Location Privacy

Final Presentation
Group #1

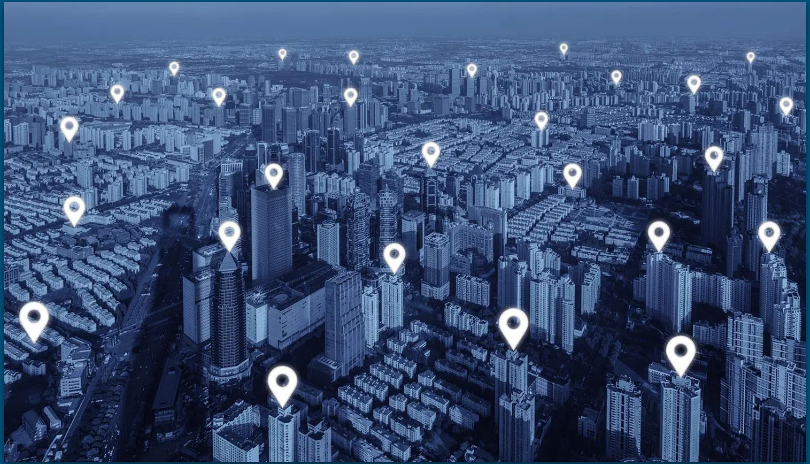
Osman Buğra Aydın	21704100
Ege Hakan Karaağaç	21702767
Mustafa Tuna Acar	21703639
Mehmet Alperen Yalçın	21502273
Ahmet Furkan Ahi	21501903
Fırat Yönak	21601931
İlhan Koç	21603429

Content

1. Introduction
2. Goal of the Project
3. Related Work
4. Current Progress
5. Methods
6. Evaluations
7. Future Work
8. Conclusion

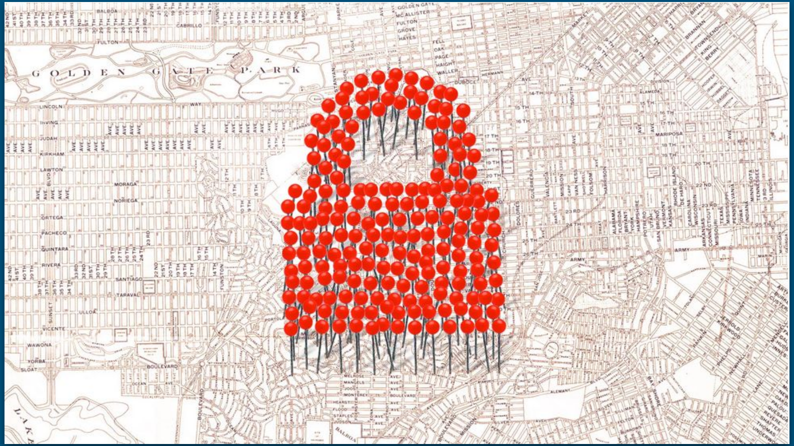
Introduction

- What is Location Privacy?
- K- anonymity and Noise Adding
- Why do we need them?



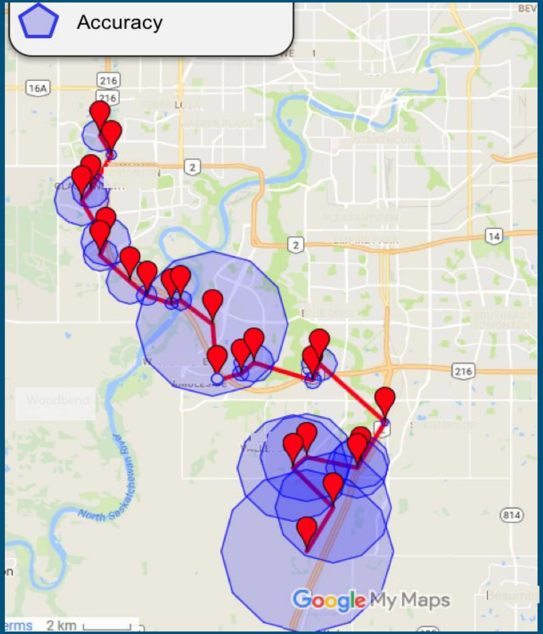
Problem Statement

What are the differences between addition of controlled noise and satisfying k-anonymity as methods to provide location privacy with respect to the same metrics?



