

LOCATION PRIVACY PROJECT

Guided By : Dr. Na Li



Prepared by

Safat
Mahmood

Tanzila
Choudhury

Ishan
Khatrri

Ayesha
Begum

OUTLINE

- Introduction
- Project Specification
- Technologies Needed
- Expertise Needed
- Project Accomplishment
- Challenges
- Conclusion
- Future works
- References

ABSTRACT

- In this presentation, we present a novel solution addressing location privacy issues on android platform. In some collaborative environments, the users are bound to share their exact location to the map application server to find directions to nearby Starbucks.
- In return, this may imply violations to their privacy. Some users may be concerned that the location based services may be able to track them by analyzing their service requests. Thus, we have designed and implemented a location-based android application giving the user an option whether they want to anonymize their location (i.e. they can send the exact location without any anonymization, or the location information manipulated by shifting it a little, or send a square area instead of a single point, to the remote service, aiming at anonymizing the real location of the requester.) before a request is sent to the google api service to get the directions to the point of interest location such as Starbucks in such a way that the users privacy is not compromised.
- We discuss the importance of the correct location in collaborative environments and we address the problem of privacy for users and show how current solutions, which aim to preserve the user privacy, can interfere with the correct behavior of some applications.

INTRODUCTION

What is a Location Based Service?

- A certain *service* that is offered to the users *based* on their *locations*.

INTRODUCTION (CONT.)

Location Services then



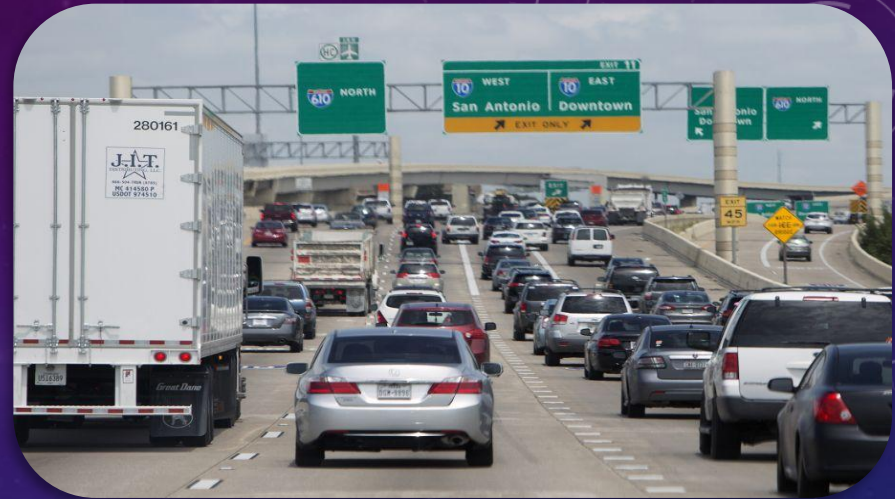
INTRODUCTION (CONT.)

Location Services now:

Location-based GPS/traffic info:

Range query: How many cars in the free way

Shortest path query: What is the estimated travel time to reach my destination



Location-based store finder:

Range query: What are the restaurants within five miles of my location

Nearest-neighbor query: Where is my nearest fast (junk) food restaurant

Location-based alerts /advertisement:

Range query: Send alerts to every cellphone user in 10 miles radius

Send E-coupons to all customers within five miles of my store



INTRODUCTION (CONT.)

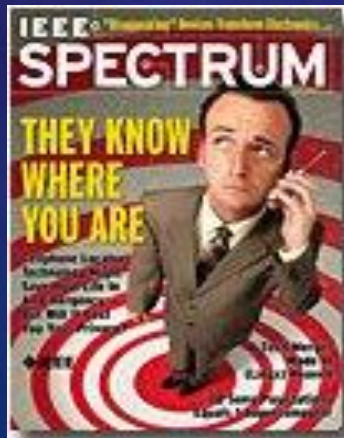
- Why we need the location services now?



- Location Privacy : Why now?
 - Do you use any of this devices
 - Ever felt that you are being tracked

“New technologies can pinpoint your location at any time and place. They promise safety and convenience but threaten privacy and security”


Cover story, IEEE Spectrum, July 2003



Threats

- **Tracking Threat:** Adversary can receive continuous location updates
- **Identification Threat:** Adversary can isolate the user's frequency
- **Profiling Threat:** Adversary can profile the person based off where user has been

INTRODUCTION (CONT.)



