

Preserving Location Information Privacy in Location Database

Abubakar Sani¹, Hadiza Ali Umar², Zauwali Sabitu Paki³, Usman Ubandawaki⁴
Graduate Assistant, Department of Computer Science, Northwest University, Kano, Nigeria¹
Lecturer II, Department of Computer Science, Bayero University, Kano, Nigeria²
Graduate Assistant, Department of Computer Science, Northwest University, Kano, Nigeria³
Lecturer III, Department of Computer Science, Niger State Polytechnic, Zungeru, Nigeria⁴

ABSTRACT: During a conference held in April 2011, a bombshell was dropped that apple iPhone and 3G iPad were recording devices locations and; this led to interrogation of other phones and apps and proved to be extracting and recording location information that are stored somewhere [1]. This collected information is being stored in a database file named “*consolidated db.*” [2]. As mobile and other handheld devices connect and disconnect from mobile network anytime anywhere, we shall be posed with privacy threat. This flexibility no doubt is being caused in the process of accessing Location based services (LBS) among others. These LBSs are applications access on mobile network by mobile devices using their current locations appropriately. Basically, the idea is that, location systems track users automatically and collect sensitive information; such should be control against eavesdroppers as well as allowing access to services. For any LBS to be offered to a user, the location server has to be contacted directly or indirectly and therefore, preserving privacy of such information in the server, is worth researching. Our proposed research focus only on those LBS where user must reveal the user identity in accessing them. Our methodology does not guarantee absolute privacy as perfect privacy is impossible to achieve as long as communication takes place [3].

KEYWORDS: Location privacy, location information, location database, LBS, ubicomp, threat, cellphone

I. INTRODUCTION

As mobile and other handheld devices have the right to join and leave a mobile network anytime, anywhere; this make the devices and their network insecure which is worrisome[4]. This dynamic connectivity of devices could be caused by accessing Location-based services (LBS) among other things. These LBS could be seen as services that require location of mobile devices plus any other information in order to provide added value to the users [5]. According to [6], it is the application that utilizes geographic location. LBS are “services that can be accessed by mobile network and utilize the current location of the mobile device appropriately” [7]. These services are day by day exploding with the rapid increase in usage of smart phones and that becomes a standard killer app on many cell phones. Majority of these LBS have their own way of collecting and retaining detailed records of the location of consumers and combine these records with other information to build profiles revealing the details of consumers’ personal lives. These contribute in revenue generation to cell phone network operators and location-based service providers. Mobile network operators, due to their own nature of services rendered to public and private individuals, have to outsource third-party operator in the provision of LBS to users as their expertise is not solely on LBS [8]. For any LBS to be offered to users, the location server has to be contacted directly or indirectly. This Location information server (LIS) is typically a database that maintains mapping for each registered user who accesses it and provides information regarding the location of resources (i.e. mobile devices) that can be identified in the network. It is a server that gives a user summarized and customized results in line with his exact location information [9]. Since it receives user’s location and remains unprotected, therefore, it is susceptible to information leakage due to operator errors, system bugs or active attack [10], [11] and ultimately humiliates, embarrasses and tarnishes reputation unjustly [12]. However, for any location information that goes viral it may inflict a high degree of physical, economical, and legal damage to individual(Rohan J. Patil et al., 2015). Consequently, this database and the risks involved is worth researching.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

So many researches have been done and a lot of architectural design, techniques, and policies had been proposed in ubiquitous computing environment with respect to protecting privacy in the Location Server, the more the research; the more issues that are uncovered.

II. PRIVACY

Historically, privacy could be dated back to 1361 which covers media, territorial, and communication & information privacy [13]. Privacy definition is ambiguous and elusive depending on the situation and context [14]. According to [13] it is right to be left alone, but [15] sees it as “control over information disclosure”. Generally speaking, these definitions give privacy a literal meaning. In Computer Science & Information Technology, it could be seen as control over disclosure of Personally Identifiable Information (PII). Since users move within ubiquitous (UbiComp.) environment and interact with ubiComp systems, it seems difficult for them to know who, when, where and, how these devices expose their privacy. According to a survey, users of smartphones by 2015 will reach about two billion [16]; confidently enough we can realize that one-third of the world population face privacy threat willy-nilly.