Goal Of The Project

- Provide an implementation that gives accurate results for comparison
- Using these results compare k-anonymity and noise addition transparently
- Come to a conclusion using these comparisons



Related Work

OneTrust

- Comply with CCPA, GDPR, LGPD
- AI & Robotic Automation [1]

Privacy Protection For Users Of Location-Based Services

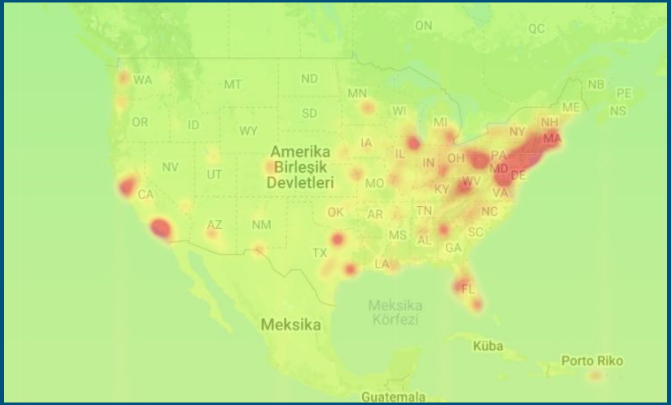
- Policy-Based Schemes
- Trusted Anonymization Server-Based Schemes
- Mobile Device-Based Schemes [2]

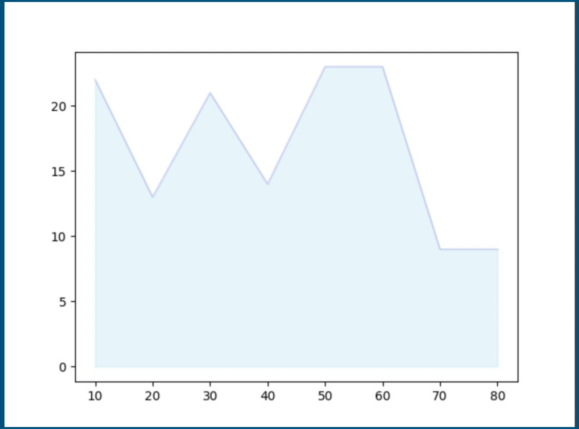
OneTrust

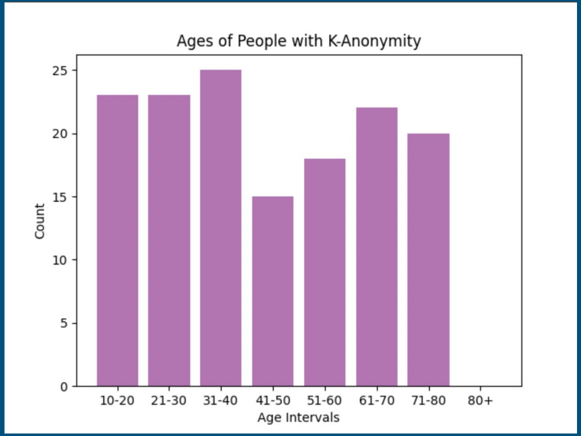
PRIVACY, SECURITY & GOVERNANCE

Current Progress

- Literature Review
- Dataset Arrangement
- Deciding Privacy Methods
- Implementation
- Evaluation







Methods For Location Privacy

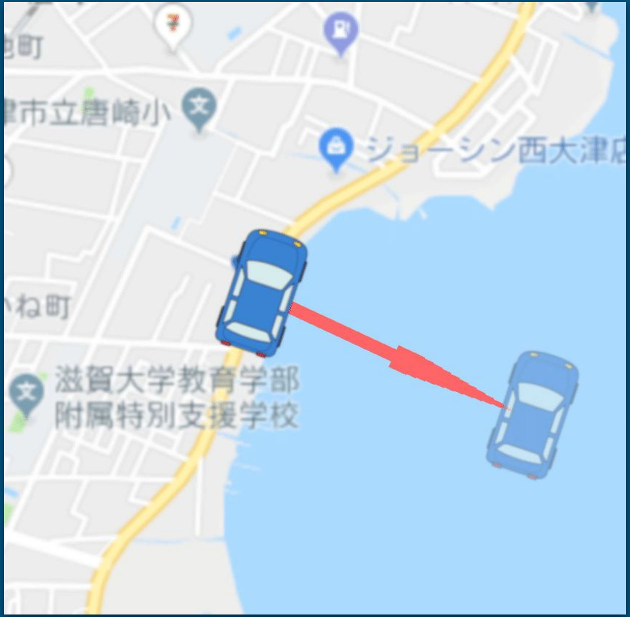
- Location Perturbation
- Laplace noise addition
- K-anonymity
- Spatial Clocking

Location Perturbation

- One of the simplest and weakest concepts[3].