Why still we
want to use
location based
services?

- To make everyday life **easier**.
- To **find places** – Where is the nearest “Starbucks” ?
- To **go places** faster – Find the quickest route to my work ?
- Learn about your **surrounding attractions** – Find the must see places near me?

PROJECT SPECIFICATION

□ *What User Wants?*

*Use location-based services
without revealing
their private location information*

PROJECT SPECIFICATION (CONT.)

- To handle the request from the app
- If the request includes a single location, the service will response the Starbucks store closest to the location included in the request
- If the request contains an area, the service will return all Starbucks stores in that area.
- Once the response is delivered back to the Android app, the requester will be able to see the Starbucks store(s) on the map embedded in the app as well as his real current location.
- Then he can choose the store really closest to him.

PROJECT SPECIFICATION (CONT.)

Options user can choose from the android application for hiding their own location.

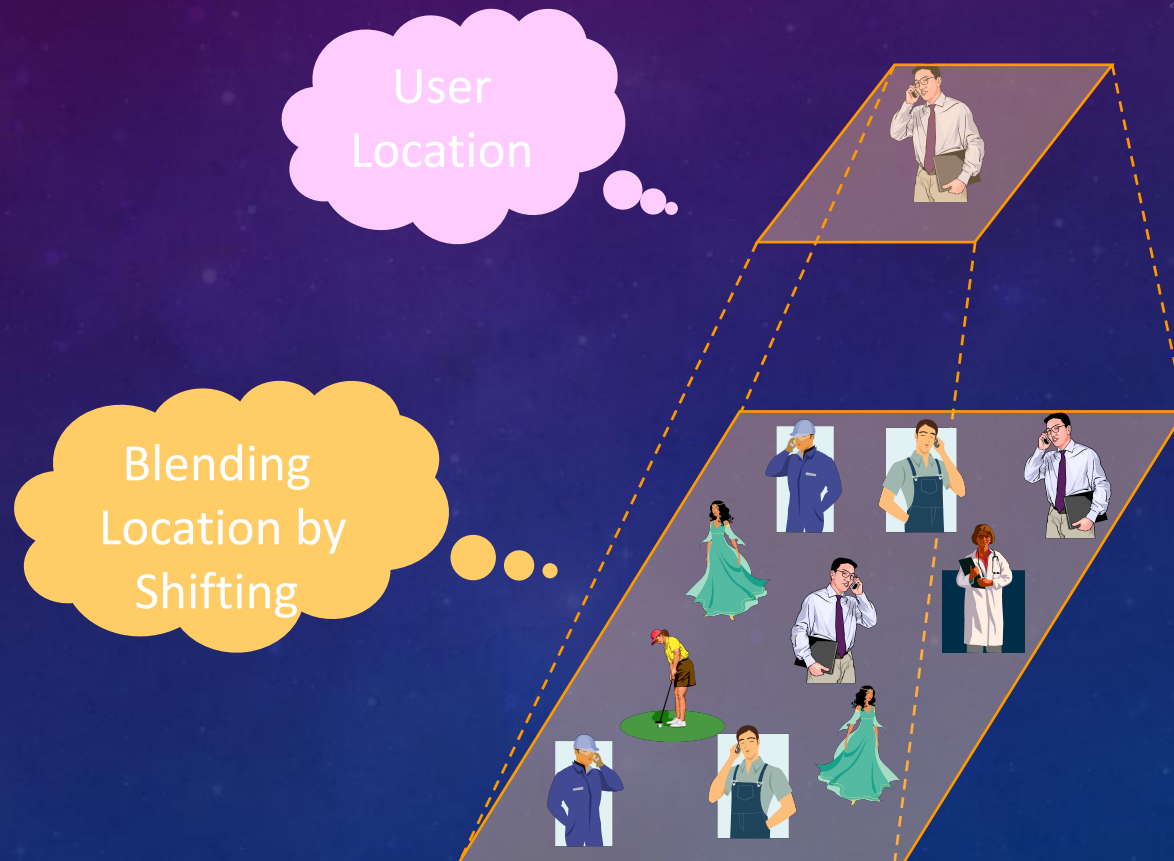
1. No anonymization.
2. Location information manipulated by shifting it a little
3. Send a square area instead of a single point.



