Vertical Fragmentation of Location Information to Enable Location Privacy in Pervasive Computing

Jeeva Susan Jacob[1] and Preetha K.G[2]

[1] Rajagiri School of Engineering and Technology, Rajagiri Valley, Cochin, India
jeevasj27@gmail.com

[2] Rajagiri School of Engineering and Technology, Rajagiri Valley, Cochin, India
preetha_kg@rajagiritech.ac.in

Abstract.

The aim of the development of Pervasive computing was to simplify our lives by integrating communication technologies into real life. Location aware computing which is evolved from pervasive computing performs services which are dependent on the location of the user or his communication device. The advancements in this area have led to major revolutions in various application areas, especially mass advertisements. It has long been evident that privacy of personal information, in this case location of the user, is rather a touchy subject with most people. This paper explores the Location Privacy issue in location aware computing. Vertical fragmentation of the stored location information of users has been proposed as an effective solution for this issue.

Keywords: Pervasive Computing, Location Aware Computing, Location Privacy, Privacy issues, Vertical Fragmentation, Ubiquitous Computing.

1 Introduction

Pervasive computing techniques integrate three converging areas namely computing, communications and user interfaces to simplify the lives of users. This is accomplished with the assistance of a handheld user device like a smartphone. It imparts the reverse concept of Virtual Reality; to create a real life situation virtually using computing technologies. Pervasive computing enables the notion of anytime anywhere computing practically possible. Communication with diverse daily use devices can be done in most situations with the help of smartphones, sensors and the transceiver devices installed in them.

As an example, consider a situation where you are walking on a road. Your pervasive device, mostly a smartphone, tracks your location and senses other parameters related to your movement. If you have an accident and you faint, your phone can sense that your location is not compatible with the travelling plan you made. In addition to that, the sensors in the device can sense your heartbeat, blood pressure, body temperature and so on. So if you are hurt the device can alert the device in the nearest hospital or ambulance communication system all by itself. Thus valuable time is saved during accidents. Figure 1 shows this example case in detail.

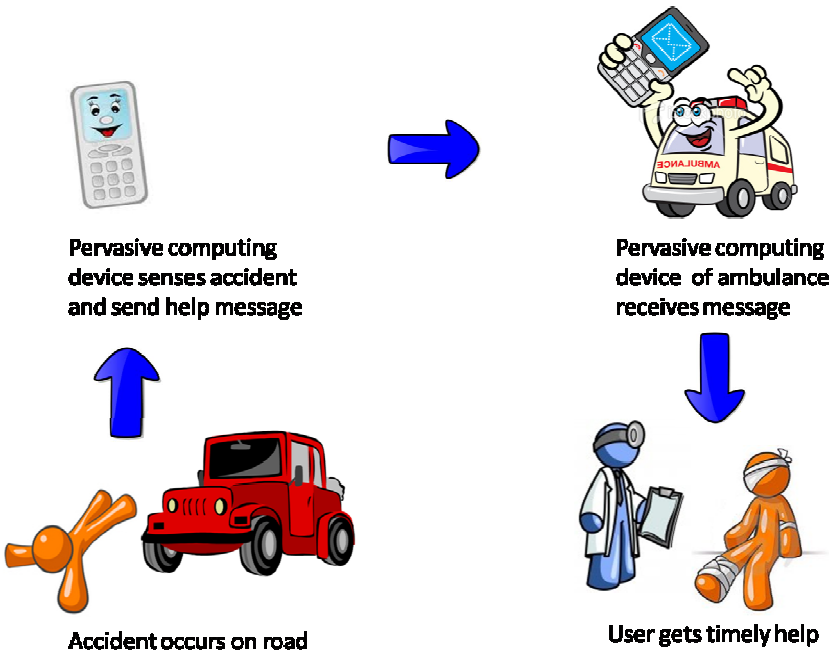

Fig. 1. Example for Pervasive Computing Application

Recent advances in technology have paved the way from pervasive computing by enhancing existing technical methods towards ubiquitous computing. Ubiquitous computing is more advanced form of pervasive computing where communication does not require a mediator device like smartphones. Any objects which have transceiver devices integrated in it can communicate with each other. Consider the previous instance of accident itself. Bear in mind that now you were travelling in a car and you had an accident. Here your car contacts the ambulance directly through the transceiver devices installed in them, thus utilizing pervasive computing. Figure 2 shows the previous example in a ubiquitous environment.

