

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Preserving User Privacy and Preventing Server Content in Location Based Service

Suhasini S. Mhetre¹, Prof. Phatak Amol A.², Prof. Pottigar Vinayak V.³

Department of Computer Science and Engineering, Sinhgad College of Engineering, Kegaon, Solapur, India

Head of Department, Department of Computer Science and Engineering, Sinhgad College of Engineering, Kegaon,
Solapur, India

Department of Computer Science and Engineering, Sinhgad College of Engineering, Kegaon, Solapur, India

ABSTRACT: In this framework an Location Based Service [LBS] is a data, excitement and utility Service for the most part open by cell phones, for example, cell phones, GPS gadgets, stash PCs, and working through a portable system. LBS can offer many Services to the clients in view of the geological position of their cell phone. The Services gave by LBS are normally in view of a state of intrigue database. By recovering the Points of Interest [POIs] from the database server, the client can find solutions to different Location based questions however while doing this client Location data can be followed by different ways and it can be utilized for Location based showcasing and other defenseless purposes. This work proposes a noteworthy upgrade upon past arrangements by presenting a two phase approach, where the initial step depends on Oblivious Transfer and the second step depends on Private Information Retrieval, to accomplish a safe answer for both sides. The arrangement it present is productive and down to earth in numerous situations. This work executes our answer on a desktop machine and a cell phone to evaluate the Efficiency of our convention. It likewise presents a security display and breaks down the security with regards to our convention. At long last, our proposed framework highlights a security shortcoming of our past work and introduces an answer for conquer it.

KEYWORDS: Location Services, Querying, Point of Interest, Location Server, Privacy Maintenance.

I. INTRODUCTION

Location Based Service is the capacity to open and close character information objects in light of the utilization of Location as well as time as a component of complex issue cryptographic key frameworks and the information they provided get to. Location based administrations today are a segment of everything from control frameworks to brilliant weapons. They are effectively utilized a great many times each day and might be a standout amongst the most intensely utilized application layer choice structure in today. LBS can delicate numerous administrations to the clients in light of the geological position of their client Location gadget.

LBS are commonly relies on upon a state of intrigue database. In current years there has been a sensational development in the quantity of cell phones questioning Location servers for data about purpose of interests. Different testing issues to the substantial sending of such application security confirmation are a noteworthy issue. For example, clients may feel hesitant to unveil their Locations to the LBS since it might be feasible for an Location server to realize who is making a specific inquiry by connecting these Locations with a private telephone directory database, since clients are probably going to perform many questions from home.

LBS need to guarantee that LS [Location Server] information is not gotten to by any unapproved client. Amid the procedure of transmission the clients ought not be permitted to find any data for which they have not paid. It is in this manner essential that arrangements be concocted that address the protection of the clients issuing inquiries additionally keep clients from getting to substance to which they don't have approval.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Location based administrations might be utilized in various applications, prescribing get-togethers in a city, asking for the closest business or administration, for example, an ATM, eatery or a retail location, turn-by-swing route to any address, assistive medicinal services frameworks, finding individuals on a guide showed on the cell phone, accepting alarms, for example, notice of a deal on gas or cautioning of a car influx, Location based versatile promoting and so forth.

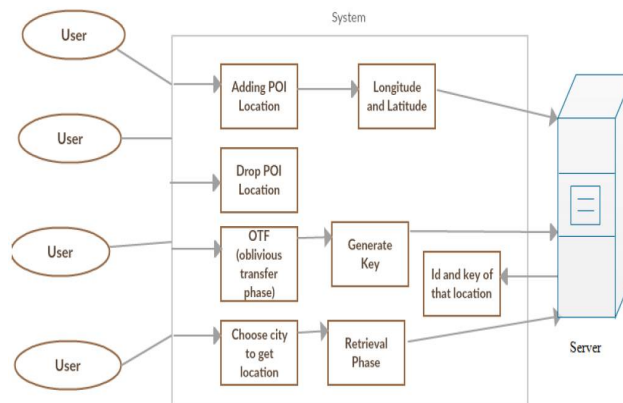


Fig.1. System Design

The system architecture consists of three parts. 1) An external LBS server 2) deployed proxies 3) Desktop clients. The Location Based Service server is responsible for managing static data objects and answering the queries submitted by the proxies. The LBS server can use any index structure to process spatial queries. The LBS server is consider not providing VRs every of the deployed proxies supervises one service area and provides of window queries for desktop clients in the service area. Base stations proxies and the LBS server are connected by a wired network. A desktop client maintains a cache to store the query results and the corresponding. When a desktop client has a spatial query, the desktop device first examines whether the current location is in the stored result. If so the stored result remains valid and the desktop device directly shows it to the client. The desktop device submits the query which is received and then forwarded by the base station to the proxy.