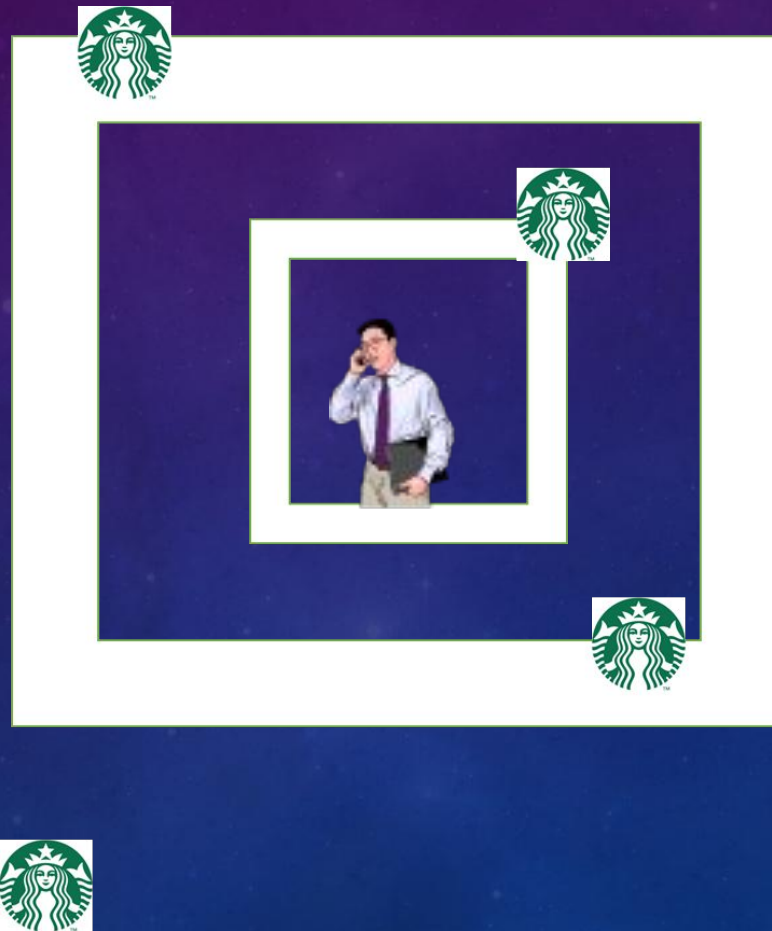
METHODS USED:

