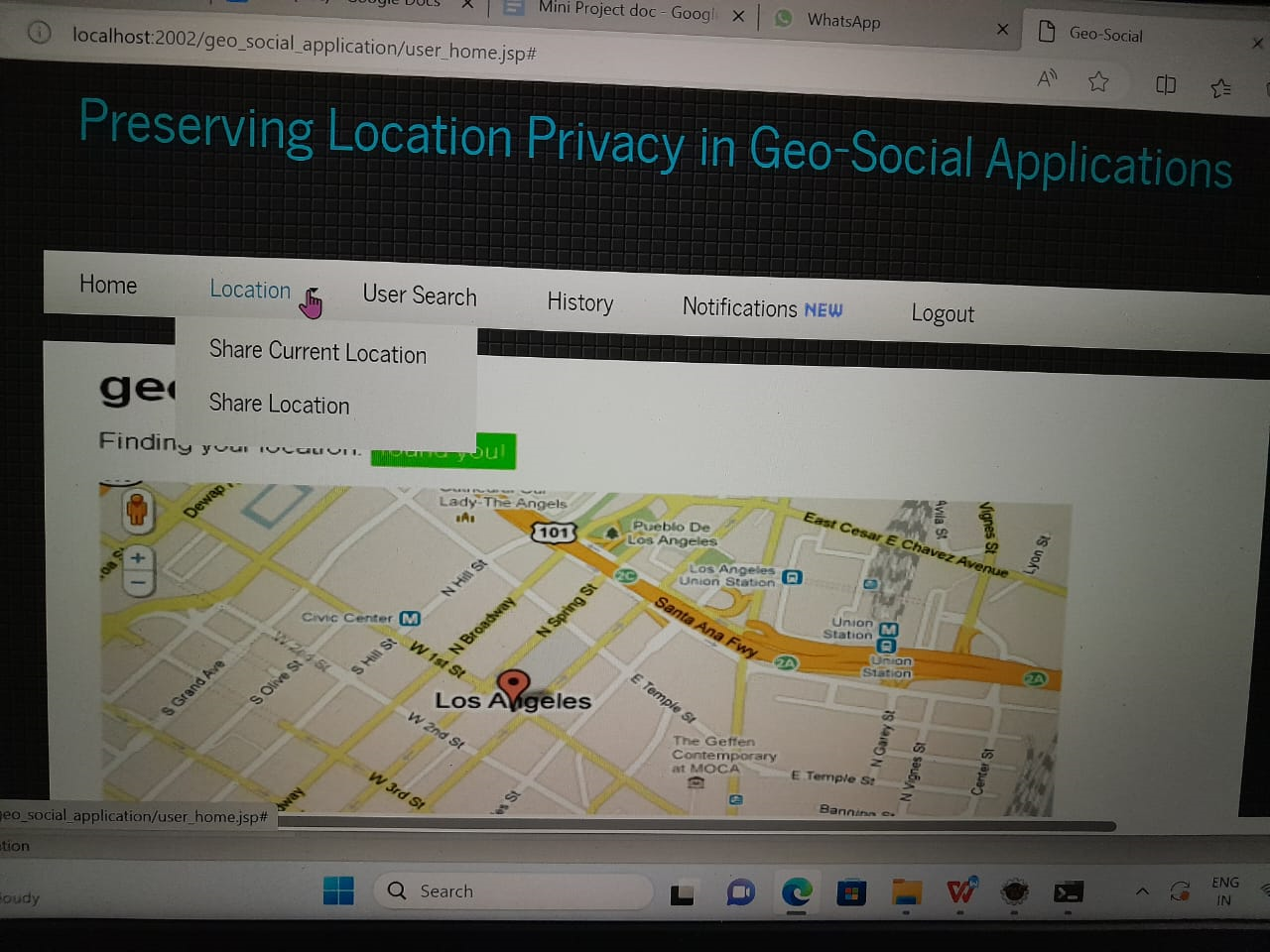
In this paper, we propose LocX (short for location to index mapping), a novel approach to achieving user privacy while maintaining full accuracy in location-based social applications (LBSAs from here on ward). Our insight is that many services do not need to resolve distance-based queries between arbitrary pairs of users, but only between friends interested in each other’s locations and data. Thus, we can partition location data based on users’ social groups, and then perform transformations on the location coordinates before storing them on untrusted servers. A user knows the transformation keys of all her friends, allowing her to transform her query into the virtual coordinate system that her friends use. Our coordinate transformations preserve distance metrics, allowing an application server to perform both point and nearest-neighbor queries correctly on transformed data. However, the transformation is secure, in that transformed values cannot be easily associated with real-world locations without a secret, which is only available to the members of the social group. Finally, transformations are efficient, in that they incur minimal overhead on the LBSAs. This makes the applications built on LocX lightweight and suitable for running on today’s mobile devices.

**RESULT:**









**CONCLUSIONS:**

This article covers LocX, a system for developing location-based social applications (LBSAs) while protecting consumer privacy, including its concept, prototype delivery, and assessment. Without introducing doubt or faults into the system or relying on any reliable servers or parts, LocX protects users' geolocation privacy. By using the social data-sharing functionality of the target applications, LocX employs an innovative strategy to offer location privacy while retaining overall system effectiveness. In LocX, users effectively encrypt all location data saved on the server and convert all of their transmitted locations with the server. A user's data can only be accessed and decrypted by friends who have the correct keys. In this procedure, we propose many strategies and examine their anonymity qualities in order to attain both effectiveness and privacy.