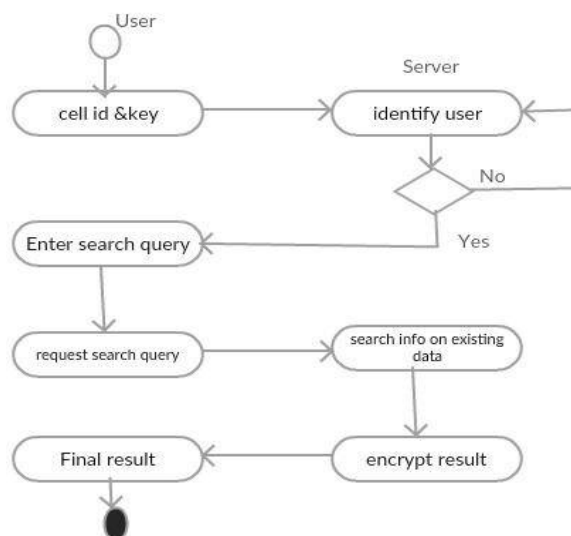


Fig.2. Activity Diagram

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

II. MOTIVATION SUMMARY

Technological promotions in desktop machine computing have spawned an increasing usage of location based services. Such services use the location information of the subscriber to supply better functionalities. But improper usage of location information may compromise the security and privacy of an individual. Privacy protection is a vital research challenge. Although progress has been made in recent years lots of complex problems are still unresolved and many solutions are needed to be put forward.

Today location privacy research has been developing independent privacy protection methods for each of the three kinds of LBSs. 1. Location based services (LBSs) that need true identity (Security policy, Cryptographic Encryption techniques) 2. Location based services that need only pseudonyms (Privacy policy, Pseudonym maintenance protocols, mix-zone based location anonymization) and 3. Location based services that need neither identity nor pseudonyms (Privacy policy, customizable location anonymization).

IV. PROJECT DESCRIPTION

The main objective of this system is to create a content protecting and privacy preserving location based system which provides accurate location based services by preserving user's location information. At the same time this system should protect the server information by applying public key algorithms which will prohibit the anonymous user from accessing the server data.

- (a) Implemented the solution on both a mobile device and desktop machine.
- (b) To provide content protecting location based service.
- (c) Add a formal security model for server data protection.

The major scope of this approach is as follows:

- (i) Implement public key algorithm to provide additional security for data present on server.
- (ii) Develop 2 stage security protocols for privacy preserving.
- (iii) Improve the performance of overall system.

V. LITERATURE SURVEY

Various looks into have been finished on protection safeguarding. However, nobody gave undeniable certainty of client's information and inquiry.

Inferable from expanding requests from versatile clients Location Based Services have gotten a ton of consideration as of late. Cases of inquiries for Location based Services incorporate discover the closest service station from my present Location, discover every one of the silver screens inside 1 km sweep, which transports will go by me in the following 10 minutes? et cetera. While information questions in the initial two illustrations are stationary, those in the last case are portable. We concentrate on inquiries issued by desktop clients on moderately static information objects, since they are the most widely recognized sort of questions in LBSs. The development of portable customers presents numerous new research issues for Location subordinate inquiry handling there are a few specialized issues required with the usage of a LBS, which incorporate finding the position of a versatile client, following and foreseeing developments, preparing inquiries productively, and bouncing Location blunders.

