International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 212-219 www.ijaem.net ISSN: 2395-5252

# Sheltered Confidentiality on Spots for Mobile Based Social Application

Mrs.K.Devibala [1], Mrs.S.Joney Babayal[2], Dr.K.A.BalaSubramanian[3]
[1,2,3] *Assistant Professor, Department.of Computer Science, Ayya Nadar Janaki Ammal College,Sivakasi,India.*
*Correspnding Author : Mrs.K.Devibala*

Date of Submission: 01-07-2024 Date of Acceptance: 10-07-2024

**ABSTRACT: —** Using geosocial appliance the inhabitants interact with their ambiance, for sharing the information. For eg., Four square, Whatsapp. Without passable seclusion protection, however this interaction can be tainted. In this paper we introduce S&D and AES algorithm to defense the spot and information. Here we are applying co-ordinate renovation, S2EI and I2ED to all spot data. The same course of action take place on both sides. This allows all spot queries to be assess appropriately by the server. But our seclusion mechanism guarantee that server are unable to see or infer the authentic spot data, from the transformed data or from the data access. We illustrate that S&D provides seclusion even against powerful antagonist form. Making it suitable for mobile gadget.

## I. INTRODUCTION:

With billions in downloads and yearly profits, smart handset appliances on hand by Apple iTunes and Android are quickly becoming the prevailing computing platform for today's addict appliances. Within these advertises, a innovative sign of geo-social appliances are fully exploiting GPS spot services to provide a "social" interface to the physical world. Examples of popular societal relevances include social assignation [1], confined friend recommendations for dining and shopping [2], [3], as well as mutual network services and sports event [4], [5]. The volatile popularity of mobile societal networks such as SCVNGR [6] and Four Square (3 million new users in 1 year) likely indicate that in the prospect, societal recommendations will be our crucial source of information about our backdrop.

Unfortunately, this new functionality comes with significantly enlarged risks to delicate . Geo-social appliances operate on fine-grain, time-stamped spot information. For current services with minimal mechanisms, this data can be used to infer a user's detailed activities, or to track and forecast the user's day by day movements. In fact, there are numerous real world examples where the illicit use of spot information has been tainted for economic gain [7], physical persecution [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 user's spot, such spot data was already used by thieves to plan home invasions [10]. Clearly, itinerant societal networks of tomorrow require stronger seclusion properties than the open to- all policies available today.

Existing systems have mainly taken three approaches to improving user seclusion in geo-social systems: (a) introducing ambiguity or blunder into spot data [11], [12], [13], (b) relying on trusted servers or intermediaries to apply anonymization to user identities and private data [14], [12], [15], and (c) relying on heavy-weight cryptographic or private information retrieval (PIR) techniques [16], [17], [18], [19]. Nothing of them, however, have verified booming on recent appliance policies. Techniques using the first approach fall short because they require both users and appliance providers to introduce ambiguity into their data, which degrades the quality of appliance results revisited to the abuser. In this loom, there is a elemental employment off between the amount of blunder introduced into the time or spot domain, and the amount of seclusion granted to the user. Users dislike the loss of precision in results, and appliance providers have a natural disincentive to hide user data from themselves, which condenses their ability to monetize the data. The subsequent approach relies on the trusted proxies or servers in the system to protect user seclusion. This is a risky assumption, since private data can be exposed by either software bugs and configuration blunders at the trusted servers or by malicious administrators. At last, relying on heavy-weight cryptographic mechanisms to obtain provable seclusion guarantees are too expensive to deploy on mobile devices [20], [21], and even on the servers

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 212-219 www.ijaem.net ISSN: 2395-5252

in answering queries such as nearest-neighbor and range queries.

The challenge, then, is to design mechanisms that efficiently protect user seclusion without sacrificing the precision of the structure, or construction tough hypothesis about the security or trustworthiness of the appliance servers. More specifically, we target geo-social appliances, and assume that servers (and any intermediaries) can be compromised and therefore are entrusted. To limit misuse, our goal is to limit accessibility of spot information from global visibility to a user's societal circle. We identify two main types of queries necessary to support the functionality of these geo-social appliances: point queries and nearest-neighbor (kNN) queries. Point queries query for spot data at a exacting point, whereas kNN queries query for k adjacent data around a given spot coordinate (or up to a assured radius). Our target is to support both query types in an proficient fashion, suitable for today's mobile campaign.

