An Art of Location Privacy on Social Media

M. I. Pramanik*, M. A. F. M. Rashidul Hasan**, B. K. Karmaker***, Tosaddek Alom****

Abstract— Now a days location based services are very much popular application in social media through mobile devices such as smartphones, PDAs, and like so. But at the same time location privacy is a major concern for social media user and so protecting personal location information is a new challenge for the social media service provider. Addressing this challenge requires a mechanism that lets users automate control of their location information, services and security. In this paper, we argue that service provider should adapt an approach where location of user will be encrypted at first and then cipher data will be stored and processed for services. In this paper dynamic pseudonyms are used by the clients to protect source location privacy from each other and also proposed an algorithm for the service provider to do that job. Our system can be implemented with the existing network infrastructure easily with little computation and power cost. This approach significantly improves user location privacy, not only this but also it is flexible enough to support a wide variety of location-based applications used today. We confident that the proposed approach provides an applied alternative design for location based services and securities in social media.

Index terms— Privacy, Social Media, Cryptography, Location, and Pseudonym

1 Introduction

Location based social applications are adopted widely in our society due to the availability of the internet enabled smartphones. For empowering users with the knowledge of their locality, which significantly improves user efficiency in a variety of contexts ranging from work and personal life to health and travels, these applications are providing significant roles. Social media users are enjoying enormous facilities by tracing the location of their friends such as users are enabled to meet with friends with surrounding([1],[2]), select good healthcare centers based on reputation, get suitable restaurants based on services and qualities [3], find proper routes based on traffic information, and like so many positive purposes. And so location based social applications are rising day after day which are exceeded several millions [4]. But at the same time location privacy is a major concern for social media user and so protecting personal location information is a new challenge for service provider. For providing the location privacy of a user we will use *networked-assisted* approach [5], location determination occurs in the network with the user device's active participation. We reviewed that the location based services are vulnerable as users are sent their locations to the service provider in plain text form and so it can easily leak from server due to operator errors, due to software bugs, or due to active attacks. In our approach we proposed to send cipher text of user's location to the server where location will be encrypted by the application functionality of client smartphones. In this paper, we proposed an algorithm with architectural design and protocol that provides a low cost, and pragmatically deployable alternative to the existing approach while providing strong user location privacy.

- * *Department of Information System, City University of Hong Kong, HongKong*
- ** *Department of Information and Communication Engineering, University of Rajshahi, Bangladesh*
- *** *Department of Electronics and Communication Engineering, JKKNU, Bangladesh*
- **** *Department of Computer Science and Engineering, Begum Rokeya University, Rangpur, Bangladesh*

2 Location-Based Social Networks

Dodgeball2 is one of the first LSN service that relies heavily on SMS to allow users to "check in" their current location and to find their friends and friends-of-friends within 10 block radius [6]. But Loopt3 leverages GPS and other signal triangulation technologies to automatically sense device location, without requiring manual location updates. In the 2005 brightkite4 was introduced to the market for LSN service that allows users to share their location, to post notes, and to upload photos through a number of interfaces, including Web, SMS, and Email. Moreover, different companies are released some native client applications on Apple iphone and are thinking to include with the Google Android phones. These native client applications, like Loopt clients, leverage GPS and other on device technologies for automatic location sensing, though still requiring users to hit "check in" button to update location. Brightkite allows users to define their friends and subscribe to their *activity streams*, including locations they checked in, their posted notes, and their uploaded photos. Another location based social network is Foursquare which is a relatively new LSN. Using Foursquare is like playing a game. The users make check-ins at venues, and they are then awarded points and sometimes "badges." By making more check-ins, the user can earn badges like "Newbie," "Adventurer, "Explorer," or "Superstar." If a user has more check-in days at a venue than anyone else in the past 60 days, she becomes the "Mayor" of that venue. Foursquare has partnered with many bars, cafes, and restaurants to reward the Mayor with free drinks or other specials. The strategy of giving interesting badges and rewarding with specials encourages users to stick to the service and make frequent check-ins. Foursquare has grown rapidly recently, and has obtained more than 1.7 million total users and signs up about 100,000 new users per week. Like

these two LSNs a good number of location based service are introduced to the online market and millions of user are already included those applications. Right now all service providers are not ready to preserve full privacy of a user due to the big data processing, which is also a cause of big concern for user.

3 System Goal and Threat Model

We will describe the Goal of our design and threat in this section.