1. **No anonymization** : Users current location is used

2. LOCATION INFORMATION MANIPULATED BY SHIFTING IT A LITTLE :

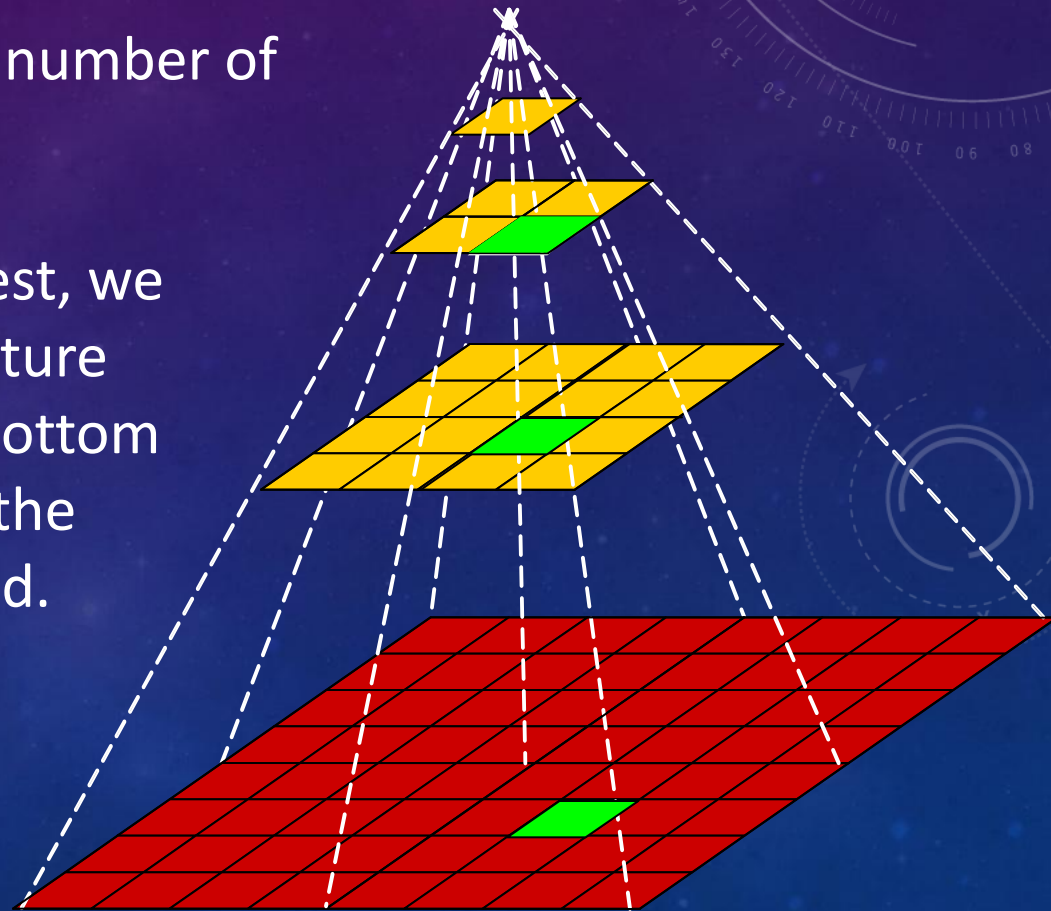


3. SEND A SQUARE AREA INSTEAD OF A SINGLE POINT. PYRAMID STRUCTURE



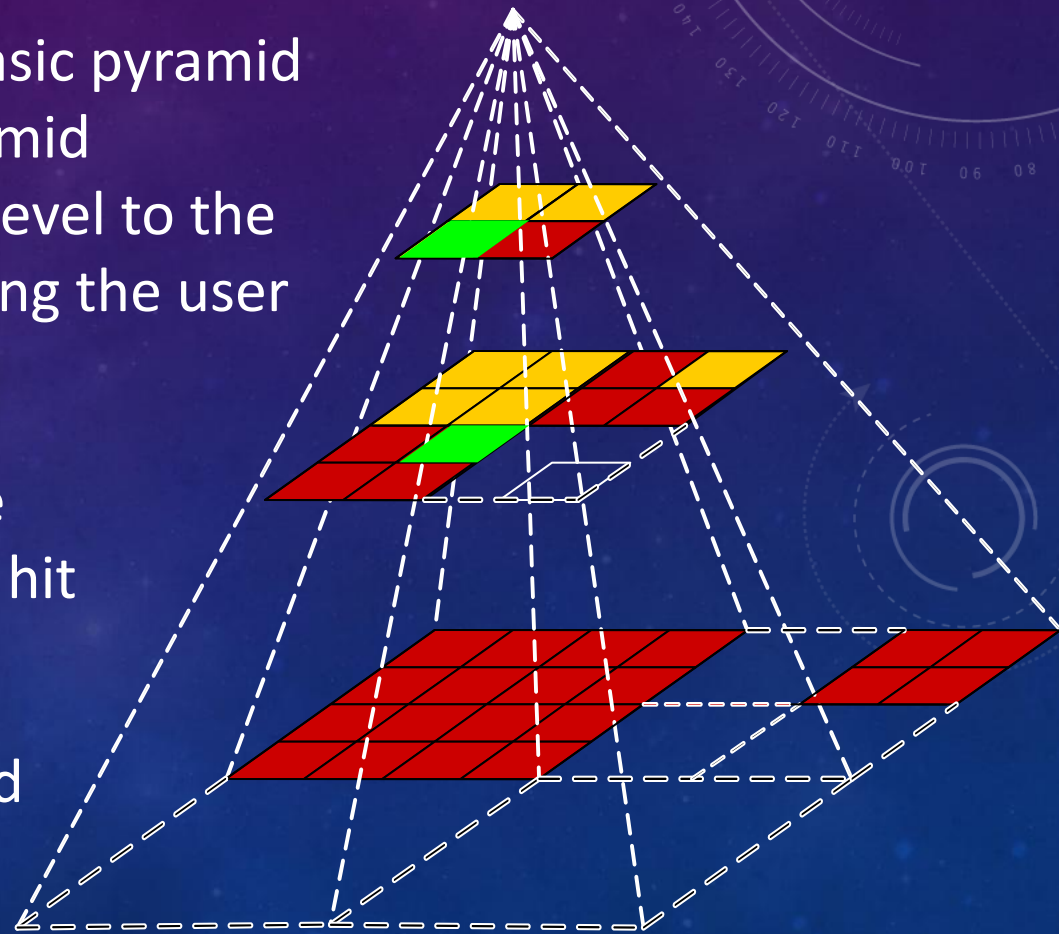
PYRAMID STRUCTURE

- The entire system area is represented as a *complete pyramid* structure divided into grids at different levels of various resolution
- Each grid cell maintains the number of users in that cell
- To anonymize a user request, we traverse the pyramid structure from the top level to the bottom level until a cell satisfying the user privacy profile is found.