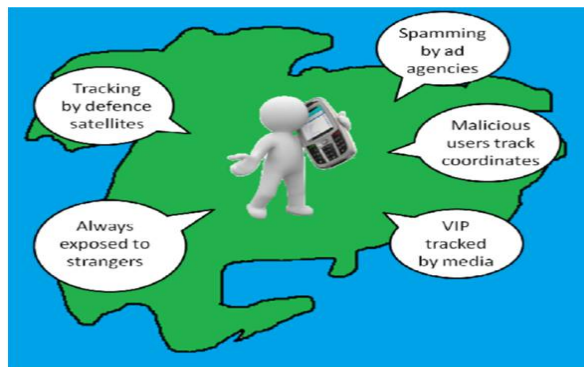


Fig 1: user being tracked in ubicomp environment (Jacob and Preetha, 2013)

A. Location Privacy

It is same as data privacy [17], and is “the ability to prevent other parties from learning one’s current or past location” [18]. The moment user location is described with respect to time, it then turns to location information [19], and this forms a bedrock of our research.

B. Location Information Technology

There exist technologies involved in collecting this information, ranging from hardware, software (application) and protocols. Some of these reveal location information as text-based while others map-based. We shall see them below:

- i. **Cell Phone:** This is the basic hardware technology close to user. As mobile device is put to on, whether user makes or answers call it discloses and updates location information to carrier’s database named *Home Location Registers* (HLR) in every 7 seconds [2]. The carriers have a choice in determining how to receive such information without users consent: - Network-based (Subscriber Identity Module) and Handset-based. To compute user’s location in network-based, SIM facilitates that through Base Station (BS) and; in Handset-based on Equipment Identity Register (EIR) attached to mobile station (MS) does that [20].
- ii. **Global Positioning System (GPS):**It is a software technology within a user’s cell phone or Personal Digital Assistant (PDA) with satellite receiver that relies on satellite in computation of location-based latitude & longitude [2]. It gives scientific location and timing, and works under any weather condition as long as the device is outdoor [21]. It gives higher accuracy than other technologies [2], [22].
- iii. **Internet Protocol (IP):** An IP is another technology in protocol suit that serves as an alternative to conveying location information when other technologies are unavailable [2], [22]. Devices connected to the internet to access location-based services or making internet call are identified when their IP is mapped to specific city around the globe.
- iv. **Wireless Positioning:** location of a device could be ascertained and stored through its access point. The issue to this is that high accuracy in revealing its location is impossible.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

C. *Parties to Location Information*

These are entities that either use location information for business purposes and/ or state security reasons. We only intend to give a brief account of how they retrieve device location.

- i. **Cell Phone Manufacturer:** Many smart phones possess in-built GPS that records user's position in real-time. This position is in form points and are being sent to their database else somewhere.
- ii. **Location-based App:** They play their role at software level. They develop and market LBS app that uses device current location (i.e. Google latitude, loopt etc.).
- iii. **Cell Phone Service Providers:** They track user's location who subscribes to their network. Real life example is, Deutsche Telekom that recorded a German politician coordinate 35000 times in six months period [2].

III. BACKGROUND REVIEW

Privacy Aware Database is a policy that is based on third-party server in the name of location anonymizer. In this, mobile user location is collected, blurred and then forwarded to Location server [23]. The imposter will find it difficult to attack the location data during transmission to the server but, since the bedrock of this scheme was encryption-based; the server could be subjected to reverse engineering and consequently may lead to location information disclosure. In [19], vertical fragmentation is applied to the location server which isolates users' personal information from the location information. On attack to the server, the third party may not link these two vital information let alone disclose it. The good side of this work was that user information is stored in the server through user's smartphone or any handheld devices that must use Location-Area Identity (LAI). This LAI plays a gigantic role in determining his/her position, as it is the composition of the Mobile Country Code (MCC), Mobile Network Code (MNC) and Location Area Code (LAC). The downside of this technique is the inability to protect Location Service providers from misusing the information as they know how to interlink the distributed fragments. But in [24], user data and location information are separated into two different servers (Data Server and Index Server). The transformed and encrypted data and location details are kept in their respective servers, and authorized users are allowed to access record of any user through untrusted proxy server provided they possess decryption keys. We can boldly say that technique use here is similar to (Jacob and Preetha, 2013), but added data modification techniques to it which makes it one step further towards preserving client location privacy and compelled users to use proxy in accessing Index/Data Server to avoid direct contact with user device. This adds to computational and communication overheads.

Dummy "Fake Users" [25] is a new technique aimed at breaking the problem of traceability link. It transforms location information of a user by adding noise to it and sent to the service provider (N-query but only one contain the true position of the user). The noise consists of false location called "dummy", hence, the name of the technique. The provider sends a reply message to user (user only extracts the response that matches his true position and ignores the rest) [26].