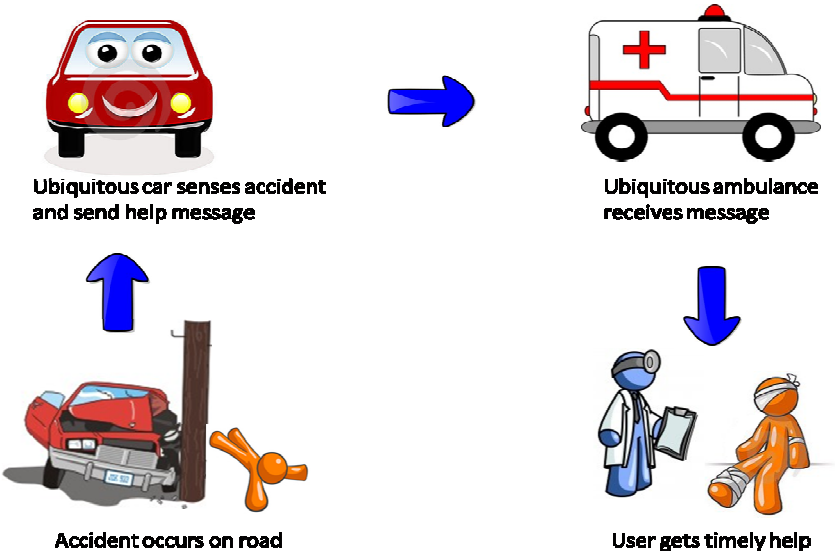

Fig. 2. Block Diagram of Location Aware Computing

Notice that in this case we are utilizing one of the significant application areas of pervasive computing; ie, Location aware computing. Location aware computing comprises of systems which percepts the location information of the users and changes their behavior or perform specific functions according to the instructions preprogrammed. In the example described, the location information of the user or the car enabled providing speedy and adequate medical attention to the injured user.

Location information describes a user's location over a specific period of time. They can be collected through the following methods.

- Locating Systems

  They detect the location of a device or find out the devices existing in a particular location. It provides the answer to the question: "What is the location of a particular pervasive device?"

- Location Systems

  They detect identification of the device and then determine the location information. It provides the answer to the question: "What pervasive devices exist in a particular region or location?"

Location aware computing consists of location sensing through the implementation of various sensing techniques, processing the location information as per location dependent or location aware queries and then provide them to advanced applications which execute functions based on this processed data. Figure 3 shows the functioning of Location aware computing.

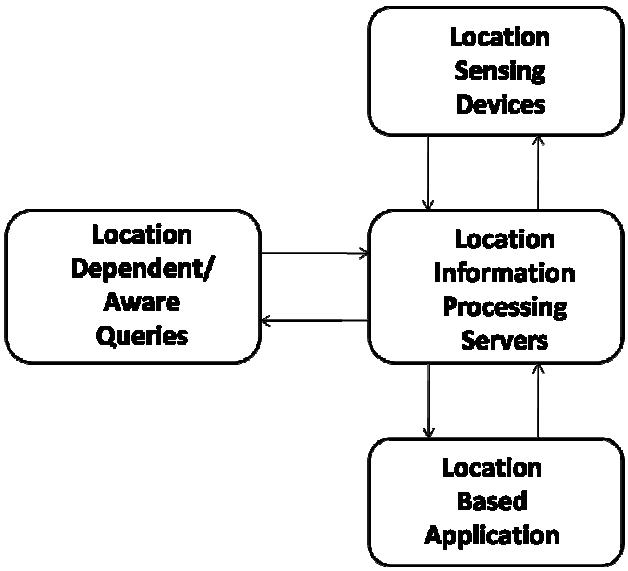

Fig. 3. Block Diagram of Location Aware Computing

Location information can be collected using the methods of proximity location sensing or triangulation. Proximity location sensing determines the nearest known location of a device or a famous site located in the proximity of the pervasive device. In the case of the triangulation location sensing, some geometrical methods based on displacement and angles are utilized for location determination. The main methods used are lateration and angulation.