3.1 System Goals

We aim to achieve the following key goals in our design.(a) Our design should *preserve location privacy* of the users while the users use the applications. To preserve privacy, all data shared in our design is encrypted, and only the user's friends will be able to decrypt a user's (location) data.(b) Our design should *preserve data privacy* of the users while the users upload it to any social media. Our new system will prohibit a user from uploading others private multimedia data to the social media. c) Our design should be *portable and low infrastructure cost* which means for all location based service it can operate and the resource cost on this system is quite low, and the fact that the applications only need to pay for only the resources they use, this provides a low-cost alternative. (d) We aim to keep the design *simple and practical* to spur its adaption. We leverage widely-used symmetric cryptography to keep the overhead on the social media low. So for gaining these four goals in this paper we present a new infrastructure of a social media provider and also design some algorithms for operating different sections of the proposed design.

3.2 Threat Model

With considering every protection provided by the proposed system, we assume a strong attacker model in this paper. In our system all attackers are reactive and inner which can work in the whole range of the network. However, this is a very strong assumption about the attacker's capability in our practice. During our privacy analysis, in Section 5(V), we also consider an even stronger attacker with power to compromise and monitor the server, checker, verifier for extended period of time, present our solutions against this attacker and the associated privacy vs. performance tradeoffs. Moreover let the adversary is able to compromise or control individual user and then communicate with others to explore private information and, the adversary can monitor, eavesdrop and analyze all the traffic in the whole range of the network. In practice, the adversary can thus be a rogue individual, a set of malicious users, or may even deploy its own arrangement by placing eavesdropping devices in the network.

Load_info (Id,value,location)	*load some data about user*
GET_INFO (CYPHER,KEY)	*Access media through reliable way*

Hence, the problem we tackle in this paper consists of collecting a set of different sections where we will store user's private information and ensure the separation of privacy knowledge. Here an attacker cannot reveal user privacy without integrating data of all sections.

4 System Architecture

We are presenting a design of a system for enforcing location privacy; we next describe the architecture of a system that ensures location privacy. We have tried to develop a system that can be used together with existing location-based services (LBS). We did not want our privacy module to interfere with the operations of existing services. Thus, one can think of our module as implementing location privacy as a service layer. This layer is implemented as a client server architecture model. The client module permits the users to achieve their privacy policies through the *client side User Interface*. Any users post their data to the social media form their device after encryption by using public key. This encryption has a major role for providing privacy on the social media.

Our architecture is presented in Figure 1, which consists of three major components, namely, *Location Provider*, *Client Devices* and *Service Provider*. Moreover, the server module consists of four major components, namely, *APIs*, Server, *Root CA*, and Verifier.

4.1 Location Provider

Location Provider locates the physical position of the user. It has GPS receiver which is responsible for location request from the client devices and location finder which computes the actual position of user with the help of its own technology. The results computed are passed back on to the querying client device.

4.2 Client Devices

Client devices include cellular phones, Computers, PDAs and other devices with GPS capabilities. Client devices find out its location by using GPS module. Clients are sent their location update to the trusted service providers, who are very much responsible for preserving privacy, such as location privacy, data privacy, for the client. Client devices communicate with the service provider by using *client side user interface* module. It sends location updates and receives event notifications from the service providers. In addition to these modules, our approach needs a *client side interface module* to allow users to manage their own privacy. In our architecture client side interface module in the client devices allows user to communicate with APIs in the server where both modules have strong contribution on privacy. In the client side interface module an encrypted data frame which includes (id,value,location) or (id,value,location,status) will send to the API module of the server.

4.3 Service Provider

Service provider consist of the major components: 1) APIs, 2) Server, 3) Root CA, and 4) Verifier.