To address this challenge, in this paper, we propose S&D (short for Spot and Data), a novel approach to achieving user seclusion while maintaining full accuracy in spot-based societal appliances (SBSAs from here on). Our imminent is that many examines do not need to resolve distance-based queries among arbitrary pairs of users, but only among contacts fascinated in each other's spot and data. Thus, we can partition spot data based on users' societal groups, and then perform renovations on the spot coordinates before storing them on entrusted servers. A user knows the renovation keys of all her contacts allowing her to renovate her query into the virtual coordinate system that her contacts use. Our coordinate renovations defend space metrics, permitting an appliance server to perform both point and nearest-neighbor queries correctly on transformed data. And encryption on the spot and data is processed. However, the encryption is secure, in that transformed values cannot be easily associated with real world spot excepting a secret, which is only available to the part of the societal group. Finally, renovations and encryption are proficient, in that they incur minimal overhead on the SBSAs. This makes the appliances built on S & D lightweight and suitable for running on today's mobile diplomacy

## II. CIRCUMSTANCES AND CONSTRAINTS

Here we demonstrate numerous circumstances we target in the situation of rising geo-social appliances that involve profound communication of users with their contacts. We use these circumstances to identify the key constraints of a geo-social spot seclusion preserving configuration.

### 2.1 Geo-social appliance circumstances

**Situation 1**:

Cadan & Dann are comrades they want to meet in a restaurant to share their moments.The cadan invite dann to restaurant by using SMS at this situation the invaders can assail the message.

**Situation 2:**

Candan is impinge on some critical problem, he want some money and he decided to claim help to his comrade.

The circumstances above, while fabricated, are not distant from Authenticity. Groupon and Living Societal are some example companies that are primary the blooming business of local actions. SCVNGR [6] offers similar examines as spot-based games. But none of these services provide any spot seclusion to users all the spot visited by the users are known to these services and to its administrators. Our goal is to build a method that caters to these circumstances and allows users to uncertainty for contacts' record based on spots, while protecting their spot and data seclusion. We want to support**:**

a) point uncertainty to uncertainty for record associated with a particular spot, b) circular series uncertainty to uncertainty for record coupled with all spots in a certain series (around the user), and c) Nearby-neighbor uncertainty to uncertainty for record associated with spots nearby to a given spot. Finally, while it is also useful to uncertainty for record that belongs to non-contacts in certain circumstances, we leave such additions for probable.

### 2.2 Method constraints

The intention circumstances more than carry out the following key constraints from an supreme spot-seclusion service.

• Sturdy spot seclusion: The servers practicing the data(and the proprietors of these servers) should not be able to discover the narration of spots that a abuser has visited.

• Spot and abuser unlink ability: The servers swarming the services should not be capable to connect if two confirmation belong to the same abuser or if a given confirmation belongs to a given user, or if a given confirmation communicates to a certain real-world position.

• Spot record seclusion: The servers should not be able to view the content of records stored at a spot.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 212-219 www.ijaem.net ISSN: 2395-5252

• Elasticity to support peak, spherical series, and adjacent-neighbor queries on spot record.
• Effectiveness in terms of division, bandwidth, and latency, to function on mobile diplomacy. The require for each of these constraints becomes more obvious when we describe the related work and their controls in more detail in the next segment. In our proposed system, S&D, we intend to achieve all these constraint.

## III. NARRATED EFFORTS.

**Preceding work on seclusion in spot based services (SBS) and geo-social services**:

In general SBS service the communication between friends can be easily identified even though the holder can change their spot. That the holder send a message with approximate spot [11],[12],[13],[14],[15]. But the intruder easily hack the communication by tracing the system. That this system provide seclusion due the technology development it can be abused. So the hacker break the system[23],[24],[25],[26].The other mechanism is that intruder change holders location frequently and data is not correctly exchanged at regular periods. So, the users communication is easily breaked. And they stole all information from holder.