To protect device location privacy in wireless environment, [27] proposed a pseudonym technique aimed at changing device pseudonym at predefined time interval coupled with *silent period* to stop the device from signal transmission temporarily. Basically, *silent period* was introduced to thwart adversary from tracking signal and, user device can be in this mode anytime anywhere at random time. New *id* is obtained at resumption of communication [28]. There are location-based applications or services that forward user query only when his true identity was identified. Ideally, user device in this policy is PSIUM-Enabled, that allows promotions of latest product that are within the specified range to be received through N query [29]. Nearest ATM, Coffee shop, nearest Filling station and any other Point-of-Interest (POI) are all what the devices received as part of location services. The greatest advantages of this work are: users send N query to LBS instead of 1, in which N - 1 queries are false. Secondly, during service access "Big Brother" might be confused in differentiating true from false query. The challenges of this work are limited to: high rate of transmission cost from LBSP and, an attack to server may reveal some vital information with regards to user coordinate.

Preserving location information could be one of these three architectures: User-centric, Client-Server and Trusted Third-Party. In (C. Yu et al. 2008), the technique proposed was Trusted third-party and used the concept of cache. Mobile user instead, sends his query to an agent called location cloaker, it then conceals his coordinate and forwards it to LBS. LBS resolves the query and sends it back to an agent which sends it to user. For any request that was sent, an agent must cache it for future request. This limits the number of servers to have contact with other user location that their future request is in agent's cache. Any attack on it limits the damage. However, location cloaker increases computational resources and power.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

[8] Used trusted third-party technique but instead of cloaking, the author chose to encrypt the location data via mobile network service provider. Encryption as it denotes “Secret Writing” [30]. The art of concealing information using encryption technique alone is not preferable as it leads to suspicion [31] and unauthorized third party may be curious enough to try to decipher it. But in [32], the stored information in the server was degraded using Generalization and Suppression method, these retain less data in the server and remove some parts of it. With this, unauthorized party might see the data useless but affect data usability.

There exist a technique in which a user contacts location server for LBS only if his/her local query could not be resolved through local response [33]. The idea behind this policy was that users operate in peers and their access to the server was limited; any peer can resolve a query locally (i.e. which was already resolved by server) to its fellow. This policy did not properly address privacy with respect to server but, rather reduces access to it. Similar architecture was proposed by (S. Leon, et al 2010) but the concept of K-anonymity was incorporated. A query goes to Anonymisation Server (AS), obfuscate it (i.e location coordinate) and forward the concealed request to server for LBS. The modus operandi in this proposal was that no user query would be allowed to pass through unless and until there exist K-1 users in his region or, otherwise expansion takes place in search of K-1 users requests. This greatly reduces network attack. With this scheme, user’s query will be temporarily suspended during expansion and, eventually get denial of services as long as his request does not satisfy k-1 user request. Hence, appraise the system unreliable. [34] introduced the idea of *k*-anonymity in protecting location privacy. Their approach is that mobile user reports his blurred area to his fellow user containing his position and positions of *k*-1 that is pseudonym-driven. Among *k* objects (mobile users), the target user is indistinguishable from other *k*-1 objects (mobile users) and the guarantee of user privacy is always 1/*k*. This idea is also applicable in data mining area. In Spatial cloaking, user location is perturbed through Anonymising Spatial Region (ASR) by a server called *anonymizer*. It then forwards the request to LBS and filtered the result back to genuine user. *k*-anonymity is applied in ASR [35]. The good work in this policy is that during service request to LBS the location is unknown. But it poses privacy threat by allowing the anonymizer to keep record of user location.

Instead of Trusted Third-Party architecture, [36] chose to propose K-anonymity using client- server architecture. Generalization and suppression was applied onto the database in order to preserve location information. Generalization is just a technique of replacing or recording values with unspecific symbolic values. Simply put, its a data distortion [37]. Mix zone is the idea of frequently changing pseudonyms for location privacy proposed by [18]. Here people (mobile users) only report their location to the server in certain regions, named “application zones”, where a location-based service is offered, such as restaurant, pilling station or hospital. In the zones outside the application zones, users receive new unused pseudonyms. This strategy prevents man-in-the-middle attack and linkability problem, because someone in the mix zone might be using it.

In RADIUS, client issues an Access-Request that contains his/her authentication information to the server and the server processes the request locally if it recognizes the user; otherwise it acts as a RADIUS Proxy "or intermediate" by transmitting it to another server. The Radius Proxy in one direction, and then in the other. When the request arrives at the Radius server corresponding to the identification item, it validates or rejects the request by sending a packet type Access- Accept or Access-Reject. The main advantage of Radius is the decentralization of the authority of authentication and the deployment of relations between servers, by propagating information from one server to another. In this technique, the forwarding of authentication data between servers increases the risk of identity disclosure of the user at several levels of Radius Proxy by a third party who has taken control of an intermediate Radius server, or by a curious server administrator who wants to read authentication data that are not destined to it [14].

MIST: Is a communication protocol that allows entities to identify and authenticate themselves in a pervasive space while preserving the user's privacy in their location. The drawback of this policy is that, user’s behaviour within the system can be observed by an intruder who is physically present in the ubiquitous space. [14]. In[38] authorized users are only allowed to use the services with the assistance of lighthouse, encryption and handlethat facilitates in separation of user identity from his location.