1) APIs*: The storage server APIs and their functions:*

Table:1 Storage server APIs and their function

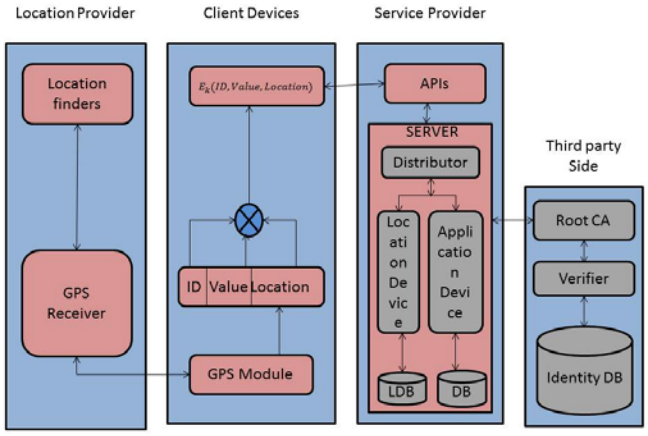

Figure 1. A Proposed System Architecture

Table-1 lists the interfaces exposed by the storage server. We argue that these function calls are flexible to support a wide variety of LBSAs. In our classification there are two requests only. One request is for inserting some information like multimedia information, location data, and time etc. for sharing with friends whereas another request is for accessing media with preserving user privacy. In big data analysis we have to handle huge data simultaneously and in social media privacy of a user's information and location is a great concern today.

Load_info.These request enable users to share application specific data in encrypted form with their friends and also enable user for sharing information about a site in the geographic location (x,y)- the longitude and latitude value obtained from a user positioning system. In the server users' location will preserve in an encrypted format as all users cannot trace her location. The key Id is the public key of the user that is putting the data, and puts are authenticated by the storage server.

Get info. Anyone in the network that knows a user's public key can get the contents from that storage server. However, since only the friends know the public key of a user which will be used to decrypt the content of user message and a friend can access user's data through get-info, all non-friend users essentially get cypher data that they cannot understand.

2) Server: It is necessary for storing the history records of user location with respect to time. It communicates directly with certificate authority. As the source identities of the location are stored as pseudonyms in the server, it is impossible for the hacker to reveal the real source of the location even it is compromised and monitored by attackers.

3) Certificate Authority: A certificate authority or certification authority (CA) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows friends to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate. So every client registers with the CA and pre-loads a set of public/private key pairs prior to entering the network. And CA is the only party who knows the mapping between real identity and pseudonyms, and work as a bridge between server and verifier. CA can retrieve location from the server and forward it to the verifier.

4) Verifier: Verifier is a third party user or an application that is authorized further the location of a user which was stored in the server. This verifier also has very important participation for preserving privacy of a user.

5 Protocol And Algorithm

5.1 Protocol

In any timestamp when a service provider needs to collect user information, it it executes the protocol in figure-2 to obtain user status from the third party side. Each user uses its N pseudonyms $X_{j=1}^{N}$ as its identity throughout the communication.

a. The client device send a user request to the service provider through its communication channel. The request should contain the user *identity*, user information –*value*, user *location* which is provided by the GPS module *and* user current *timestamp.* This request is signed and hashed by the client to make sure that no attacker can access or modify the request. In order to protect from traffic monitoring or eavesdropping attacks the requests are also encrypted by the server public key.

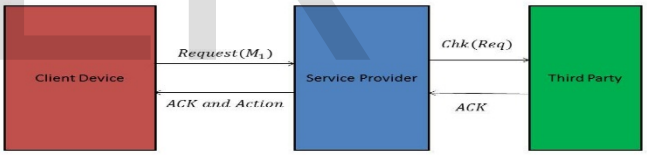

Figure 2. User verification protocol

b. After receiving the request from the client device, service provider will forward it to the third party side for checking the status of user as identity database is placed in the third party side. The forwarding message includes user id, user value, and server current timestamp T_s. By using decision making logics third party side will take decision regarding the status of requesting user with the integrating services of root CA, verifier and identity database. Then it acknowledges the user status to the client device via service provider.

Four possible decisions on user status will be taken. First one is "TT" which means that user is authentic and her value will not be concerned for others privacy, second one is "TF" which means that user is authentic but her content may provide somewhat privacy risk for other user, third one is "FT" and last one is "FF". In last two cases users are not authentic and so their access will be terminated.

c. After the initial request when client device will continue its communication then the subsequent requests must include user status in its requesting message which will contribute to the velocity of whole system.

5.2 Algorithm

Suppose for a user I has a set of pseudonyms $P_1, P_2, \ldots P_N$ while change periodically, and distinct parameters λ_1, λ_2 ,……..λ_N for each pseudonym are predetermined. If each pseudonym $P_j$changes its locations such that the inter-change interval follows Poisson distribution with parameter λ_j, then the entire inter-change intervals for node ifollow Poisson distribution with a parameter of $\lambda = \lambda_1 + \lambda_2 + \ldots\ldots + \lambda_N$. Pseudonym has important properties which we will describe in the next section and will prove them mathematically.