That now a day GPS is used to set a latitude and longitude. The friends and unknown persons can easily trace the system and hack the communication and may attack the information holders. These kind of hacking can be solved by our S&D system. Here 3 step process is followed. In first, data transformation is done for latitude and longitude. Then the spot(latitude, longitude) is encrypted by symmetric key encryption .The third process is data is encrypted and pseudo random number is generated. That S&D provides more seclusion on the spot and data. So, the holder can easily communicate with their recommendation.

**In conviction servers**:

All the details of the holder can stored in the database. That the server is in conviction then the information can be hacked by the servers. There are many technique such as Persona and Adeona system used to trace the system. So, the untrusted server can hack yhe information of holders. To avoid this S&D provide the higher seclusion on the holder information. So, the malicious server cann't stole the information.

## IV. SYSTEM DESIGN:

Here we describe S&D in detiled.

### 4.1 Term and Attacks:

Terms: Spot co-ordinate refers to the holder's latitude and longitude. That GPS is used for dynamic generation of spot. Spot data refers to the information of the holder which is exchanged between their recommendations.

**Attack:**

The server is the only responsible for securing the dataand spot..But they become attacker in some scenario. Also some user may become an attacker.The intruder can easily access all the data stored on the servers , and can also monitor which user device is accessing which piece of information on the servers. Our goal is to preserve the spot and data seclusion of the user in mobile communication.

### 4.2 A Basic Design:

The term used in this design are spot co-ordinate and spot data. Malicious server and attacker break the spot and data seclusion of the users. To avoid this we proposed 3 step process. They are,1.Coordinate transformation 2.Coordinate Encryption and 3.Data Encryption. In Coordinate transformation we uses Rotation Angle($\theta_r$),secret Shift ($s_u$) , In co-ordinate encryption $symm_u$ is used to encrypt the spot.In data encryption AES(Advanced Encryption Standard) with block cipher is used.For example, The holder is(h) and their spot is (m,n) .The holder want to sent information to their friend with seclusion. So,the co-ordinate is transformed to (m',n').

### 4.3 Overview of S&D:

In S&D, we split the mapping between the spot and data into two pairs (ie) S2EI (Spot to encrypted index) I2ED (Index to encrypted data) In S2EI operation two server are used Proxy server & Index server. The co-ordinate value & information is sent to proxy server, Here the coordinate value is transformed. And transformed co-ordinate and data is send to the index server. The index server encrypt the co-ordinate value. In I2ED the data is encrypted .The encrypted coordinate value & data is sent to Data server, while transforming this the secret key is sent to the recipient via e-mail. Then the recipient decrypt the spot and data. Here encrypted data is represented as, (EN(d)), decrypted data is represented as (DE(d)) and encrypted spot is represented as (EN(s)),decrypted spot is represented as(DE(s));

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 212-219 www.ijaem.net ISSN: 2395-5252

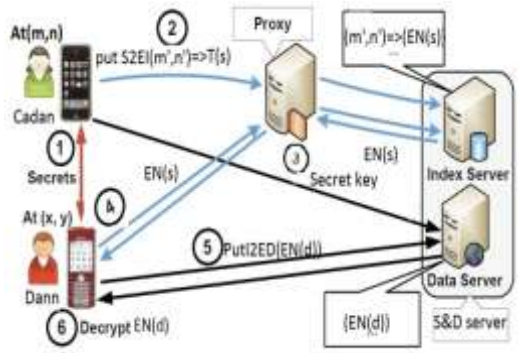


**Fig.1. Design of S&D:1) Cadan and Dann exchange their secrets. 2)The spot and data is sent to proxy. In proxy spot is transformed (S2EI(m',n'))=>T(s). 3)while senting the information to the recipient the holder send a secret key. 4)By using decryption original spot is retrived. 5)proxy sent transformed spot to index server. here spot is encrypted then data is encrypted by the data serverI2ED(EN(d)). 6)By using decryption and secret key the original data is retrived.**

The output from the proxy server is T(s) here T represents transformation .In S2EI (EN(s)) is stored and I2ED(EN(d)) is stroed. That in index server encrypted spot is stored and in data server encrypted data is stored. Then it is exchanged with their recommendation.