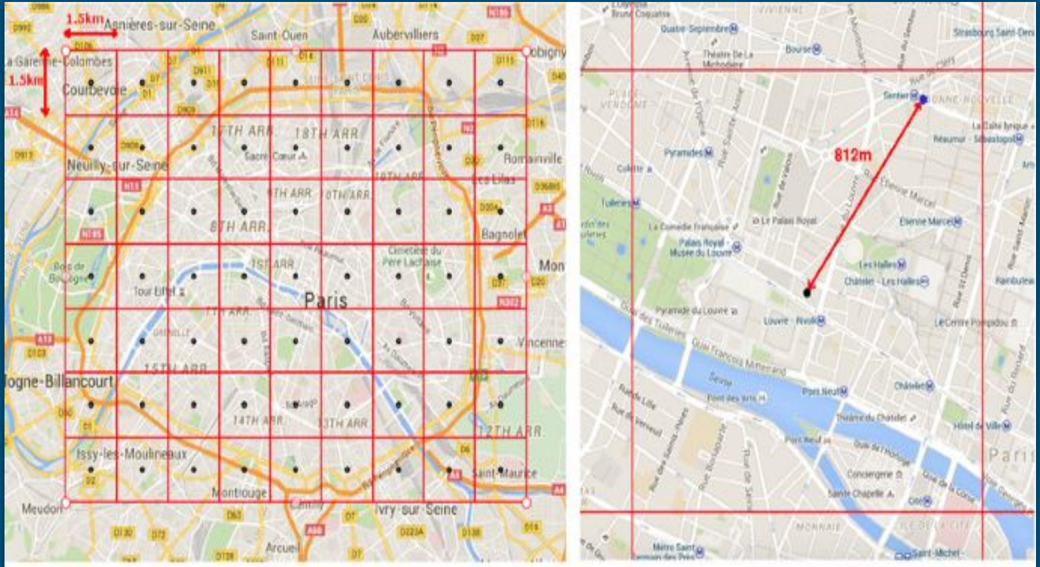
- The user location is represented with a wrong value, the privacy is achieved from the false reported location[3].

- The accuracy and the amount of privacy mainly depends on how far the reported location from the exact location[3].



Laplace Noise Addition

$$\mathrm{Lap}(x|b) = \frac{1}{2b}\exp\left(-\frac{|x|}{b}\right)$$



(a) (b)

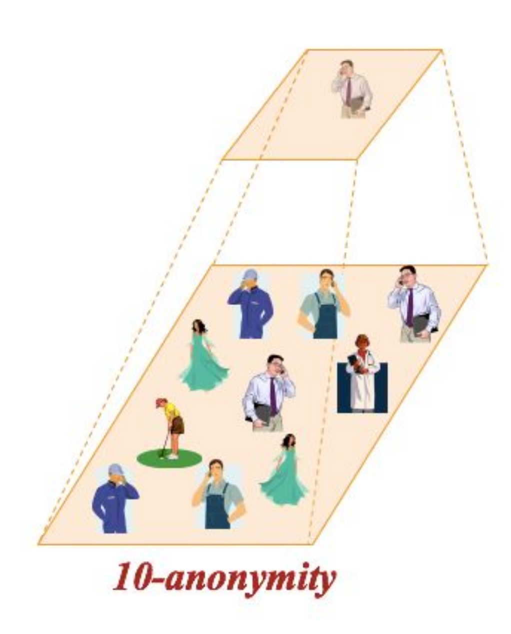
[4]

K-anonymity

- The concept is the same as in databases privacy[3].

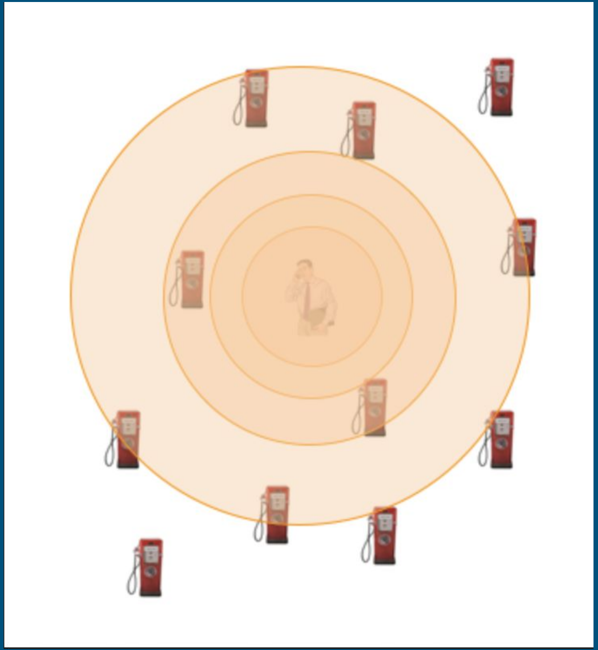
- The cloaked region contains at least k users and the user that asks the query is indistinguishable among other k users[3].