Algorithm: Random Pseudonym for location Privacy
Input: A slot of users $N(U_1, U_2 \ldots\ldots U_N)$
Step1: Generate N distinct parameter $\lambda_1, \lambda_2, \lambda_3, \ldots\ldots\ldots\ldots \lambda_N$ such that $\lambda = \lambda_1 + \lambda_2 + \ldots\ldots\ldots\ldots + \lambda_N$
Step2: **for** $U_{i=1,2\ldots\ldots N}$ **do**
Step2: Assigned user pseudonym
Step3**: for** each pseudonym i**do**
Step4: **if** running process follow the Poisson distribution with parameter λ_i **then**
Step5: M_i= Encrypt(Location(x,y) and ID)
Step6: **else** goto step 2
Step7: **attest (M_i)**
Step8:**end if**
Step9:**end for**
Step10**: end for.**

6 Privacy Analysis & Performance Trade-off

In this section we describe the intuition behind the privacy guarantees provided by our design. We first describe the properties of source location privacy and then the server interface in order to prevent some possible attack in the given design.

Form the location proof history we can obtain some sort of knowledge on how attacker may reveal location of a user through violating privacy. Assume that attackers are very strong (has sufficient resources). Attacker will follow some steps for violating privacy where at first she simply monitor the communication and content of a user and search the real name of a user and location. Secondly even if the user name is encrypted she back to the record and analysis location activities for recognizing the targeted user name and secret information. Lastly she will try to correlate with the user pseudonym and location as in our design pseudonyms are changing periodically.

In our design all steps of an attacker will be faced as we used here dynamic pseudonym instead of real name of a user and distributed storage mechanism where different private information are stored in different point.

Proposition 1: (Distribution of Privacy Knowledge)

In this design privacy related knowledge are separately preserved in the processing module for providing strong security. In the processing module each part only has partial knowledge. Strong privacy is generated form this type of distribution mechanism. In this design server has user's pseudonym and location, CA only knows real name and pseudonym whereas verifier has information about real identity and location.

Hackers cannot reveal any user's private information even if they can leak the server and also can compromise with the checker. As attackers are unable to learn a user's location and identity without integrating all the knowledge.

In our system all pseudonyms are unpredictable and independent and so even if any hacker can compromise with any user or any part of the system she cannot calculate the next pseudonym of the user.

Proposition 2: (Pseudonym Independency)

As one pseudonym is not derived from another name and so all of our pseudonyms are statistically random. In our system if we consider PO possible observation of an attacker and $SP_1, SP_2, SP_3 \ldots\ldots SP_n$ are the possible pseudonym of an user.

Our all pseudonym must support the following equation-

$$\forall i, j, \forall PO, Probability\ of\ (SP_i|PO) \neq Probability\ of (SP_j|PO)$$
$$where\ i, j \in \{1, 2, \ldots, n\}, i \neq j.$$

Pseudonym independency also extends the user privacy as attacker cannot link one name to another name and also she will be confused about tracing the location of users. And so we can say that users' location will be undefined due to pseudonym independency.

Proposition 3: (Location Undefined)

In our system all users are assigned by some dynamic pseudonyms which are independent and this property will provide another privacy on user location named "location undefined". Location is valueless if you cannot treat who he/she is. If there is PO observation in our system and I is the identity of an user then I is undefined if and only if $\forall PO, Probability\ of\ (I) = Probability\ of\ (I|PO)$.

So from the proposition 2 and 3 we can summarize that a system must be location undefined if that system has the property of pseudonym independency.

There is another important term time which has pivotal contribution in our system. Various times we have to consider for describing our system. Setup time, time required to setup the request of a requesting user. The setup time of a system is approximately constant. Holding time is an average duration of a typical user involving on a media through a single initial request. In aspect of user social media is an intermittent communication network and so we have to consider inter request delay for a pseudonym.

Suppose a request can occur several times within a given unit of time. When the total number of occurrences of the request is unknown, we can think of it as a random variable. This random variable has a Poisson distribution if and only if the time elapsed between two successive occurrences of the request has an exponential distribution and it is independent of previous occurrences.

A random variable having a Poisson distribution is the number of request calls received by a SMP (social media

provider). If the time elapsed between two successive request calls has an exponential distribution and it is independent of the time of arrival of the previous calls, then the total number of calls received in one hour has a Poisson distribution.