### 4.4 Seclusion Preserving Data Storage

**Storing S2EI on the index server**:

Here the coordinate transformation is processed by the equation

$(m',n') <- (\cos\theta_r m - \sin\theta_r n + s_u, \sin\theta_r m + \cos\theta_r n + s_u)$

m,n is world co-ordinates

m',n' virtual co-ordinates

$\theta_r$ secret rotation angles$_u$secret shift.

The symmetric key is used to perform the coordinate encryption.That is ($E_{symmu}(k)$).The user then stores this S2EI, [(m' ,n'), $E_{symmu}(k)$]

**Storing I2ED on the data server:**

Here the data is encrypted by the use of symmetric key encryption using AES algorithm with block cipher. Here the user stores this I2ED ($E_{symm}$ (m,data))

Both index server and data server is commonly known as S&D server(Spot and Data server)Then the encrypted message and data is send to the recipient. By using the secret key they decrypt the message and spot. Due to the co-ordinate transformation, the index server does not see the real world coordinate. And also the co-ordinate encryption and data encryption the malicious cannot see the original coordinate and original data. With adequate secret key the data and coordinate cannot be easily retrieved. These significantly raise the bar for attacks.

### 4.5 Seclusion Preserving Data Retrieval

Here the information about all holders can be stored in the WAMP server. In S&D the data retrieval place a major part. Because without correct coding the value cannot be retrived. Only the recipient know the secret key the information can be retrieved and the intruder cannot access the data. When sending information to friends the virtual spot is created. If the original spot is(m,n) then the virtual part is (m',n').The co=ordinate values are $(a_1, b_1)(a_2,b_2)$ and $(a'_1,b'_1)(a'_2,b'_2)$ then the distance between two spot is calculated by distance formula.

The S&D has mainly two parts: First, The transformed and encrypted value must be secure. Else the intruder easily breakup the seclusion. Second, The recipient and holder must know the secret key and secret message. Else they cannot access the data. Due to the data secret key and secret message generation the S&D is high efficient.

**Seclusion while questioning the index server and Efficiency**

Due to the spot and Data encryption the information is high secure. The attacker and malicious server cannot access the data. Because If the intruder attack the proxy they do not find spot because the co-ordinate is changed. Else if the index the spot is encrypted. Else The data is encrypted in the data server. So the intruder cannot find any information. That the S&D provide high seclusion on the information.

Here many user can interact with their surroundings effectively. The holder can easily create an account for himself. The user, proxy and index can open their account only they knows the ID and Password. Due to the secret key and secret message generation the information has high seclusion and holder can easily interact with their recommendations effectively.

**Easy to retrieve and supporting all user**

The spot and data can be easily retrieved from the server by using a e-mail. That while transferring message to the friends the secret and secret message is send to recipient e-mail. So, by using that the information can be retieved. It supports all user that they were in any country .Also the circlular, nearest-neighor can use this for efficient communication.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 212-219 www.ijaem.net ISSN: 2395-5252

## V. SECLUSION SCRUTINY

### 5.1 Inkling Behind seclusion in S&D

Here we describe the inkling behind S&D's seclusion, and how it meets all of our constraints.

The records stored on both servers do not expose any in sequence about their spots to the invader. The S2EIs on the index server contain altered match ups and the records on the record server are all encrypted. As a result, an invader access the record on the servers cannot de-innominize the record to co-relate users with their spots entree. The invader can monitor both servers, the indices are stored and encrypted in the index server. Only the user know how to decrypt the encrypted records. Without the secret keys, the invader cannot link these records. Next the I2EDs are encrypted the users entrée them through indices. The record server can link together the indices entreed by the same user. Finally, the users store and regain S2EI on the index server via proxies.

### 5.2 Seclusion During Spot Record Entrée inject certainity novel efficiency

Here we present a theoretical scrutiny of the seclusion properties during record access in S&D. When a user entrees her friends' records by altering her own spot to different points in the altered space and transfer them in a query, a malevolent index server find out the different, altered match ups that map to the same, real world spot(which is the user's recent spot). The problem is whether an invader could use this in sequence to receive the user's real-world spot. Here, we discuss the primary restraints we need to protect in S&D to prevent the server from ensuing in such assails.

