1.  
Assalamualaykum

I am Niamul hasan

My Id is 17201026  
Now, I am going to present a research paper   
this paper is titled as

An effective Privacy Architecture to preserve user Trajectories in Reward Based LBS Application

So, let’s start:

Next slide

2.

Overview……………….!

* Basically, this paper is all about a  
  client-server privacy architecture which may able to preserve user privacy while using Reward based LBS Applications.
* Now here is a question:   
  How can training performance data be collected, measured, and published in a mobile program while preserving user privacy?
* This question is becoming important in the context of the growing use of reward-based location-based service (LBS) applications.
* One of the main concerns of such applications is the privacy of user trajectories, because the applications normally collect user locations over time with identities.
* In this paper, identified personal privacy problem in a reward-based LBS application and propose privacy architecture with a bounded perturbation technique to protect user’s trajectory from the privacy breaches. Bounded perturbation uses global location set (GLS) to anonymize the trajectory data.

Next slide

3.

* LBS applications is basically, location-based service applications………………!  
  Now days, user locations are used in a wide range of LBS applications such as health and wellness programs where walking or running trajectories are measured for training purposes.
* increasing number of companies are rewarding employees based on their training data. Such LBS applications are called reward-based LBS applications.

Next slide

4.Now,  
The breach of identified trajectories……………….!

* The data logs generated by a reward-based LBS application have trajectories with exact locations and the corresponding user identities, which can be used for spam advertisements, individual-based assaults, and linking attacks
* The breached user trajectories could be used to identify a user and her points of interest in the other publicly available datasets.
* The breach of identified trajectories thus brings serious security and privacy issues for implementing reward-based LBS applications.
* Here in this picture (মাউস নিয়ে জাব পিচ এর উপর)

We can see an example of location data breaching.  
This is about a weather forecast app, which Accuweather Sharing Geolocation Data with a Third-Party Firm.

* Here what happens in this situation:

The user of the app shares his location to get the proper weather forecast.

* The weather app that gets your location details.
* That location data will be sent to a third party firm.
* Reveal mobile will discover your coordinates using public data along with MAC address of router you are connected to.
* By using public data, someone could find you anywhere in the world in just a few minutes.

Next slide

5.

Inference and Linking Attacks

* Now, In reward-based LBS applications, we know that the location data has been submitted to the organization with the user identity. From the inference attack, an adversary could gain knowledge about mobility frequency for a user’s particular route. Therefore, inference attacks help an adversary to link the user with the publicly available data sources to identify the user’s corresponding sensitive information, which is called a linking attack.
* The related work shows that trajectories are of importance to user privacy. In this paper, we are focusing on hiding user visiting trajectories which are generated by reward-based LBS applications in order to avoid inference and linking attacks.

Next slide

6.

**A Client-Server-Based Privacy Methodology**

Now here we will see the client-server privacy architecture, followed by the proposed bounded perturbation technique to effectively anonymize identified trajectories with utility preservation.

* The fundamental functionality of the proposed privacy architecture lies in anonymizing the user trajectory in a client-server privacy setting to ensure that the data contributors are safe in a dataset.

In the privacy architecture, it has the following components: end-user (employee), intermediary device (client), central server, business organization (or employer), and data processing organization (insurance company).

* Here in the picture: (মাউস নিয়ে জাব পিচ এর উপর)

We see an Example overview of the proposed client-server privacy architecture about insurance company,

So, in the example: we see

* An employee generates LBS application-specific data by health fitness devices that link with the intermediary device for the trajectory anonymization. An intermediary device could be a cell phone, a computer, or any suitable device that executes the procedure to complete the anonymization processes. It anonymizes the trajectory at the user end by applying the bounded perturbation technique. For anonymization, the intermediary device requests that the global location is set to the central server and anonymizes the visiting locations of the user.
* The central server supports the anonymization process, which generates the global location set and keeps the records from users. An employer is the facilitator to introduce a reward-based LBS application. Moreover, an employer uses the application-specific data to give rewards to end-users for being active in daily life and to negotiate with insurance companies to reduce insurance cost.
* An insurance company is a third-party business organization that would use end-user data for analysis.