- The cloaked area largely depends on the surrounding environment. For example, a value of k=100 may result in a very small are if the user is on a stadium but a huge area if he is in the desert[3].



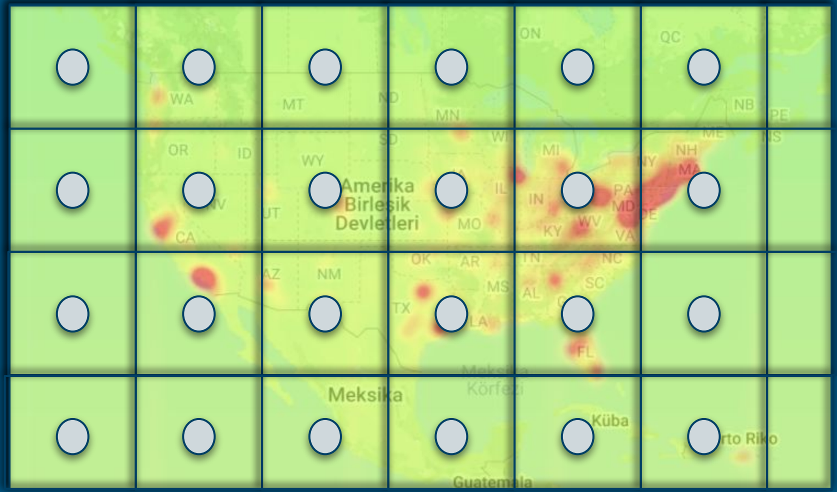
Spatial Cloaking

This technique is known as location cloaking, spatial blurring or location obfuscation, and the user location is represented as a region that contains the exact user location. An adversary knows that the user is located in the cloaked region, but has no clue where the user is exactly located. The area of the cloaked region achieves a trade-off between the user privacy and the user service[3].



Evaluations

- **Utility:**
  1. Accessing Individual Location
  2. Count in Distance & Area
- **Privacy:**
  1. Unlinkability
  2. Precision in Error Expectation



NEW YORK
RHODE
ISLAND
ENSİLVANYA
New York
DELAWARE
İRGİNİA

Utility

1. Accessing Individual Location

A. Relative Location

Spatial Cloaking

B. Real Location

Location Perturbation & Laplace Noise

& K-Anonymity

2. Count in Distance & Area

A. Distance: Spatial Cloaking

B. Area: K-Anonymity

Privacy

1. **Unlinkability**
    A. Distance

    Spatial Cloaking & Location Perturbation

    B. Exact Location [5]

    K-Anonymity & Laplace Noise

2. **Precision in Error Expectation**
    A. Systematic Errors

    Laplace Noise & Spatial Cloaking

    B. Random Errors

    Location Perturbation

Future Work

- Returning Dataset with Anonymity
- Adding Dummy Rows
- Adding Data to MySQL Database

Conclusion

- Location Privacy
- Privacy with different methods
- Metrics

THANKS FOR LISTENING

Do you have any questions?

References

[1] OneTrust. (2021, October 26). *Privacy management*. OneTrust. Retrieved November 8, 2021, from https://www.onetrust.com/solutions/privacy-management/.

[2] IEEE Xplore temporarily unavailable. (n.d.). Retrieved November 8, 2021, from https://ieeexplore.ieee.org/abstract/document/6155874.

[3] *Privacy in location based services - part 1: ~elf11.github.io*. Privacy in Location Based Services - Part 1 | ~elf11.github.io. (n.d.). Retrieved December 20, 2021, from https://elf11.github.io/2017/05/06/lbs-part-1.html

[4]E. ElSalamouny and S. Gambs, “Optimal noise functions for location privacy on continuous regions,” *International Journal of Information Security*, vol. 17, no. 6, pp. 613–630, 2017.

[5] Dantas, J. (2021, August 16). Differential privacy and K-anonymity for machine learning. Medium. Retrieved December 20, 2021, from https://towardsdatascience.com/differential-privacy-and-k-anonymity-for-machine-learning-fbb416f32b6