Lateration senses the location of a user by performing calculations based on displacements with a known object. Angulation is a similar method to sense location based on the calculation of angles existing between lines of visions with known objects nearby. Another method for location sensing which utilizes nonmathematical steps is the scene analysis method. Here the location can be sensed by comparing and analyzing it with the locations of other prominent objects in the scene observed. These location sensing methods are shown in figure 4.

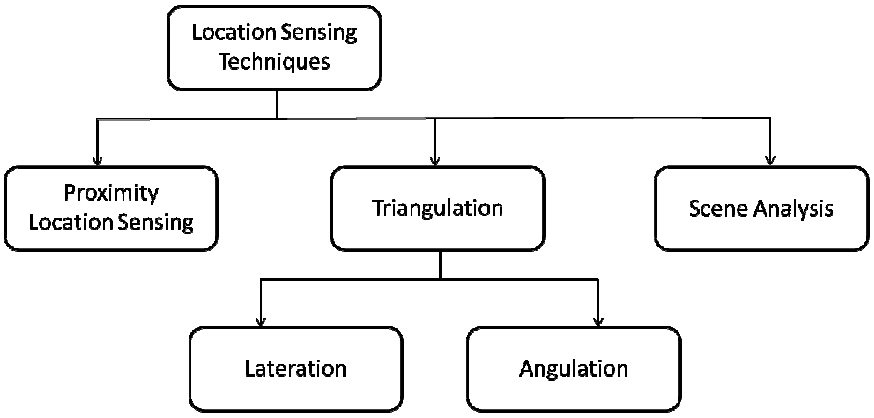

Fig. 4. Classification of Location Sensing Techniques

2 Location Privacy: Armament for Pervasive Computing

The major applications of location aware computing include location based advertising, instantaneous medical services, independent travels, resource discovery, network route selection and the like. The reduction in prices of location sensing hardware and the rise in the widespread use of personal handheld devices are opening up new opportunities in the domain of location aware computing.

One of the major challenges in location aware computing is ensuring privacy by the protection of location information of users. Privacy can be a sensitive issue when it comes to the majority of people. People insist on maintaining the right to determine who should be acquainted with what amount of information about them. Misusing location information can lead to major trouble to people. Exposure of the location information about some public figures might even be a threat to their lives.

Disclosing the location of a person can also lead to fraudulent attacks or spam attacks. Who will be responsible if someone changes the value of a coordinate in our location information to frame us for a crime we have not committed? Who would be okay with being under the limelight for each and every second of our lives? Users might always have the feeling of being exposed or constantly being tracked by alien eyes. This is because location information can uniquely identify us, just like our genetic profile. Figure 5 shows the bad effects of revealing the precise location of an individual.