By using the social data-sharing functionality of the target applications, LocX employs an innovative strategy to offer location privacy while retaining overall system effectiveness. In LocX, users effectively encrypt all location data saved on the server and convert all of their transmitted locations with the server. A user's data can only be accessed and decrypted by friends who have the correct keys. In this procedure, we propose many strategies and examine their anonymity qualities in order to attain both effectiveness and privacy.

**REFERENCES:**

[1] M. Motani, V. Srinivasan, and P. S. Nuggehalli, “Peoplenet: engineering a wireless virtual social network,” in Proc. of MobiCom, 2005.

[2] M. Hendrickson, “The state of location-based social networking,” 2008.

[3] P. Mohan, V. N. Padmanabhan, and R. Ramjee, “Nericell: rich monitoring of road and traffic conditions using mobile smartphones,” in Proc. of SenSys, 2008.

[4] G. Ananthanarayanan, V. N. Padmanabhan, L. Ravindranath, and C. A. Thekkath, “Combine: leveraging the power of wireless peers through collaborative downloading,” in Proc. of MobiSys, 2007.

[5] M. Siegler, “Foodspotting is a location-based game that will make your mouth water,” <http://techcrunch.com/2010/03/04/foodspotting/>.

[6] <http://www.scvngr.com>.

[7] B. Schilit, J. Hong, and M. Gruteser, “Wireless location privacy protection,” Computer, vol. 36, no. 12, pp. 135–137, 2003. [8] F. Grace, “Stalker Victims Should Check For GPS,” Feb. 2003, [www.cbsnews.com](http://www.cbsnews.com).

[9] DailyNews, “How cell phone helped cops nail key murder suspect secret ’pings’ that gave bouncer away,” Mar. 2006.

[10] “Police: Thieves robbed homes based on facebook, social media sites,” WMUR News, September 2010, <http://www.wmur.com/r/24943582/detail.html>.

[11] M. Gruteser and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking,” in Proc. of Mobisys, 2003.

[12] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, “The new casper: A privacyaware location-based database server,” in ICDE, 2007.

[13] B. Gedik and L. Liu, “Location privacy in mobile systems: A personalized anonymization model,” in Proc. of ICDCS, 2005.

[14] T. Jiang, H. J. Wang, and Y.-C. Hu, “Preserving location privacy in wireless lans,” in Proc. of MobiSys, 2007.

[15] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing location-based identity inference in anonymous spatial queries,” TKDE, 2007.

[16] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, “Private queries in location based services: anonymizers are not necessary,” in SIGMOD Conference, 2008.

[17] S. Papadopoulos, S. Bakiras, and D. Papadias, “Nearest neighbor search with strong location privacy,” PVLDB, 2010.

[18] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, “Location privacy via private proximity testing,” in Proc. of NDSS, 2011.

[19] G. Zhong, I. Goldberg, and U. Hengartner, “Louis, lester and pierre: Three protocols for location privacy,” in Proc. of PET, 2007.

[20] N. Daswani and D. Boneh, “Experimenting with electronic commerce on the palmpilot,” in Financial Cryptography. Springer, 1999.

[21] A. Khoshgozaran and C. Shahabi, “Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy,” in Proc. of SSTD, 2007.

[22] G. Ghinita, P. Kalnis, and S. Skiadopoulos, “Prive: anonymous locationbased queries in distributed mobile systems,” in Proc. of WWW, 2007.

[23] P. Golle and K. Partridge, “On the anonymity of home/work location pairs,” in Proc. of Pervasive Computing, 2009.

[24] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, “Enhancing security and privacy in traffic-monitoring systems,” in IEEE Pervasive Computing Magazine, 2006.

[25] B. Hoh et al., “Preserving privacy in gps traces via uncertainty-aware path cloaking,” in Proc. of CCS, 2007.

[26] J. Krumm, “Inference attacks on location tracks,” in Proc. of Pervasive Computing, 2007.

[27] A. Beresford and F. Stajano, “Mix zones: User privacy in location-aware services,” in Proc. of Pervasive Computing, 2004.

[28] M. L. Yiu, C. S. Jensen, X. Huang, and H. Lu, “Spacetwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services,” in Proc. of ICDE, 2008.

[29] D. Lin, E. Bertino, R. Cheng, and S. Prabhakar, “Position transformation: a location privacy protection method for moving objects,” in Proc. of Security and Privacy in GIS and LBS, 2008.

[30] C.-Y. Chow and M. F. Mokbel, “Enabling private continuous queries for revealed user locations,” in SSTD, 2007, pp. 258–275.

[31] E. O. Turgay, T. B. Pedersen, Y. Saygin, E. Savas, and A. Levi, “Disclosure risks of distance preserving data transformations,” in Proc. of SSDBM, 2008.

[32] S. Mascetti, C. Bettini, and D. Freni, “Longitude: Centralized privacypreserving computation of users’ proximity,” in Proc. of SDM, 2009.

[33] S. Mascetti, C. Bettini, D. Freni, X. S. Wang, and S. Jajodia, “Privacyaware proximity based services,” in Proc. of MDM, 2009.

[34] R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The secondgeneration onion router,” in USENIX Security Symposi.