A corresponding system to the blend zone approach depends on k-namelessness. The idea of k-namelessness was presented as a technique for protecting security while discharging delicate records. This is accomplished by speculation and concealment calculations to guarantee that a record couldn't be recognized from $(k - 1)$ different records. The answers for LBS utilize a put stock in anonymiser to give secrecy to the Location information, with the end goal that the Location information of a client can't be recognized from $(k - 1)$ different clients.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

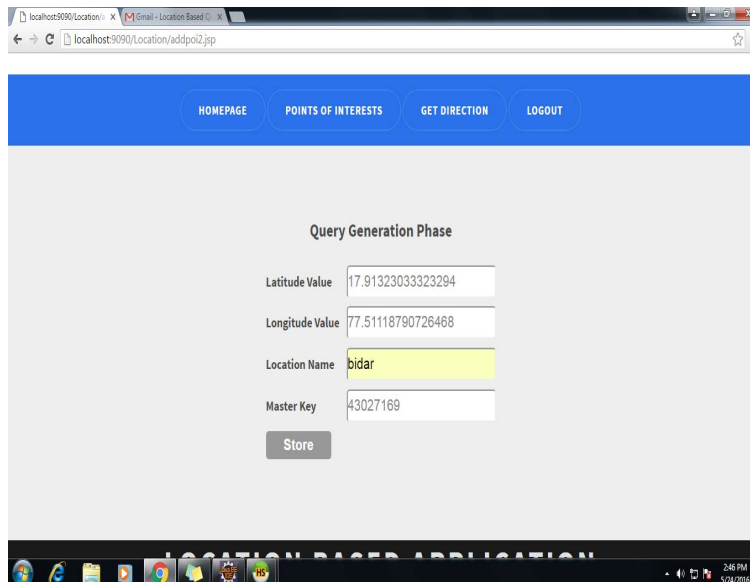
Way disarray was displayed by Hoh and Gruteser. The fundamental thought is to add vulnerability to the Location information of the clients at the focuses the ways of the clients cross, making it difficult to follow clients in view of crude Location information that was k-anonymized.

Consider a registering domain with an expansive number of Location mindful versatile articles. We need to recover the portable protests inside an arrangement of client characterized spatial locales and ceaselessly screen the number of inhabitants in these windows over a day and age. In this paper, we allude to such consistent inquiries as range-observing questions. Effective preparing of range-observing inquiries could empower numerous valuable applications. So also, we might need to track movement condition stick some range and dispatch more police to the locale if the quantity of vehicles inside surpasses a specific edge.

In such applications, it is exceedingly alluring and at some point basic to give precise outcomes and refresh them stick continuous at whatever point portable items enter or leave the locales of intrigue. Not at all like regular range inquiries, is a range-observing question a constant inquiry. It remains dynamic until it is ended expressly by the client. As articles keep on moving, the inquiry comes about change appropriately and requires constant updates. A straightforward system for processing range observing questions is to have each protest report its position as it moves. The server utilizes this data to recognize the influenced inquiries, and updates their outcomes as needs be. This straightforward approach requires exorbitant Location updates, and clearly is not versatile. Every Location refresh comprises of two costs - portable correspondence cost and server handling cost.

VI. EXPERIMENTAL RESULTS

The following figure shows the query generation phase of oblivious transfer algorithm.



The screenshot shows a web browser window with the URL `localhost:9090/Location/addpoi2.jsp`. The page has a blue header with navigation links: `HOME PAGE`, `POINTS OF INTERESTS`, `GET DIRECTION`, and `LOGOUT`. The main content area is titled "Query Generation Phase" and contains a form with the following fields:

Latitude Value	<input type="text" value="17.91323033323294"/>
Longitude Value	<input type="text" value="77.51118790726468"/>
Location Name	<input type="text" value="bidar"/>
Master Key	<input type="text" value="43027169"/>

Below the form is a `Store` button. The browser's taskbar at the bottom shows the system tray with the time `2:46 PM` and date `5/24/2015`.

Fig.4. Query Generation Phase

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

The following figure shows, adding the POI successfully.