The concept is illustrated by the plot above, where the number of request calls received is plotted as a function of time. The graph of the function makes an upward jump each time a request call arrives. The time elapsed between two successive request calls is equal to the length of each horizontal segment and it has an exponential distribution. The number of calls received in 60 minutes is equal to the length of the segment highlighted by the vertical curly brace and it has a Poisson distribution.

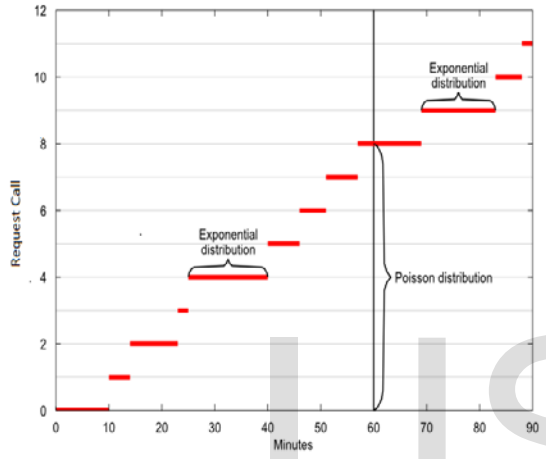

Figure 3. Request Call with Time Function Including Distribution

We assume that inter request delay *(D)* between two requests *y* and *y+1* from a pseudonym i of a user be $D^i_y = \tau^i_{y+1} - \tau^i_y$ where τ^i_y is the requesting time of y from pseudonym *i* and τ^i_{y+1} is the requesting time of *y+1* from the pseudonym *i*. So the total update delay for the pseudonym *i* is $Z=D^i_1, D^i_2, D^i_3, \ldots\ldots$ And the distribution of total request delay of a user is statistically distinct from each other as it is impossible to correlate them with each other. And total update delays are statistically distinct if and only if they follow same type of probabilistic distribution with distinct parameter.

We can consider here a random Poisson distribution. Let W be a discrete random variable. Let its support be the set of positive integer numbers:

$$R_z \in Z_+$$

Let $\lambda \in R_{++}$. We say that W has a Poisson distribution with parameter λ if its probability mass function is

$$f(Z=w) = \begin{cases} e^{-\lambda}\frac{1}{z!}\lambda^z & iff \quad w \epsilon R_z \\ 0 & iff \quad w \notin R_z \end{cases}$$

From the figure the time elapsed between two successive request calls is equal to the length of each horizontal segment and it has an exponential distribution but we consider here Poisson distribution to control the rate of request from the user. Poisson distribution has strong relation with exponential distribution and it is more popular distribution in an intermittent network as Poisson distribution has some similar properties with request rate of social media.

The relation between the Poisson distribution and the exponential distribution is summarized by the following Lemma:

Lemma 1: The number of occurrences of an event within a unit of time has a Poisson distribution with parameter if and only if the time elapsed between two successive occurrences of the event has an exponential distribution with parameter and it is independent of previous occurrences.

Proof: Let

τ_1 the time elapsed before the first event occurs

τ_2 the time elapsed between the first and the second occurrence of the event

…… ……..

τ_n the time elapsed between the (n-1)th and the n-th occurrence of the event

and by χ the number of occurrence of the event. Since $\chi \geq x$ if and only if $\tau_1 + \tau_2 + \cdots + \tau_x \leq 1$ (convenience yourself of this fact), the proposition is true if and only if $P(\chi \geq x) = P(\tau_1 + \tau_2 + \cdots + \tau_x \leq 1)$ for any $x \epsilon R_x$. To verify that the equality holds, we need to separately compute the two probabilities.

We start with $P(\tau_1 + \tau_2 + \cdots + \tau_x \leq 1)$.

Denote by the Z the sum of waiting times: $Z = \tau_1 + \tau_1 + \cdots + \tau_1$

Since the sum of the independent exponential random variables with common parameter λ is a Gamma random variable with parameters 2x and x/λ, then Z is a Gamma random variable with parameters 2x and x/λ, i.e its probability density function is

$$f_Z(Z) = \begin{cases} cz^{x-1}e^{-\lambda Z)} & if \; z \epsilon [0, \propto) \\ 0 & if \; z \notin [0, \propto) \end{cases}$$