[39] Proposed a technique that masks client true identity as well as true nature of his service request. One out of the request sent by a client is true and the rest are false. The beauty of this is that, third party and providers will find it difficult to detect the actual id and request. The shortcoming in this technique is that the service providers must keep true location coordinate and the result that were previously used.

(Kurkovsky et al. 2013) proposed a mechanism that collects location information about its users by creating digitally signed location objects that encapsulate user location data and their privacy requirements. This model provides coupling of data when location information passed between multiple applications. Path confusion is the approach

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

propose by [40] where perturbation algorithm is use in gathering client location. The algorithm cross path user area (users that are within same location or close to each other) and also cross path users moving in parallel with the aim of fooling and confusing an attacker from location inference.

From the literature above, we can argue that only two authors have worked on LBS that requires user to reveal his identity but, provided insufficient technique to preserving locational data. Therefore, we propose an architecture that sufficiently shields user location information in LBS server.

IV. OUR ARCHITECTURE

Our proposed architecture is based on Client-server where, all users send their LBS request to the server without an agent (middleware/ Anonymous server) and the server applies the best suitable privacy technique. To impleement this, either of the following way could be used: implementation on the stored data at row, column or table level, and or on the entire database schema. MySQL Workbench 6.2 would assist us in achieving the desired goal.

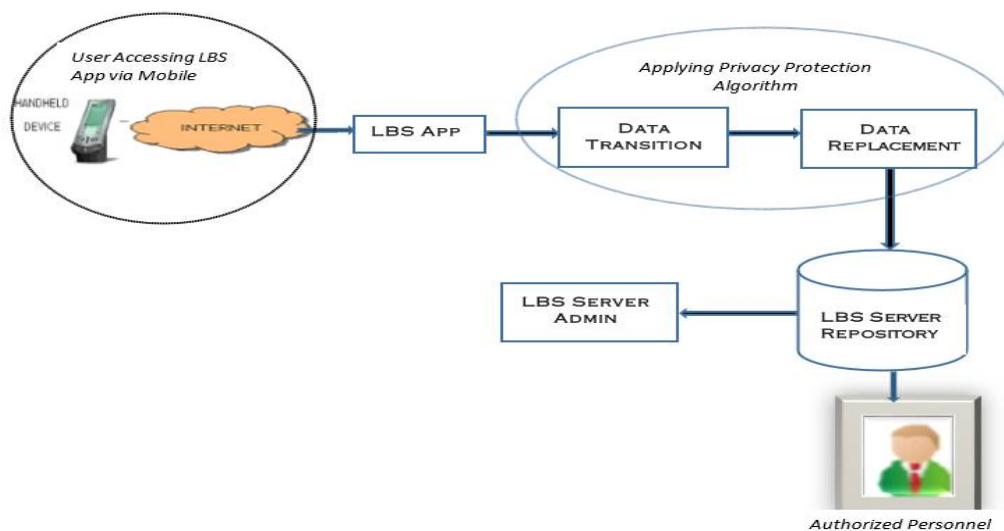
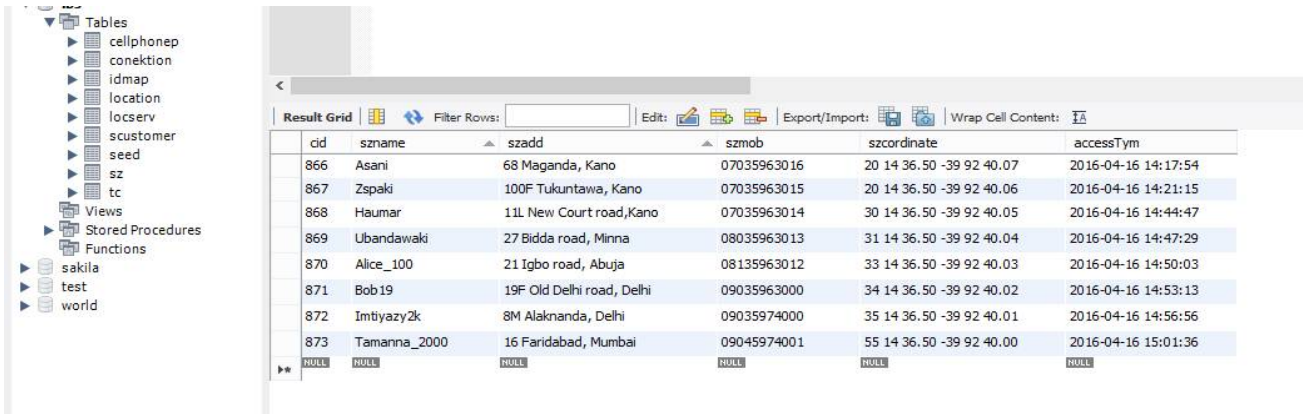


Figure 2: Architecture Diagram

Basically, user accesses such LBS that is not pseudonym driven or does not work anonymously via his smart phone. His location detail will be transformed in *Data Transition* stage and goes to the server. On arrival to the server, second stage of transformation takes place in *Data Replacement* stage. This conceals the information in the server and, in case of external or internal attack, the data there is distorted and difficult to establish valuable information. Our strategy provide more privacy in the database in the sense that the, stages in preserving it is in two level (Transition level and Replacement level).