Restraints in querying the index server.

Assume first that the users directly entree the index server, without any proxies. Each user has a furtive angle, θ, and a furtive shift, b, to alter her spot matchup. Suppose a user has s friends and she issues t location questions. In each of the locations,($p_r$, $q_r$) the user seeks for $t_r$ ($t_r \leq t, 1 \leq r \leq s$) comrades in sequence. Let us presume that all comrade in sequence is questioned at all spots, and let us also presume the bad case circumstance where the comrade's altered points are questioned in the same array. Believe that the index server is malevolent and sees the altered match up of the user's comrades( $p_{ur}$ , $q_{ur}$ ) in all quries. The invader then construct ($2t_1+2t_2+\ldots+2t_s$) equations as follows(2 equations for each appeal comrade at one spot)in order to solve 2s unknown real match up($p_r$,$q_r$) and 2t unknown comrade furtive($\theta_u$ ,$b_u$),where $1 \leq r \leq s, 1 \leq u \leq t$.

$$\begin{aligned} \cos\theta_u .p_1 - \sin\theta_u .q_1 + b_u &= p_{i1} \\ \sin\theta_u .p_1 + \cos\theta_u .q_1 + b_u &= q_{i1} \quad \ldots \quad = \ldots \\ \cos\theta_u .p_s - \sin\theta_u .q_s + b_u &= p_{is} \\ \sin\theta_u .p_s + \cos\theta_u .q_s + b_u &= q_{is} \end{aligned} \qquad (1)$$

The sum of unknown erratic is 2s+2t.For the invader to crack all the unknowns, the following must hold:

$2t_1+2t_2+\ldots 2t_s \geq 2s+2t$ (2)

$\Rightarrow t_1+t_2+\ldots+t_s \geq s+t$ (3)

To protect the user's spots and comrade's furtive is being surmise by the invader, the reverse formula is:

$t_1+t_2+\ldots+t_m < s+t$ (4)

If the users query all t comrades record at each spot,$t_r = t$,a stronger version of formula(4) hold:

$st < s + t$

To satisfy formula(5),there are two special cases.

s=1,the altered match ups of comrades should be only observed in one spot.

t=1,the user is bounded to entrée only one,diverse comrades records at each of s spot.

For the general crates of $s > 1, t > 1$,we choose to utilize the first crate for our propose, since we do not desire to bound users as in the second crate.

Thus, we have verified that the unlinkabilty of doubts due to proxies protects user's seclusion in S&D.

### 5.3 Other assails and securities

We now discuss about other possible assails the server can perform, in addition to the assails described before, and our suggested solutions to region sour these assails.

**Query bonding assails by the index server.**

The index server effort to bond the quries from the same user using the query "fingerprints". For occurrence, the server guess are belong to the same user, but it impossible to have many user to use the same proxy. Privilege we extends of adding noise to the request. The noise that are added varies in query and it is difficult to the server to perform such assails.

**Fingerprinting using cookies and confine based assails.**

We presume that the proxies scour the outgoing connections using such tools Privoxy[46] which is used to remove the user in sequence, this is common in all protecting systems but it does not work in S&D. If the users tie to the data server ,the user's spots can only be find out by

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 212-219 www.ijaem.net ISSN: 2395-5252

using their IPs. The spot from confine equipment is at the coarse of tens of mile[47],to protect these assails the latest intend means help us reducing the confine correctness and conquer these assails.

**Instance assails by the index server and assails due to wrap or conciliation user mechanism and comrades**.

The index server might bond different request that are arrive at the server to the same user. For occurrence ,the server say that the request for I2ED belong to the same user. Priviliged we can influence preceding work on spot seclusion here[49],[11],[12],[13],[22].We can sense these assails by using some system such as setback the request arbitrarly to the server etc. An invader access to user's furtive is attain by the concillation. This is a natural problem shared by other social schemes that have relied on comrade's record to the server[41],[39],[40],[37].First, the user can only spread her comrade's record to the server. By achieving network ample evident for an invader will need huge amount of user which is hard. Second to reduce the distortion of the assail we use the attributed based encryption (ABE)[50]which is similar to Persona[37].The invaders wiil get many comrades and finally the user easily retract the keys of a comrade to re-request the keys and thus it be "snip" their only to the trusted comrade.