Next slide

7.

**Anonymization**

* Identified trajectories would breach user privacy, and we must anonymize such trajectories before sharing them with the central server. To anonymize the trajectories, we introduce a global location set to perform bounded perturbation.
* For that,   
  Now, see the block 1 (মাউস নিয়ে জাব পিচ এর উপর)  
  Let u denote a user in the reward-based LBS system. A movement of user u updates a tuple<id,(x, y, t)>, where id represents the identity of the user u, and the tuple describes that the user u visited point (x, y) at time t. Here, x is the longitude, y is the latitude, and t is the detailed recording of time. The user movement history can be used to draw the movement patterns of the user.
* Now let’s see the block 2,

Identified trajectory  
An identified trajectory is a sequence of successive PoIs visited by an identified user along time t, represented as this equation

(মাউস নিয়ে জাব পিচ এর উপর)  
where id is the identity of user u and these are the (মাউস নিয়ে জাব পিচ এর উপর)

visited points at every t times.

Here any independent part of a user u with a start and end point is called a route.

a unique route might identify a user and threaten his privacy.

Here, a global location set (GLS) is introduced to perform the anonymization operation.

Next slide

8.

* Now, Global location set (GLS))
* A GLS consists of all the points of interest or PoIs in a region. Every PoI has a location and a description for its semantic meaning.
* GLS is generated by using OpenStreetMap API.  
  In the figure is an example of a global location set, where nodes represent the PoIs.  
  Generally, PoIs are connected with each other by the road networks.
* we consider that the PoIs are connected with each other by a distance d.
* Here, For trajectory anonymization, we may append the random noise r (মাউস নিয়ে জাব পিচ এর উপর) with the visited PoIs, which will result in new PoIs.

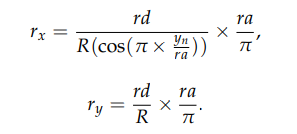
It may happen that the new pols   
are impossible to visit in reality.  
Therefore, we propose bounded perturbation techniques with the global location set GLS to anonymize the location trajectory

Next slide

9.**Bounded perturbation**

* Now, bounded perturbation includes random noise r with the actual data points, but it takes the global location set GLS into consideration to guarantee its availability. Therefore, the generated data points would not include invalid places. This reduces the utility of the generated trajectories.
* For instance, the new PoIs are generated by adding some random noise r
* So, the equation is (মাউস নিয়ে জাব পিচ এর উপর) this

where rx is the random noise for xn and ry is the random noise for yn.

Then, the random noise rx, ry is (মাউস নিয়ে জাব পিচ এর উপর)   
 these equations

* We compare the generated point with the global location set GLS by the map matching techniques
* If it is in the GLS, we keep it as a newly generated anonymized point. Otherwise, we recompute the point with new random noise until it is in the GLS.
* Given an identified trajectory L and applying bounded perturbation technique to generate the anonymized trajectory L’ , represented by

 (মাউস নিয়ে জাব পিচ এর উপর) this

* An anonymized trajectory L’ is the newly generated trajectory bounded by GLS with the visited timing information, and it excludes original visited places from the identified trajectories, so that the anonymized trajectory L’ will protect the user’s PoIs, unique routes, and frequent routes.
* The primary goal for preserving user privacy is anonymizing the trajectory, and we must also consider the data utility. Therefore, in the anonymized dataset, we measure the data utility by the relative distortion.

Next slide

10.

* In this section, we will look at two algorithms to perform anonymization of identified trajectories. We introduce the global location set to do the anonymization process effectively.
* Algorithm 1: produces a global location set. Taking the daily identified trajectory L and the global location set as arguments.  
  basically this algorithm is introduced to complete the perturbation process for user-visited locations over a particular time period. As a perturbation process may generate invalid PoIs, we introduce a global location set GLS, and the generation of PoIs will be within the set in order to avoid problems. We thus call the perturbation process a bounded perturbation. Algorithm 1 produces the GLS at the server side, and an intermediary device requests it in order to complete the anonymization process.
* Algorithm 2: outputs the anonymized trajectory L’ for the corresponding L.