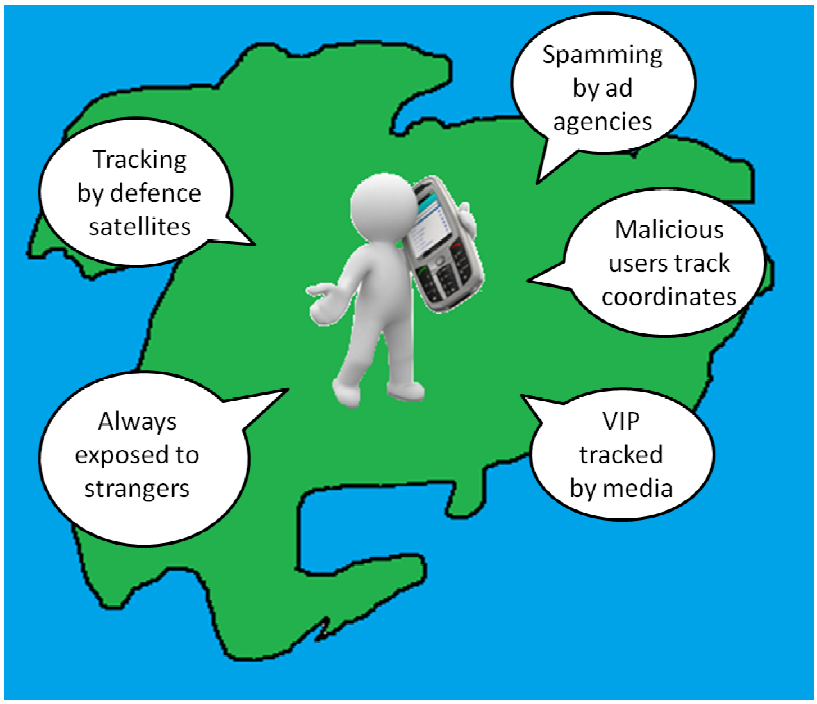

Fig. 5. User being tracked with respect to the location

Major location privacy attacks comprises of impersonation attacks, spam attacks and constant tracking of user's whereabouts. Laws have been passed in various countries to preserve the right of people to take decisions on the usage of data regarding their whereabouts by the government or other communication service providers. But these do not cover the location tracking of users and using this location information for various applications. Effective methods need to be developed for ensuring location privacy in pervasive computing.

3 Related Work

Numerous methods have been proposed by researchers around the world in this field. Privacy Sensitive Information Diluting Mechanism (PSIUM) [17] ensures privacy in the user location data collected by service providers by sending multiple location information messages along with service requests. Device can select the accurate information from these, but the service providers cannot. Use of mix nodes [1] reorders the packet flow thus confusing attackers since these packets appear to be independent of each other.

LocServ [1] acts as a middleware layer between location sensing devices and location dependent applications. It gives the control of location information to corresponding users. Thus it prevents transfer of location information to other third party agencies which may query the server for location data of users. Another technique is Mist [1], which is specially designed to provide location privacy for users in pervasive computing environments. The GeoPriv [18] model integrates location based services with location privacy preservation measures for effective implementation of location based applications. This is designed for applications dealing with surveying, mapping, tracking and so on.

Majority of these proposals are for preventing privacy attacks by tracking the traffic flow through these systems. In this paper, a proposal for preserving privacy of location information

of users by preventing attacks on the servers using fragmentation techniques is discussed. Third party attacks and tracking attacks on the information storage base in the location servers can thus be prevented by this method.

4 Fragmentation: A Database Trait for Preeminent Storage

Fragmentation is a technique commonly used in database management systems to classify data belonging to a single database and store them properly. Usually it is done in the case of distributed systems, where systems distributed among geographically distant regions share resources and applications. Fragmentation and replication of databases is done to ensure durability and redundancy of significant data in distributed systems. These are mainly of the types: horizontal fragmentation and vertical fragmentation.

Horizontal fragmentation is done based on the rows or tuples of the database. This is done to separate tuples or records belonging to a single database into parts. This may happen when storage of data need to be divided into separate sections or to retrieve some tuples belonging to a particular category which complies with some constraint. Reconstruction of the original database is much easier in this case. Each horizontal fragment with tuples can simply be joined together or can be joined in the order of their primary key.