Where $C = \frac{\lambda^x}{\Gamma x} = \frac{\lambda^x}{(x-1)!}$

And the last equality stems from the fact that we are considering only integer values of x. We need to integrate the density function to compute the probability that Z is less than 1:

$$P(\tau_1 + \ldots + \tau_x \leq 1) = P(Z \leq 1)$$

$$= \int_{-\infty}^{1} f_z(z)dz$$

$$= \int_{0}^{1} cz^{x-1} \exp(-\lambda z)dz$$

$$= c\int_{0}^{1} z^{x-1}\exp(-\lambda z)dz$$

The last integral can be computed integrating by parts x-1 times:

$$\int_{0}^{1} z^{x-1}\exp(-\lambda z)dz$$

$$=[-\tfrac{1}{\lambda}z^{x-1}\exp(-\lambda z)]_0^1 + \int_0^1 (x-1)z^{x-2}\tfrac{1}{\lambda}\exp(-\lambda z)dz$$

$$= -\tfrac{1}{\lambda}\exp(-\lambda) + (x-1)\tfrac{1}{\lambda}\int_0^1 z^{x-2}\exp(-\lambda z)dz$$

$$= -\tfrac{1}{\lambda}\exp(-\lambda) + (x-1)\tfrac{1}{\lambda}\{[-\tfrac{1}{\lambda}z^{x-2}\exp(-\lambda z)]_0^1 + \int_0^1 (x-2)z^{x-3}\tfrac{1}{\lambda}\exp(-\lambda z)dz\}$$

$$= -\tfrac{1}{\lambda}\exp(-\lambda) - (x-1)\tfrac{1}{\lambda^2}\exp(-\lambda) + (x-1)(x-2)\tfrac{1}{\lambda^2}\int_0^1 z^{x-3}\exp(-\lambda z)dz = \ldots..$$

$$= -\sum_{i=1}^{x-1}\tfrac{(x-1)!}{(x-i)!}\tfrac{1}{\lambda^i}\exp(-\lambda) + \tfrac{(x-1)!}{1}\tfrac{1}{\lambda^{x-1}}\int_0^1 \exp(-\lambda z)dz$$

$$= -\sum_{i=1}^{x-1}\frac{(x-1)!}{(x-i)!}\frac{1}{\lambda^i}\exp(-\lambda) + \frac{(x-1)!}{\lambda^{x-1}}[-\frac{1}{\lambda}\exp(-\lambda z)]_0^1$$

$$= -\sum_{i=1}^{x-1}\tfrac{(x-1)!}{(x-i)!}\tfrac{1}{\lambda^i}\exp(-\lambda) - \tfrac{(x-1)!}{\lambda^x}\exp(-\lambda) + \tfrac{(x-1)!}{\lambda^x}$$

Multiplying by c, we obtain

$$= \quad c\int_0^1 Z^{x-1}e^{(-\lambda Z)}dz$$

$$= \frac{\lambda^x}{(x-1)!}\int_0^1 z^{x-1}e^{(-\lambda Z)}dz$$

$$= -\sum_{i=1}^{x-1}\frac{\lambda^{x-i}}{(x-i)!}e^{-\lambda} - e^{-\lambda} + 1$$

$$= \quad 1 - \sum_{i=1}^{x}\frac{\lambda^{x-i}}{(x-i)!}e^{-\lambda}$$

$$= \quad 1- -\sum_{j=0}^{x-1}\frac{\lambda^j}{j!}e^{-\lambda}$$

Thus we have obtained

$$\mathrm{P}(\tau_1 + \ldots + \tau_x \le 1) = 1 - \sum_{j=0}^{x-1}\frac{\lambda^j}{j!}\exp(-\lambda)$$

Now we need to compute the probability that χ is greater than or equal to x:

$$\mathrm{P}(\chi \ge x) = 1 - \mathrm{P}(\chi < x)$$

$$= 1 - \mathrm{P}(\chi \le x - 1)$$

$$= 1 - \sum_{j=0}^{x-1} P(\chi = j)$$

$$= 1 - \sum_{j=0}^{x-1} Px(j)$$

$$= 1 - \sum_{j=0}^{x-1}\frac{\lambda^j}{j!}e^{(-\lambda)}$$

$$= \mathrm{P}(\tau_1 + \tau_2 + \cdots + \tau_x \le 1).$$

$$\mathbf{P(\chi \ge x) = P(\tau_1 + \tau_2 + \cdots + \tau_x \le 1).}$$

(Proved)

So in this method all occurrences are independent. Here pseudonym has individuality to each other and so location of users is undetectability.