The anonymized location trajectory algorithm is executed at the user end in a suitable device called the intermediary device to anonymize the user’s visited locations.

Next slide

11.

Experimental Evaluation

* In this section,  
  demonstrated the experiment on real-world datasets it shows that

the bounded perturbation method can successfully anonymize the trajectory points at the intermediary device.

* The experiments are divided into two parts:
* The 1st part was designed to present the personal privacy breach and test the effectiveness of the proposed bounded perturbation algorithm for trajectory anonymization in comparison with the perturbation methods.
* In the 2nd part, we measure the effectiveness of bounded perturbation and perturbation techniques in preserving data utility as compared with the original trajectory data

Next slide

12. **Conclusions and Future Work**

This research demonstrated the significance of the anonymization of identified trajectories. In this paper, the proposed client-server privacy architecture was able to preserve user privacy while keeping the data utility of the identified trajectories.

Now For the future work……!  
aim to improve the bounded perturbation method by completing the anonymization process locally.

Next slide

13.

That’s all about.

Thank you

END:

Experimets:

(এখানে শুরুতেই privacy brach করে দেখানো হইছে। যে কত সহজে attacker attack করে privacy breach করে।

এরপর

Location Trajectory Anonymization অর privacy setting

Use করে দেখা হয়েছে।  
তাতে user এর বিক্ষিপ্ত লোকেশান দেখা গেসে এবং যা থেকে adversary কোন প্রয়োজন মত data পায় না।

)

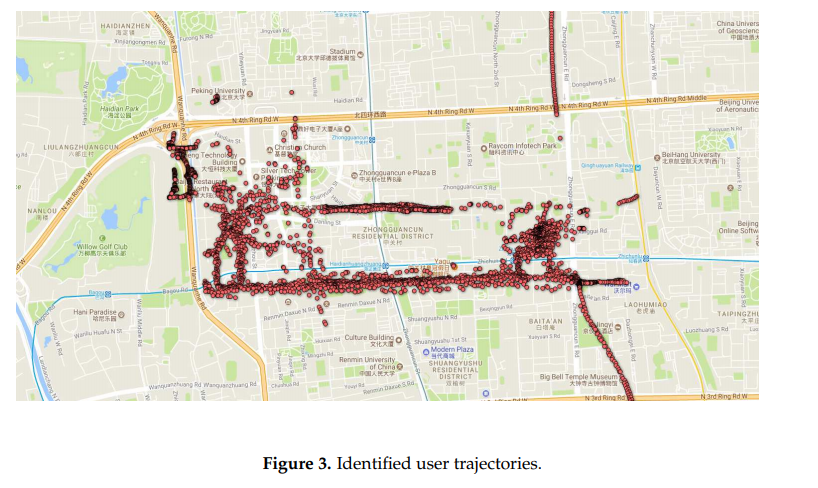
In the experiment, used the Geolife project dataset to simulate the reward-based LBS application.  
To assemble the experimental environment.

used OpenStreetMap API

Privacy Breach:

In this section, we present the significance of protecting the user privacy of identified trajectories in a real-life setting. Figure 3 demonstrates user trajectories over a period of time, and it gives the confidence to the adversary to learn about the particular user and can initiate an inference attack or conduct a linking attack to an available dataset. From the trajectories for a period, the adversary can find the user’s frequent routes and the points of interest.

Therefore, the identified trajectories from a reward-based LBS application might breach user privacy.



Location Trajectory Anonymization:

From the privacy breach section, it is observed that the user’s privacy was breached by revealing points of interest and frequent routes, which may lead to an inference attack and a linking attack. In this case, it is necessary to anonymize the identified trajectory before presenting it to the organization’s central server or a third-party service provider. In the privacy setting, we anonymized the user’s daily trajectory and submitted it to the central server. Figure 4 shows the anonymized locations of a user for a period of time, and the figure demonstrates that it has no frequent routes which the adversary may use to breach user privacy