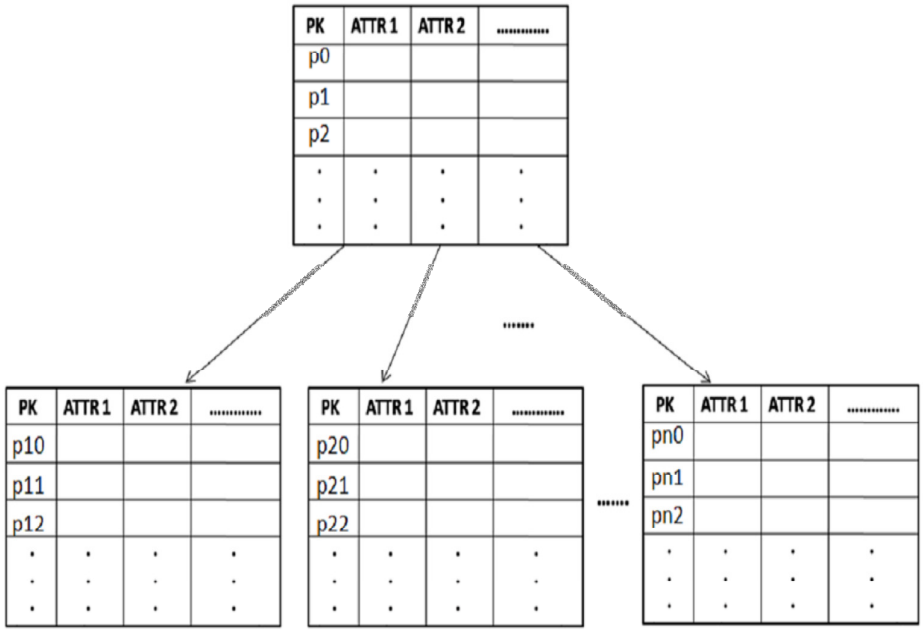

Fig. 6. Horizontal Fragmentation of Database

Vertical fragmentation is done based on different attributes of a database. Each fragment is separated based on a particular attribute related to the tuples. On each fragment a unique key field is attached so that queries can be executed without rejoining these fragments. In most cases the primary key of the database is replicated in each fragment.

Figure 7 shows the vertical fragmentation of a database where each fragment has the primary key field, PK, to interlink them as and when required. By using this method we can fragment the data regarding the users stored in location servers. This separates the location information from the user's personal information. Thus an attack on the data storage cannot effectively

reveal a particular user's location. A malicious attacker may never be able to connect the user with the corresponding location information when the details of the user lies in separate fragments of storage.

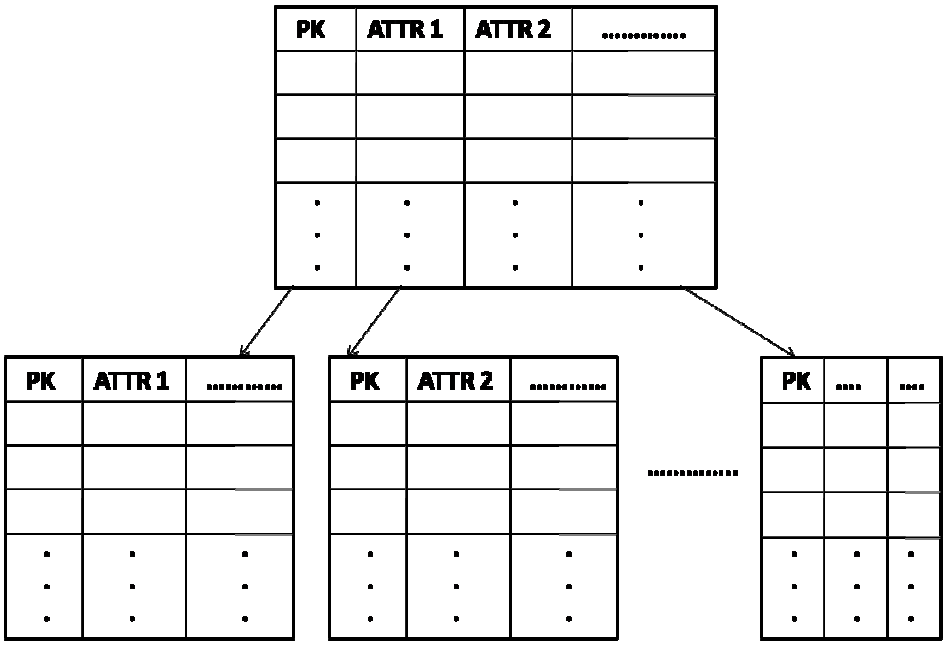

Fig. 7. Vertical fragmentation of Database with PK as the primary key field

5 Vertical Fragmentation on Location Information

Location information of users is usually maintained in the location servers using Location Area Identity (LAI). This uniquely identifies the location area (LA) of a particular user at a particular instant of time.

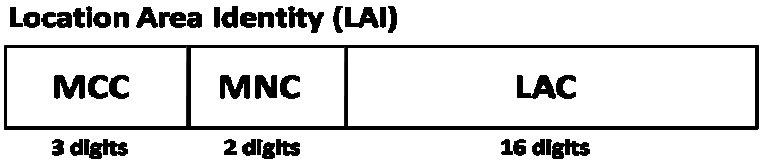

Fig.8. Vertical Fields of Location Area Identity (LAI)

This information is stored in the Visitor Location Register (VLR) of the communication network infrastructure used by the user's smartphone or handheld device. LAI comprises of Mobile Country Code (MCC) which identifies the country, Mobile Network Code (MNC) which identifies the mobile network used and the Location Area Code (LAC) which identifies unique locations.