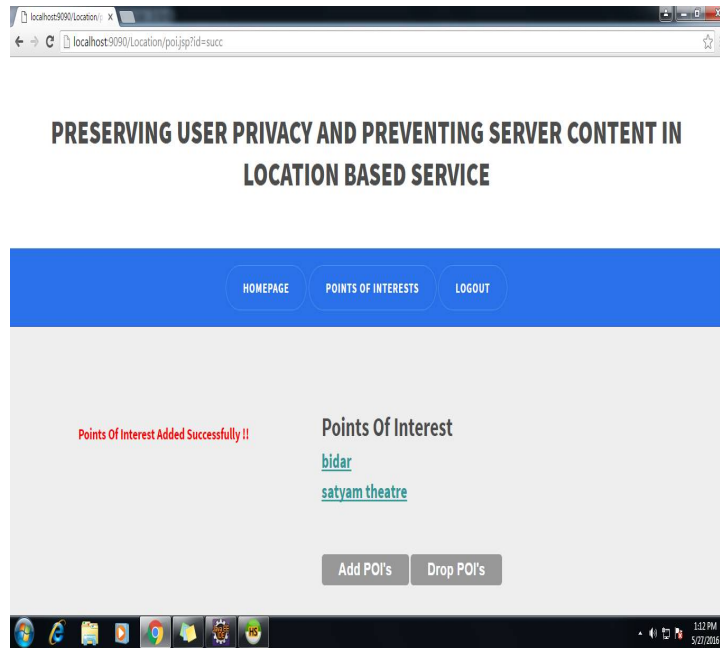


Fig.5. Adding Point Of Interest

The following figure shows, Response generation phase of oblivious transfer algorithm.

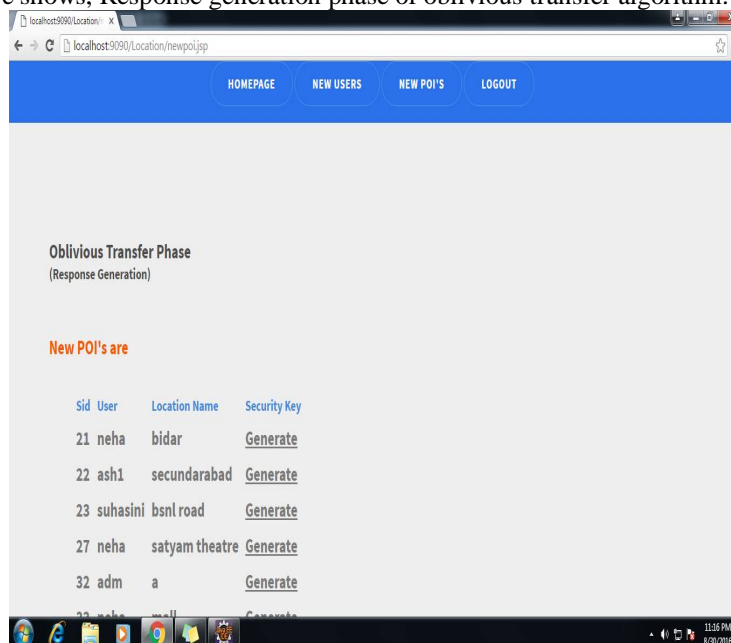


Fig.6. Response Generation Phase

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

The following figure shows the generated ID and symmetric key of that location.

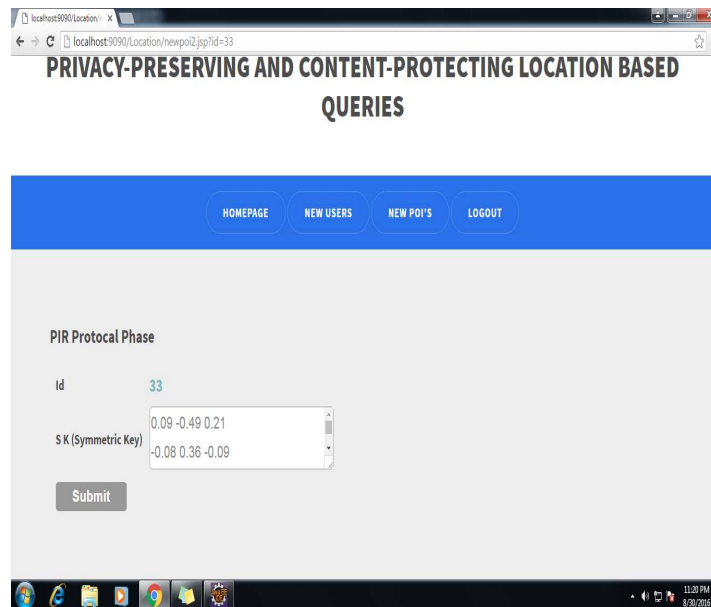


Fig.7. PIR Protocol Phase

The following figure shows, selecting starting point.