V. EXPERIMENTAL RESULTS

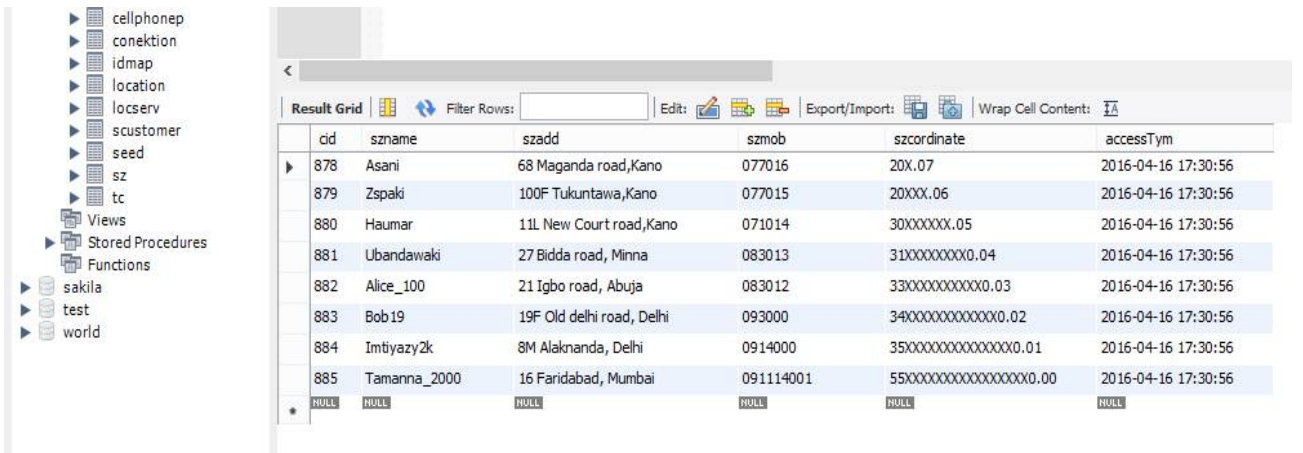
Figure 3 (a) shows clear text of user location information extracted while accessing LBS before applying the privacy preserving technique. In 3 (b), two columns **szmob** (device ID) and **szcordinate** (device cordinates) that were assumed to be very critical with regards to user's location information were transformed on arrival to the server. The last figure 3 (c) shows that the said two transformed-columns values were also replaced automatically with pre-defined auto-generated random values.



cid	szname	szadd	szmob	szcordinate	accessTym
866	Asani	68 Maganda, Kano	07035963016	20 14 36.50 -39 92 40.07	2016-04-16 14:17:54
867	Zspaki	100F Tukuntawa, Kano	07035963015	20 14 36.50 -39 92 40.06	2016-04-16 14:21:15
868	Haumar	11L New Court road,Kano	07035963014	30 14 36.50 -39 92 40.05	2016-04-16 14:44:47
869	Ubandawaki	27 Bidda road, Minna	08035963013	31 14 36.50 -39 92 40.04	2016-04-16 14:47:29
870	Alice_100	21 Igbo road, Abuja	08135963012	33 14 36.50 -39 92 40.03	2016-04-16 14:50:03
871	Bob19	19F Old Delhi road, Delhi	09035963000	34 14 36.50 -39 92 40.02	2016-04-16 14:53:13
872	Imtiyazyzk	8M Alaknanda, Delhi	09035974000	35 14 36.50 -39 92 40.01	2016-04-16 14:56:56
873	Tamanna_2000	16 Faridabad, Mumbai	09045974001	55 14 36.50 -39 92 40.00	2016-04-16 15:01:36
NULL	NULL	NULL	NULL	NULL	NULL

Figure 3 (a)