When a communication or some other service is requested by the user, the location server tracks the current location of the user through the handheld device and then provides the

suitable service. Thus on querying the database which stores the user's profile with personal as well as location information the user can be tracked without much difficulty. So, in order to prevent attacks on these databases, vertical fragmentation can be applied fragmenting the personal information and location information into separate modules of storage.

The values for the unique key field to be added to each of these fragments need to be carefully calculated. Here the Subscriber Identity Module (SIM) (19-20 digits), International Mobile Equipment identity (IMEI) (15 or 17 digits), MCC (3 digits) and MNC (2 digits) values are considered. These are mathematically combined and a fixed length hash value is generated using a suitable hash function. These values will vary for each user and thus the new key value generated will also be unique.

A key field with unique key values thus calculated is added to each of the database fragments containing personal information and location information respectively. When a service request is sent by the user, the server can calculate the unique key field value and then combine the required records of the fragments to form the original record with both personal and location information. The request is then processed based on the information gathered and the requested service can be provided as per the user's eligibility for receiving that service.

Figure 9 shows the vertical fragmentation of location server databases. In the case of an attack on the server, the attacker cannot identify which tuple in the location information fragment corresponds to the particular entry in the personal information fragment. Also fake requests can be identified since imposter would not be able to fake location information since SIM and IMEI numbers are both considered here. In order to ensure more security to the method the hash function used can be changed periodically.

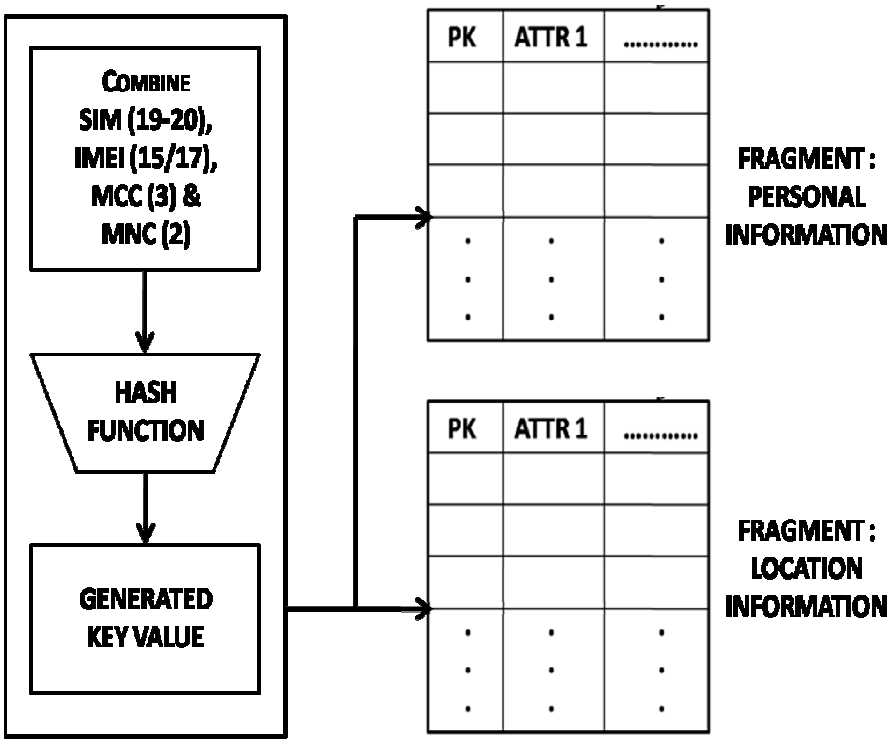

Fig.9. Vertical Fragmentation to ensure Location Privacy

Thus, this method ensures privacy to the users by preventing attacks on the location server databases by third party or malicious agencies. Since this method separates the location information from the personal information any outsider who intends to attack finds a whole load of data with no connection to one another. Unfortunately, it cannot prevent the misuse of location information by the service provider itself, since all the values considered are known to it.

6 Future Enhancements

Although the proposed method can ensure privacy of location information from external attacks, measures need to be adapted to prevent misuse of it by the service provider network. Privacy Laws may prevent it up to a limit, but effective techniques are required. One method would be to provide only an approximate value for the location information instead of the accurate coordinates of the location.