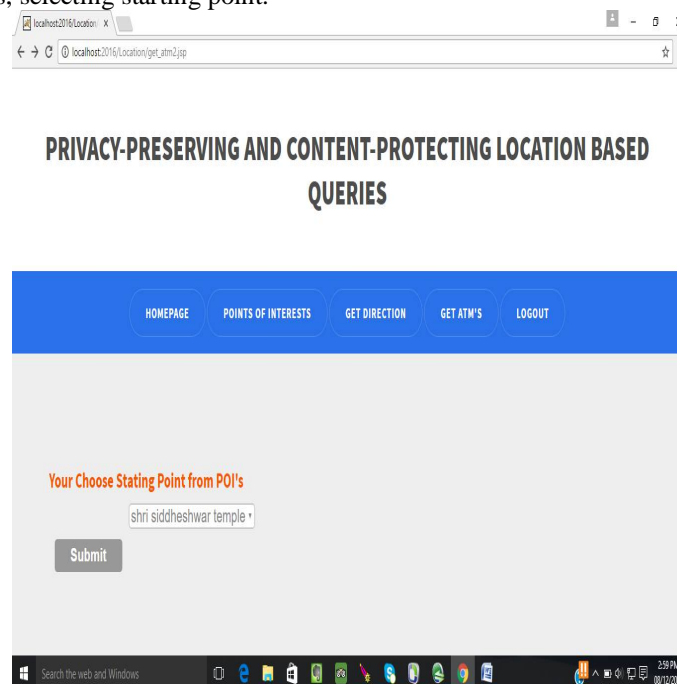


Fig 8 . Starting Point Selection

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

The following figure shows, Private information Retrieval Phase.

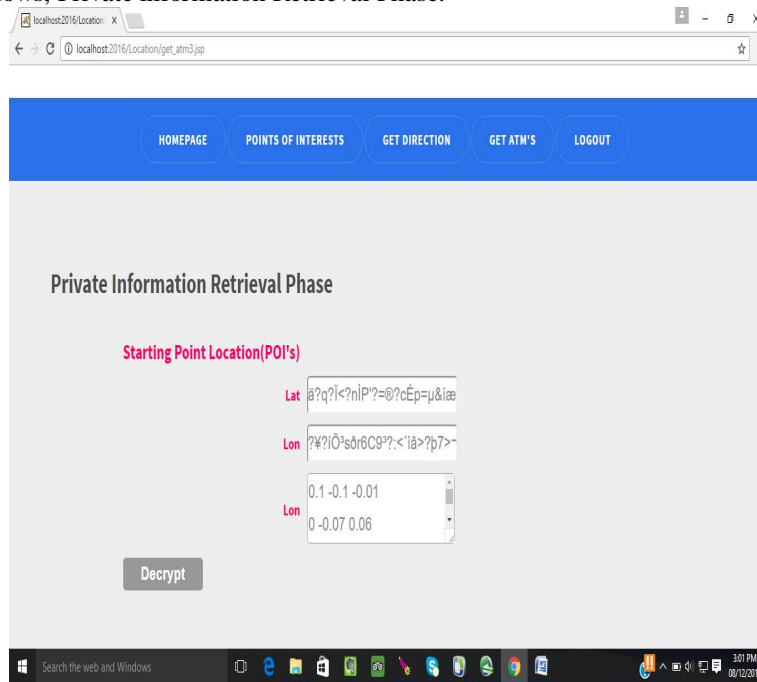


Fig 9 . PIR Phase

The following figure shows that, After decrypting the records we get nearest ATM's of selected starting point.