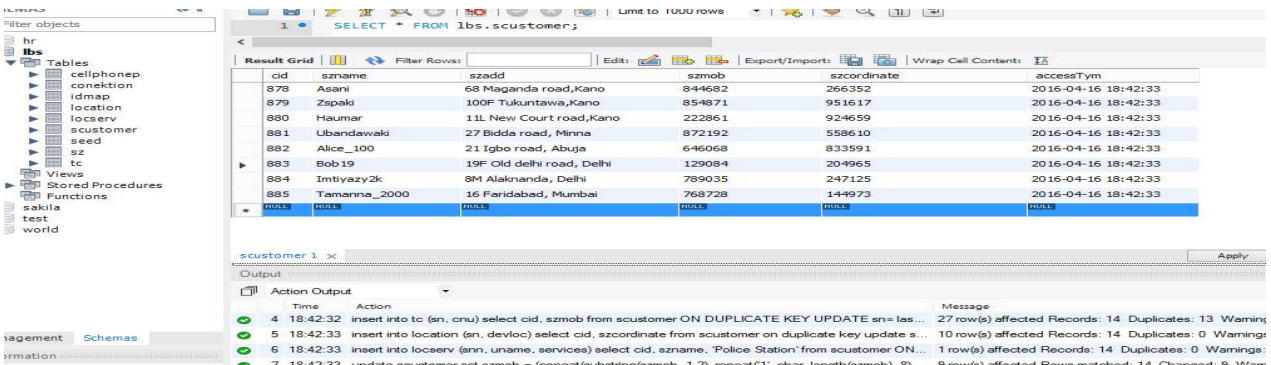
From the figure 3(a), we can see that all the supposed informations(**username, user address, cell phone number, current cordinate ponit at the time of access and the access time**) required for LBS user to enjoy one or more LBS services were extracted by the server but, not save as they are.



cid	szname	szadd	szmob	szcordinate	accessTym
878	Asani	68 Maganda road,Kano	077016	20X.07	2016-04-16 17:30:56
879	Zspaki	100F Tukuntawa,Kano	077015	20XXX.06	2016-04-16 17:30:56
880	Haumar	11L New Court road,Kano	071014	30XXXXXXXX.05	2016-04-16 17:30:56
881	Ubandawaki	27 Bidda road, Minna	083013	31XXXXXXXXXX.04	2016-04-16 17:30:56
882	Alice_100	21 Igbo road, Abuja	083012	33XXXXXXXXXXXX.03	2016-04-16 17:30:56
883	Bob19	19F Old delhi road, Delhi	093000	34XXXXXXXXXXXX.02	2016-04-16 17:30:56
884	Imtiyazyzk	8M Alaknanda, Delhi	0914000	35XXXXXXXXXXXX.01	2016-04-16 17:30:56
885	Tamanna_2000	16 Faridabad, Mumbai	091114001	55XXXXXXXXXXXX.00	2016-04-16 17:30:56
NULL	NULL	NULL	NULL	NULL	NULL

Figure 3 (b)

From the figure 3(b) above, we can observed that the first level of privacy was applied to a column called (**szcordinate**) that tracks and record user current cordinates. Another column (**szmob**) that tracks user cell phone number was also disguise by removing some digits and replacing them with predefined digits.



cid	szname	szadd	szmob	szcordinate	accessTym
878	Asani	68 Maganda road,Kano	844682	266352	2016-04-16 18:42:33
879	Zspaki	100F Tukuntawa,Kano	854871	951617	2016-04-16 18:42:33
880	Haumar	11L New Court road,Kano	222861	924659	2016-04-16 18:42:33
881	Ubandawaki	27 Bidda road, Minna	872192	558610	2016-04-16 18:42:33
882	Alice_100	21 Igbo road, Abuja	646068	833591	2016-04-16 18:42:33
883	Bob19	19F Old delhi road, Delhi	129084	204965	2016-04-16 18:42:33
884	Imtiyazyzk	8M Alaknanda, Delhi	789035	247125	2016-04-16 18:42:33
885	Tamanna_2000	16 Faridabad, Mumbai	768728	144973	2016-04-16 18:42:33
NULL	NULL	NULL	NULL	NULL	NULL

Action Output

Time	Action	Message
4 18:42:32	insert into tc (sn, cnu) select cid, szmob from scustomer ON DUPLICATE KEY UPDATE sn= las...	27 row(s) affected Records: 14 Duplicates: 13 Warnings: 0
5 18:42:33	insert into location (sn, devloc) select cid, szcordinate from scustomer on duplicate key update s...	10 row(s) affected Records: 14 Duplicates: 0 Warnings: 0
6 18:42:33	insert into locserv (sn, uname, services) select cid, szname, 'Police Station' from scustomer ON...	1 row(s) affected Records: 14 Duplicates: 0 Warnings: 0
7 18:42:33	update scustomer set szmob = (sn, devloc) from tc, location on (sn, devloc) = (sn, devloc) ON...	8 row(s) affected Records: 14 Changed: 8 Warnings: 0

Figure 3 (c)

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

In the figure 3(c), second level of privacy was applied to columns **szmob** and **szcordinate** respectively. In these two columns, replacement algorithm concept was used with pre-generated unique random numbers. These values in the said columns is what the server will store against each user location informations.