Future work also involves research on methods for preventing other kinds of privacy attacks. Since enhanced pervasive computing or ubiquitous computing techniques does not depend on handheld user devices, other hardware independent measures need to be developed. Advancements in hardware technology and communication standards can accelerate the transformation from Pervasive computing to Ubiquitous computing.

7 Conclusion

As Anthony Burgess says, “To be left alone is the most precious thing one can ask of the modern world”. In a world which is evolving into a global apartment building from a global village, ensuring location privacy is a crucial fight against the peeping toms of the communication world. Measures from the world governments, like the Location Privacy Protection Bill (2011) which forces Google and Apple to get user’s permission before location information is tracked, reassure the public that all is not lost yet.

This paper discusses the issue of Location Privacy of users in Pervasive computing environments. Vertical Fragmentation technique has been proposed as a solution for the attacks on Location Servers and theft of location information. Its effectiveness in preventing third party attacks and fake users have been analyzed theoretically. Even though internal attacks cannot be prevented, it ensures location privacy for the users of a reliable service provider.

References

1. Pankaj Bhaskar, Sheikh I Ahamed, Privacy in Pervasive Computing and Open Issues, Second International Conference on Availability, Reliability and Security (ARES07), April 2007.
2. Nilothpal Talukder, Sheikh I Ahamed, How much Room before you Rely: Balancing Privacy control and Fidelity in the Location-based Pervasive Applications, Nineth International Conference on Mobile Data Management Workshops, April 2008.
3. Sebastian Fischmeister, Guido Menkhaus, Alexander Stumpfl, Location-Detection Strategies in Pervasive Computing Environments, Proceedings of the First International Conference on Pervasive Computing and Communications (PerCom03), March 2003.
4. A. Michael Berman, Sue M. Lewis, Anthony Conto, Location-Aware Computing, in page http://net.educause.edu/ir/library/pdf/DEC0803.pdf, November 2008.
5. Young Jae Kim, Location Aware Computing, in TermPapers page http://crystal.uta.edu/˜kumar/cse6392/termpapers/Young Paper.pdf , November 2002.
6. Claudio A. Ardagna, Marco Cremonini, Sabrina De Capitani di Vimercati, Pierangela Samarati, Location Privacy in Pervasive Computing, in page http://spdp.dti.unimi.it/papers/CL 2008 2.pdf, November 2008.

7. Matt Duckham, Lars Kulik, Location Privacy and Location-aware Computing, in Papers page http://www.geosensor.net/papers/duckham06.IGIS.pdf, December 2005.

8. Mike Hazas, Andy Ward, A High Performance Privacy-Oriented Location System, Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom'03), 2003.

9. Denise Anthony, David Kotz, Tristan Henderson, Privacy in Location-Aware Computing Environments, Published by the IEEE Computer Society, IEEE 2007.

10. Claudio A. Ardagna, Marco Cremonini, Sabrina De Capitani di Vimercati, Pierangela Samarati, An Obfuscation-based Approach for Protecting Location Privacy, IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING, 2009.

11. A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. PERVASIVE computing, IEEE CS and IEEE Communications Society, (1):46–55, 2003.

12. Patterson, C.A.; Muntz, R.R.; Pancake, C.M.; Challenges in location-aware computing, Pervasive Computing, IEEE, June 2003

13. Lin Yao; Chi Lin; Xiangwei Kong; Feng Xia; Guowei Wu;, A Clustering-Based Location Privacy Protection Scheme for Pervasive Computing, Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom), March 2011.

14. Reddy, Y.V., Pervasive Computing: Implications, Opportunities and Challenges for the Society, Pervasive Computing and Applications, 2006 1st International Symposium on, January 2007.

15. Jacobsson, M.; Niemegeers, I., Privacy and anonymity in personal networks, Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on, March 2005.

16. Myles, G.; Friday, A.; Davies, N., Preserving privacy in environments with location-based applications, Pervasive Computing, IEEE, April 2004.

17. Cheng, H.S.; Zhang, D.; Tan, J.G., Protection of privacy in pervasive computing environments, Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on, May 2005.

18. John Morris; Jon Peterson; Who's Watching You Now?, Security & Privacy, IEEE, February 2007.

19. Konings, B.; Schaub, F., Territorial privacy in ubiquitous computing , Wireless On-Demand Network Systems and Services (WONS), 2011 Eighth International Conference on, February 2011.