**Assails using peripheral in sequence**

The invaders can do several assails on the user which they are aimed by using the in sequence about them..For occurrence, Dann is an worker of the restaurant he might know the address of the candan. Knowing two spots of candan and the time transom when of these spots alteration are stored on the server. Dann might conspire with the server to try to findout candan's furtives. While securing against all such assails based on the outside in sequence is dispute. These assails are difficult against S&D. First, this assail can work only on those users whose in sequence is already known. Second, against timing assails can major and increase the time transom and the assails has to process. Third, the invader keep monitoring the in sequence which the user send. So, to break these (θ,b) are used, the invader still needs to bond upcoming request to that user. The attacker easily connect the points in the virtual co-ordinate and easily trace our information. That, if the virtual co-ordinate is not transformed then the attacker can easily hack our information. Also, the attacker make a denied of service while communication. That, when the holder sends information do their recommendations the intruder make a denied of service on the transformation. So, the recipient connection will disconnected and the hacker can easily hack the messages.

But our S&D eliminate these kind of operation and it provide seclusion to the data and spot.

## VI. EVALUATION:

**6.1.Setup:**

We implemented S&D in java. The WAMP server used as a database to store all the user information. When performing the operation the result is stored in WAMP server. That it very secure ,and we can use it any operating system. It is fast to access and easy to perform the operation.

**Experimental setup:**

Normally the database server has no security. But our S&D provide the seclusion on the spot and data. That the spot provide seclusion is S2EI and I2ED.Here AES provide yhe encryption and decryption. For making the speed, block cipher is used.

**6.2 Experimental results:**

**High performance:**

The performance of spot & data seclusion is high due to proxy and index server.

**Scalability**:

That large data can be stored and S&D provide the communication over n number of peoples.

**High seclusion**:

Due to the co-ordinate transformation, co-ordinate encryption & data encryption. The S&D provide high seclusion on user communication. Also, the people can interact with the recipient who are in high distance.

**Application:**

S&D is mainly useful to provide the secured communication between the user and recipient with high seclusion. In smart phones it is implemented and used.

## VII. CONCLUSION:

Our new S&D provide novel approach to mobile communications. This paper describes the new S&D approach, the S&D provides spot and data seclusion for the user without instilling errors into the system.

The S&D takes a narrative approach to provide spot and data seclusion, while maintaining the overall system effectively. Here the user effectively altered all their spots and data shared with recipient and encrypt all their spot and data records stored on the server by using the furtive keys. Only the comrade's who have the correct keys can query and decrypt the user's record.

Our paper only deals with static communication and geo-social based queries only execute in future, We implement the dynamic communication.

## 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.
[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 privacy ware 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 location based 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]. R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: An online social network with user defined privacy," in Proc. of SIGCOMM, 2009.
[28]. A. Mislove, K. Gummadi, and P. Druschel, "Exploiting social networks for internet search," in Proc. of HotNets, 2006.
[29]. A. Mislove, A. Post, P. Druschel, and K. Gummadi, "Ostra: Leveraging trust to

thwart unwanted communication," in Proc. of NSDI, 2008.

[30]. T. Isdal, M. Piatek, A. Krishnamurthy, and T. Anderson, "Privacy preserving p2p data sharing with oneswarm," in SIGCOMM, 2010.

[31]. J. Manweiler, R. Scudellari, and L. P. Cox, "Smile: Encounter-based trust for mobile social services," in Proc. of CCS, 2009.

[32]. Krishna P.N.Puttaswamy,Shiyuan Wang, Troy Steinbauer,Divyakant Agarwal,Amr EI Abbadi,Christopher Kruegel and Ben Y.Zhao Department of Computer Science,UC Santa Barbara