VI. CONCLUSION

We are now aware of the threat location information poses to every mobile phone user irrespective of whether he makes or receives call. Ideally, service providers are trustworthy; then who breaks into their server? Who will infer our information for economic gain? Can we trust them? LBS apps permeate into our daily life activities and we are unaware of the location and locating systems interacting with our cell phones. It is necessary to provide a privacy upon what our devices transmit in a pervasive environment.

REFERENCES

- [1] Coitlin D. Cottrill, "Location Privacy: Who Protect?," URISA Journal, vol. Volume 23, no. Issue 2, pp. 49-59, 2011.
- [2] Laurie Thomas Lee, "Location-Based Communication Systems A Look at Intelligent Networking and Privacy Concerns," Global Media Journal, vol. Volume 11, no. Issue 19, pp. 1-11, 2011.
- [3] Amit Kumar Tyagi and N. Sreenath, "A Comparative Study on Privacy Preserving Techniques for Location Based Services," British Journal of Mathematics & Computer Science, pp. pp1-25, 2015.
- [4] E. Gokulakannan and K. Venkatachalapathy, "A Survey on Preserving Privacy Towards Location Proof," Asian Journal of Information Science and Technology, vol. 1, no. 2, pp. 10-14, 2013.
- [5] C. Yu, B. Jie, Wie-Shinuku and H. Juin-Long, "Cache Management Techniques For Privacy Preserving Location-Based Services," In Proceedings of the 2nd International Workshop on Privacy-Aware Location-based Mobile Services (PALMS 2008), in conjunction with the 9th International Conference on Mobile Data Management (MDM), Beijing, China, pp. 88-93, 2008.
- [6] S. Leon, S.Y. Phillip and W. Ouri, "Mobile Systems Location Privacy: "Mobipro" A Robust K Anonymous System," in 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications, 2010.
- [7] K. Pantea, M. Norlia, Z. Nasriah and S.I. Muhammad, "E-Torch: A Mobile Commerce Location-Based Promotion System," The International Technology Management Review, vol. 3, no. 3, pp. 140-159, 2013.
- [8] H. Urs, "Hiding Location Information From Location-Based Services," in 2007 International Conference on Mobile Data Management, Mannheim, 2007
- [9] Rohan J. Patil, Prof. K.K. Joshi and Prof. Sowmiya Raksha, "Analysis On Preserving Location Privacy," International Journal Of Advance Research In Computer Science And Software Engineering, vol. 3, no. 3, pp. 562-566, March 2015.
- [10] M.I. Paraminik, M.A.F.M. Rashidul Hasan, B.K. Karmaker and Tosaddek Alom, "An Art Of Location Privacy On Social Media," International Journal Of Science & Engineering Research, vol. Volume 5, no. Issue 12, pp. pp 1115-1122, 2014.
- [11] Hemlata Jadhav, Nitish Dhotre and S.G. Shaikh, "Preserving Location Privacy in Geosocial Application," Global Journal of Engineering Sciences and Researches, pp. 13-16, March 2015.
- [12] Reshmi K.U and Suja M.S, "A Survey On Preserving State Of Location Privacy In Geo-Social Application," International Journal Of Innovative Research in Computer and Communication Engineering, vol. 3, no. 1, pp. 328-333, January 2015.
- [13] Langheinrich, "Principles of Privacy-Aware Ubiquitous System," in UbiComp '01 Proceedings of the 3rd international conference on Ubiquitous Computing, London, pp. 273-291, 2001.
- [14] D.N. Mohammed, "A Novel Authentication Mechanism Protecting Users' Privacy in Pervasive Systems," IAJIT, pp. 1-10, October 2013.
- [15] Jafari, Mtenzi, O'Driscoll, Fitzpatrick and O'Shea, "Measuring Privacy in Ubiquitous Computing," International Journal of Digital Society (IJDS), Volume 2, Issue 3, September 2011, vol. Volume 2, no. Issue 3, pp. 547-550, September 2011.
- [16] Mahesh Kadibagil and H.S. Guruprasad, "Position Detection and Tracking System," International Journal of Computer Science and Information Technology & Security, vol. 4, pp. 67-73, June 2014.
- [17] Swapnil Ramesh Jadhv and Rajesh Nandkumar Phursule, "A Survey on Privacy Preserving and Content Protecting Location Based Queries," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 2, no. 11, pp. 3548-3551, November 2014.
- [18] A.R.Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Security and Privacy, vol. 2, pp. 46-55, 2003.
- [19] Jacob and Preetha, "Vertical Fragmentation Of Location Information To Enable Location Privacy in Pervasive Computing," International Journal of Ambient Systems and Applications, vol. Vol.1, no. Issue 1, pp. pp. 11-21, 2013, March 2013.
- [20] W.Y. Sven, "Forensics and GSM Mobile Telephone System," International Journal of Digital Evidence, vol. 2, no. 1, pp. 1-17, 2003.
- [21] K. Pantea, M. Norlia, S.I. Muhammad and Z. Nasriah, "E-Torch: A Mobile Commerce Location-based Promotion System," vol. 3, no. 3, pp. 140-159, 2013.
- [22] Janice Y., Tsai, K.G. Patrick, C.F. Lorrie and S. Noman, "Location-Sharing Technologies: Privacy Risks and Control," Journal of Law & Policy for the Information Society, pp. 1-26, 2010.
- [23] K.B. Priya Iyer and Dr. V. Shanthy, "Privacy Aware Spatial Queries," IJCSE, vol. 3, no. 4, pp. 564-573, 2012.
- [24] Reshmi K.U and Suja M.S, "A Survey On Preserving State Of Location Privacy In Geo-Social Application," International Journal Of Innovative Research in Computer and Communication Engineering, vol. 3, no. 1, pp. 328-333, January 2015.
- [25] Amit Kumar Tyagi and N. Sreenath, "A Comparative Study on Privacy Preserving Techniques for Location Based Services," British Journal of Mathematics & Computer Science, pp. pp1-25, 2015.
- [26] H. Kido, Y. Yutaka and S. Tetsuji, "Protection Of Location Privacy Using Dummies For Location-Based Services," in 21st International