7 Privacy Evaluation

As stated in section V our method has the property of pseudonym individuality and statistically strong source location undetectability. So statistically it is proved that the source privacy of location information can be well preserved. Here we evaluate our system against powerful traffic analysis and statistical test.

As an attacker if you want to detect that two pseudonym belongs to the same user then you have to search whether two probabilistic distributions of time intervals from the two pseudonyms are identical. For the attacker the hypotheses of the test are:

H_1-Two pseudonyms belongs to the same user, and H_2-Two pseudonyms belongs to the different user.

False negative has some effects in our system whereas false positive has no effect in our model and so it has very much potential possibility to prevent active or passive attacks. In our approach when attacker makes a decision to attack, there are enough risks to get wrong detection. If H_1 is in fact true accepting $H_2$is a false negative. In other case if H_2 is true accepting H_1 is a false positive. We are not concern for false positive attack but somewhat concern for false negative. From our observation result it is assumed that privacy of our system will be preserved through appropriate selection of standard deviation δ, and threshold value $\in$.

8 Related Work

Location privacy which is a particular type of data privacy, and it is defined as the ability to prevent other unauthorized parties from learning one's current or past location[7].The

need for location privacy is recognized in some of the earliest literature on information privacy (e.g., [8]) and location-aware computing (e.g., [9, 10, 11]). Recently in different literature on information privacy identified at least three key negative effects, Location-based "spam", Personal wellbeing and safety, and Intrusive inferences, associated with failures to protect location privacy within a location-aware computing environment.[12,13,14].In recent times several solutions have been proposed to improve location privacy like pseudonym and silent times[15],spatial and temporal cloaking. AnonySense[17] recently proposed using an anonymous routing overlay to preserve user location privacy. SmokeScreen[17] is designed to share presence information only with trusted users, and missed connections[18] looks at connecting users that shared a physical location without compromising their privacy at the server. Obfuscation [19] is an important technique for protecting an individual's location privacy within a pervasive computing environment. Mohamed F.M in [20] proposed three different architectures for hiding the user private location information, namely, the non-cooperative architecture, the third trusted party architecture, and the cooperative peer-to-peer architecture. Similarly different research works on location privacy is going on for solving new arrival privacy related problems and for providing the secure and reliable modern communication.

9 Conclusion And Future Work

This paper proposed a privacy method in social media which can be easily implemented in existing network with low cost and complexity. We used statistically dynamic pseudonym for each device to protect user location from each other. We argued in this paper that location-based applications need to take an approach where client will provide encrypted location point to the server. We proved here that this approach is flexible enough to implement several widely-used applications, and yet preserve location privacy of the users. In future we will try to expedite the scalability of this system and to extract a workload model from location updates to evaluate the performance of location based information-sharing and privacy-preserving algorithms.

Acknowledgment

I would like to thank my wife who encourage me to write a good dissertation on social media privacy. She also sacrificed a lot of romantic moments and recalled me about my research especially in the weekend. I would like to thank my Master's supervisor M.A.F.M Rashidul Hasan for his nice and valuable cooperation.

References

[1] Miluzzo, Emiliano, Nicholas D. Lane, Kristóf Fodor, Ronald Peterson, Hong Lu, Mirco Musolesi, Shane B. Eisenman, Xiao Zheng, and Andrew T. Campbell, "Sensing meets mobile social networks: the design, implementation and evaluation of the cenceme application." In *Proceedings of the 6th ACM conference on Embedded network sensor systems*, pp. 337-350. ACM, 2008.

[2] Motani, Mehul, Vikram Srinivasan, and Pavan S. Nuggehalli. "Peoplenet: engineering a wireless virtual social network," *Proceedings of the 11th annual international conference on Mobile computing and networking*.ACM, 2005.

[3] Hendrickson, M, "The state of location-based social networking on the iphone." *TechCrunch, September* 28 (2008).

[4] Mobile LBS on the move, Oct. 2008. http://www.emarketer.com/Article.aspx?R=1006609.

[5] Schilit, Bill, Jason Hong, and Marco Gruteser, "Wireless location privacy protection." *Computer* 36.12 (2003): 135-137.

[6] Humphreys, Lee, "Mobile social networks and social practice: A case study of Dodgeball." *Journal of Computer-Mediated Communication* 13, no. 1 (2007): 341-360.

[7] Ling Liu, "From Data Privacy to Location Privacy: Models and Algorithms" *VLDB '07*, September 23-28, 2007, Vienna, Austria.

[8] A. F. Westin, "*Privacy and freedom*.Atheneum." New York, 1967.