20. Schlott, S.; Kargl, F.; Weber, M., Short paper: Random IDs for preserving location privacy, Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on, March 2006.

21. Prof.Yenumula Venkataramana Reddy ," Pervasive Computing: Implications, Opportunities and Challenges for the Society" 1st International Symposium on Pervasive Computing and Applications,2006.

22. Bosheng Zhou, Alan Marshall, Tsung-Han Lee, "Wireless Security Issues in Pervasive Computing",Fourth International Conference on Genetic and Evolutionary Computing (ICGEC), 2010.

23. M. Gruteser, J. Bredin, and D. Grunwald. "Path privacy in location-aware computing", In Proc. of the Second International Conference on Mobile Systems, Application and Services (MobiSys2004), Boston, Massachussetts, USA, June 2004.

24. S. Patil and J. Lai, "Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application," Proc. SIGCHI Conf. Human Factors in Computing Systems (CHI 05), ACM Press, 2005, pp. 101–110.

25. B. Gedik and L. Liu. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. IEEE Transactions on Mobile Computing, 7(1):1–18, January 2008.

26. B. Ho and M. Gruteser. Protecting location privacy through path confusion. In Proc. of IEEE/CreateNet SecureComm 2005, Athens, Greece, September 2005.
27. M. Langheinrich. A privacy awareness system for ubiquitous computing environments. In Proc. of UBICOMP 2002, Goteborg, Sweden, September-October 2002.
28. R. Kui, L. Wenjing, "Privacy enhanced access control in pervasive computing environments", 2nd International Conference on Broadband Networks, Oct 2005, pp. 384-393.
29. M. R. Stytz, "Protecting Personal Privacy: Hauling Down the Jolly Roger", Security & Privacy Magazine, IEEE, Volume 3, Issue 4, July-Aug 2005, pp. 72-74
30. A. R. Jacobs, G. D. Abowd, "A Framework for comparing perspectives on privacy and pervasive technologies", Pervasive Computing, IEEE, Volume 2, Issue4, Oct-Dec 2003, pp. 78-84.
31. R. K. Thomas, R. Sandhu, "Models, protocols, and architectures for secure pervasive computing: challenges and research directions", Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 14-17 March 2004, pp. 164-168.
32. Z. Feng, M. W. Mutka, L. M. Ni, "A Private, Secure, and User-Centric Information Exposure Model for Service Discovery Protocols", IEEE Transactions on Mobile Computing, Volume 5, Issue 4, July-Aug. 2006, pp. 418-429.
33. M. Tentori, J. Favela, M. D. Rodriguez, V. M. Gonzalez, "Supporting Quality of Privacy (QoP) in Pervasive Computing", Sixth Mexican International Conference on Computer Science, 26-30 Sept. 2005, pp. 58-67.
34. M. Decker. Location privacy-an overview. In ICMB '08: Proceedings of the 2008 7th International Conference on Mobile Business, pages 221–230, Washington, DC, USA, 2008. IEEE Computer Society.
35. B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady. Enhancing security and privacy in traffic-monitoring systems. IEEE Pervasive Computing, 5(4):38–46, 2006.
36. K. Nahrstedt, D. Xu, D. Wichadakul, and B. Li. QoS-aware middleware for ubiquitous and heterogeneous environments. IEEE Communications Magazine, pages 140–148, November 2001.
37. A.R. Beresford and F. Stajano. Mix zones: User privacy in location aware services. In Proc. of IEEE PERCOMW 2004, Orlando, FL, USA, March 2004.

Authors

Ms. Jeeva Susan Jacob

M.Tech scholar at Rajagiri School of Engineering and Technology, Cochin, India. Completed B.Tech Degree from Mahatma Gandhi University, Kerala India. Research areas of interest include Mobile Computing, Pervasive Computing, Green Computing, Computer Networks and Wireless Communication.

Ms. Preetha K.G.

Assistant Professor at Rajagiri School of Engineering and Technology, Cochin, India. Currently pursuing research in Mobile Adhoc Networks. Research areas of interest include Mobile Computing, Adhoc Networks, Computer Networks, and Wireless Communication.