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Conference On IEEE, pp. 1248, 2005.

- [27] Jiang T., Wang HJ. and Hu YC., "Mobile Systems, Applications and Services," in 5th International Conference on Mobile Systems, Applications and Services, Puerto Rico, pp. 246-257, 2007.
- [28] Huang L., Matsura K., Yamane H. and Sezaki K., "Towards Modeling Wireless Location Privacy," in Workshop on Privacy Enhancing Technologies, pp. 59-77 2005.
- [29] R. Rusyaizila , Z. Nasriah and S. Putra, "Privacy Issues in Pervasive Healthcare Monitoring System: A Review," International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:4, No:12, pp 1913-1919, 2010.
- [30] Sabu M. Thampi, "Information Hiding Techniques: A Tutorial Review", ISTE-STTP on Network Security & Cryptography, pp. 1-18, LBSCE 2004.
- [31] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "Information Hiding- A Survey," Proceeding of the IEEE, special issue on protection of multimedia content, vol. 87, no. 7, pp. 1062-1078, July 1999.
- [32] H.J.W Van Heerde and N. Anciaux, "Data Degradation To Enhance Privacy For The Ambient Intelligence," RT-CTIT Report, Centre for Telematics and Information Technology, University of Twente, pp. 1-8, 2006.
- [33] S. Reza, P.P. Theodorakopoulos, K. Ehsan and H. Jean-Pierre, "Hiding in the Mobile Crowd: Location Privacy Through Collaboration," Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 500-509, 2014.
- [34] M. Gruteser and Grunwald D., "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in First International Conference on Mobile Systems, Application and Services (Mobi Sys), pp. 31-42, 2003.
- [35] Tan, Lin and Mouratidis, "Spatial Cloaking Revisited: Distinguishing Information Leakage from Anonymity," 11th International Symposium on Advances in Spatial and Temporal Databases, pp. 117-134, 2009.
- [36] V. Ciriani, S. Foresti, P. Samarati and S. De Capitani di Vimercati, "K-Anonymity," Secure Data Management in Decentralized Systems, pp. 323-353, 2007.
- [37] J.Al-Muhtadi, R. Campbell, A. Kapadia, D. Mickunas and S.Yi, "Routing Through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments", in International Conference of Distributed Computing Systems, Vienna, Austria, pp. 65-74, 2002.
- [38] Cheng, Zhang and Tan, "Protection Of Privacy in Pervasive Computing Environment," in International Conference on Information Technology: Coding and Computing, pp. 242-247, 2005.
- [39] Z. Xu and Y.B Hae, "Location Positioning And Privacy Preservation Methods in Location-based Services," International Journal Of Security And Its Application, vol. Volume 9, no. Issue 4, pp. 41-52, 2015.
- [40] S. Latanya, "K-Anonymity Privacy Protection Using Generalization and Suppression," International Journal on Uncertainty, Fuzziness and Knowledge-based Systems
vol. Volume 10, no. Issue 5, pp. 571-588, May 2002.
- [41] B. Hoh and M. Gruteser, "'Protecting Location Privacy Through Path Confusion'," in 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, pp. 194-205 2005.