[9] Harper, Richard HR, "Looking at ourselves: an examination of the social organisation of two research laboratories." In *Proceedings of the 1992 ACM conference on Computer-supported cooperative work*, pp. 330-337. ACM, 1992.

[10] R. H. R. Harper, M.G. Lamming, and W. M, "Newman.Locating systems at work: Implications for the development of active badge applications." *Interacting with Computers*, 4(3):343–363, 1992.S.

[11] B.N. Schilit and M. M, "Theimer.Disseminating active map information to mobile hosts" .*IEEE Network*, 8(5):22–32, 1994.

[12] Gruteser, Marco, and Dirk Grunwald, "A methodological assessment of location privacy risks in wireless hotspot networks." In *Security in pervasive computing*, pp. 10-24. Springer Berlin Heidelberg, 2004.

[13] B. N. Schilit, J.I. Hong, and M. Gruteser, "Wireless location privacy protection." *IEEE Computer*, 36(12):135–137, 2003.

[14] Kaasinen, Eija, "User needs for location-aware mobile services." *Personal and ubiquitous computing* 7, no. 1 (2003): 70-79.

[15] Jiang, Tao, Helen J. Wang, and Yih-Chun Hu, "Preserving location privacy in wireless LANs."*Proceedings of the 5th international conference on Mobile systems, applications and services*.ACM, 2007.

[16] Cornelius, Cory, Apu Kapadia, David Kotz, Dan Peebles, Minho Shin, and Nikos Triandopoulos, "Anonysense: privacy-aware people-centric sensing." In *Proceedings of the 6th international conference on Mobile systems, applications, and services*, pp. 211-224. ACM, 2008.

[17] Cox, Landon P., Angela Dalton, and Varun Marupadi, "Smokescreen: flexible privacy controls for presence-sharing." *Proceedings of the 5th international conference on Mobile systems, applications and services*.ACM, 2007.

[18] Manweiler, Justin, Ryan Scudellari, Zachary Cancio, and Landon P. Cox, "We saw each other on the subway: secure, anonymous proximity-based missed connections." In *Proceedings of the 10th workshop on Mobile Computing Systems and Applications*, p. 1. ACM, 2009.

[19] M.Duckham and L.Kulik, "A Formal Model of Obfuscation andNegotiation for Location Privacy", Springer-Verlag Berlin Heidelberg 2005.

[20] Mokbel, Mohamed F, "Privacy in Location-based Services: State-of-the-art and Research Directions." *Mobile Data Management, 2007 International Conference on*. IEEE, 2007.

Md.Ileas Pramanik, Assistant Professor in Computer Science and Engineering Department, Begum Rokeya University, Rangpur, Bangladesh. Currently he is a PhD candidate in Information System Department in City University of Hong Kong. He is also a member of Hong Kong Computer Society. He was Head of Department in Computer Science and Engineering, Begum Rokeya University, Rangpur.
E-Mail: mpramanik2-c@my.cityu.edu.hk

Mirza A. F. M. Rashidul Hasan received the B.Sc.(Hons), M.Sc. and M.Phil. degrees in Applied Physics and Electronic Engineering from University of Rajshahi, Bangladesh in 1992, 1993, and 2001, respectively. In 2006, he joined University of Rajshahi, Rajshahi, Bangladesh as a faculty member, where he is currently serving as an Associate Professor in the Department of Information and Communication Engineering. He was a visiting researcher at Waseda University, Japan from 2003 to 2004 and as junior fellow of IWMI from 2006 to 2007. He received his D. Engg. degree in 2012 from the Graduate School of Science and Engineering, Saitama University, Saitama, Japan.
E-Mail: mirza_iu@yahoo.com

Bijoy Kumer Karmaker.Assistant Professor in Electronics and Communication Engineering Department, **Jatiya Kabi Kazi Nazrul Islam University,**Bangladesh.
E-Mail: bijoy_ice@yahoo.com

M.Tosaddek Alam is a B.Sc.(Engg) student in Computer Science and Engineering Department, Begum Rokeya University, Rangpur, Bangladesh. His research interest in Cryptography, Data mining, Communication.
E-Mail: tosaddek05@gmail.com

Corresponding Author:
Md.Ileas Pramanik, PhD candidate in Information System Department in City University of Hong Kong. He is also a member of Hong Kong Computer Society. E-Mail: mpramanik2-c@my.cityu.edu.hk