**EFFICIENT LOCATION PRIVACY**

FNU Kanchan kk2064@rit.edu | Advisor Dr. Peizhao Hu

---

### Motivation
- Many social apps offer nearby friends feature, which requires GPS coordinates. Releasing location data leads to privacy concerns such as tracking by service providers.
- Location data stored in third-party server may lead to privacy threats including insider attacks e.g. employees of a company exploiting private data.
- This project aims to develop an efficient location masking technique that offers privacy and usability of location data.
- We follow spatial cloaking approach.

### Common GeoHashing Technique
- We use a technique called Z-order curve (used in Bing map tile system [1]), which maps two dimensional coordinates into a binary string.
- This mapping preserves locality of points. The closer the two points, the smaller the two enclosing bounding box.

#### Trusted Server Version:
- Common solution for location privacy uses spatial cloaking.
- GPS location data is sent to a trusted sever.
- Server operates prefix matching to compute bounding box to be sent back as result. This box encloses all the communicating users.

#### Problems:
- The default GeoHashing technique lacks precision for some location points, even if the two users are close.
- Error can be significant, thus contains lot of noises in the result of a distance query.

### New Approaches

#### Two-Party Computation version:
- Infrastructureless & ad hoc approach.
- Masked bounding box or coordinates are exchanged or shared among communicating parties without any server or third party intervention.
- **Issues:** scalability.

#### Location Privacy with Control Version:
- Location encoded as binary key is sent to trusted server.
- Level of detail is only shared initially or on user’s request.
- If there is a third party request for a user’s details, encoded location of the user, masked to the level of detail, is sent back.
- Less noise than the basic GeoHashing technique.
- **Issues:** trusted server required.

#### Homomorphic Encryption (HE) without Trusted Server Version:
- Very efficient and secure approach in terms of HE.
- Level of detail is only shared initially or on user’s request.
- Encoded location data is encrypted and shared with server.
- The encrypted binary key is masked with the level of detail and sent to the user interested or exchanged between users.
- The result is decrypted on the user’s side.

### Spatial Cloaking

**For Privacy:**
- Reveal the box, not the location point.

**For Usability:**
- Allow users to control the level of details (LoD).

- Different boxes depending on the distance between two points and the level of detail.
- Size of box and hence, error shows exponential change as the level of detail changes.

### Evaluations & Conclusions

<table>
<thead>
<tr>
<th>User1</th>
<th>User2</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="User1" /></td>
<td><img src="image2.png" alt="User2" /></td>
<td><img src="image3.png" alt="Server" /></td>
</tr>
</tbody>
</table>

**Table:**
- Two Party Comp. Version:
- Trusted Server Version:
- Loc. Privacy w Control Version:
- HE w/o Trusted Server Version:
- N/A Server View Not Possible

**For Usability:**
- Our method reduces error and yields better results as compared to the previous approach.
- It provides a new insight to give some control to user in the area of location privacy.

**For Privacy:**
- Incorporate these techniques into Homomorphic Encryption. Location data will be encrypted, thus don’t need a trusted server.
- Prepare a technical paper for publication.

### Planned Future Work

### References