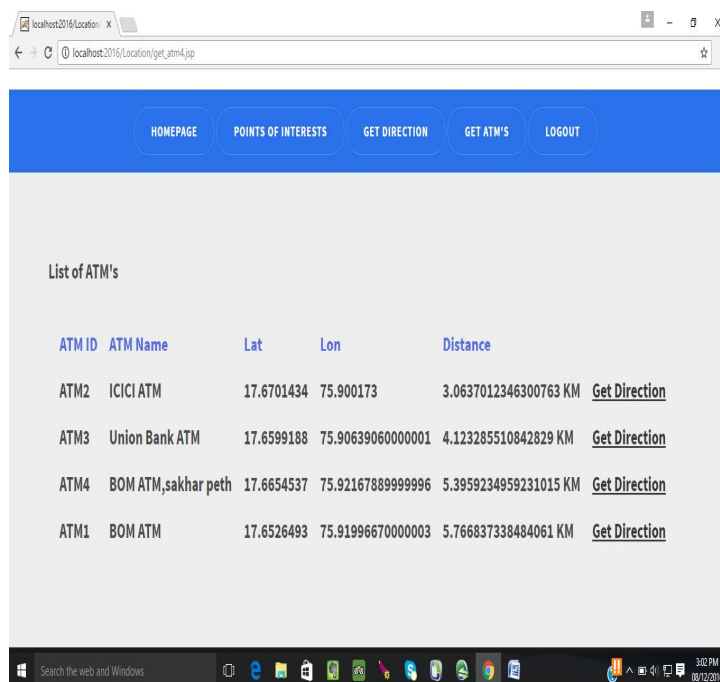


Fig 10. Nearest ATM

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

VII. CONCLUSION AND FUTURE SCOPE

With the development of powerful smart phones, LBS will become more and more popular. When enjoying these convenient services, users need to provide their privacy information such as location which is likely abused. Many kinds of existing privacy preserving technologies are reviewed. Several attacks (for example: transition attack, timing attack, etc.). The importance of privacy enhancing technologies to protect user's privacy is also discussed. Also introduces Satellite-based LBS and web-based LBS which is rife nowadays, and pointed out the privacy threats that users encounter and possible solutions. We also use technologies, such as location cloaking techniques (k-anonymity, p-sensitivity, location spatial cloaking, and Spatio-temporal cloaking), then Mix-zone, Fake points, path confusion, location obfuscation and pseudonyms approach etc.

Finally some future views with open challenges are summarized with respect to the privacy-aware location query processing. But there doesn't exist a comprehensive privacy preserving techniques or framework that covers all privacy requirements or issues to maintain location privacy in a secure manner. We have presented a location based search (LBS) solution that employs two protocols that enables a user to privately determine and get the location data.

We analyzed the performance of our protocol and found it to be both computationally and communicationally more efficient than the solution by Ghinita et al., which is the most recent solution. Future work will involve testing the protocol on many distinct mobile devices. Privacy preserving demanded techniques seems an appropriate approach to address such problem.

REFERENCES

- [1] (2011, Jul. 7) Openssl[Online]. Available: <http://www.openssl.org/>
- [2] M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," in Proc. CRYPTO, 1990, pp. 547–557.
- [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] C. Bettini, X. Wang, and S. Jajodia, "Protecting privacy against location-based personal identification," in Proc. 2nd VDLB Int. Conf. SDM, W. Jonker and M. Petkovic, Eds., Trondheim, Norway, 2005, pp. 185–199, LNCS 3674.
- [5] X. Chen and J. Pang, "Measuring query privacy in location-based services," in Proc. 2nd ACM CODASPY, San Antonio, TX, USA, 2012, pp. 49–60.
- [6] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," J. ACM, vol. 45, no. 6, pp. 965–981, 1998.
- [7] M. Damiani, E. Bertino, and C. Silvestri, "The PROBE framework for the personalized cloaking of private locations," Trans. Data Privacy, vol. 3, no. 2, pp. 123–148, 2010.
- [8] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in Proc. 3rd Int. Conf. Pervasive Comput., H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, pp. 243–251, LNCS 3468.
- [9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inform. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.
- [10] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in Proc. ICDCS, Columbus, OH, USA, 2005, pp. 620–629.
- [11] C. Gentry and Z. Ramzan, "Single-database private information retrieval with constant communication rate," in Proc. ICALP, L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., Lisbon, Portugal, 2005, pp. 803–815, LNCS 3580.
- [12] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "A hybrid technique for private location-based queries with database protection," in Proc. Adv. Spatial Temporal Databases, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., Aalborg, Denmark, 2009, pp. 98–116, LNCS 5644.
- [13] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection," GeoInformatica, vol. 15, no. 14, pp. 1–28, 2010.
- [14] 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.
- [15] G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacy-preserving matching of spatial datasets with protection against background knowledge," in Proc. 18th SIGSPATIAL Int. Conf. GIS, 2010, pp. 3–12.