ADAPTIVE PYRAMID STRUCTURE

- Instead of maintaining all pyramid cells, we maintain only those cells that are potential cloaked regions
- Similar to the case of the basic pyramid structure, traverse the pyramid structure from the bottom level to the top level, until a cell satisfying the user privacy profile is found.
- Most likely we will find the cloaked region in only one hit
- Scalable. Less overhead in maintaining grid cells. Need maintenance algorithms

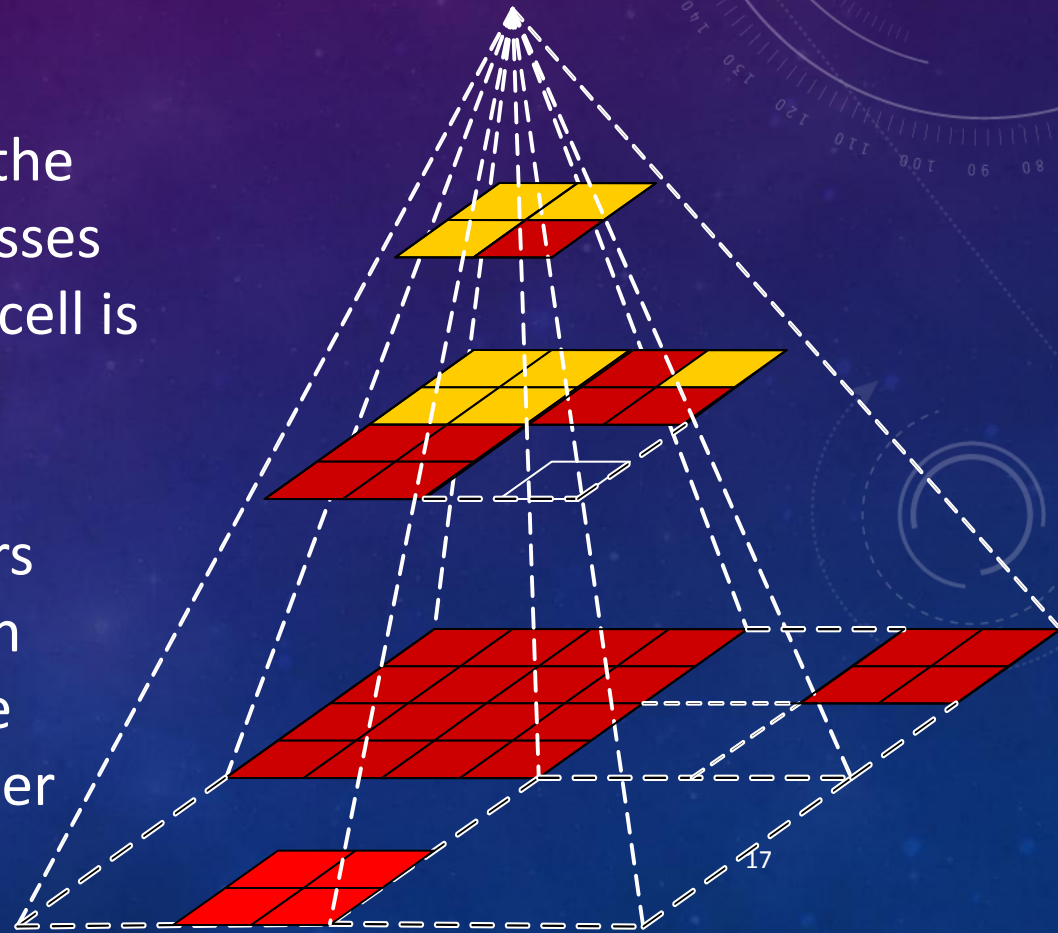


ADAPTIVE PYRAMID STRUCTURE: MAINTENANCE

- To guarantee its efficiency, the adaptive pyramid structure dynamically adjusts its maintained cells based on users' mobility

- **Cell Splitting:** Once one of the users in a certain cell expresses relaxed privacy profile, the cell is split into four lower cells

- **Cell Merging:** Once all users within certain cells strength their privacy profiles, those cells can be merged together



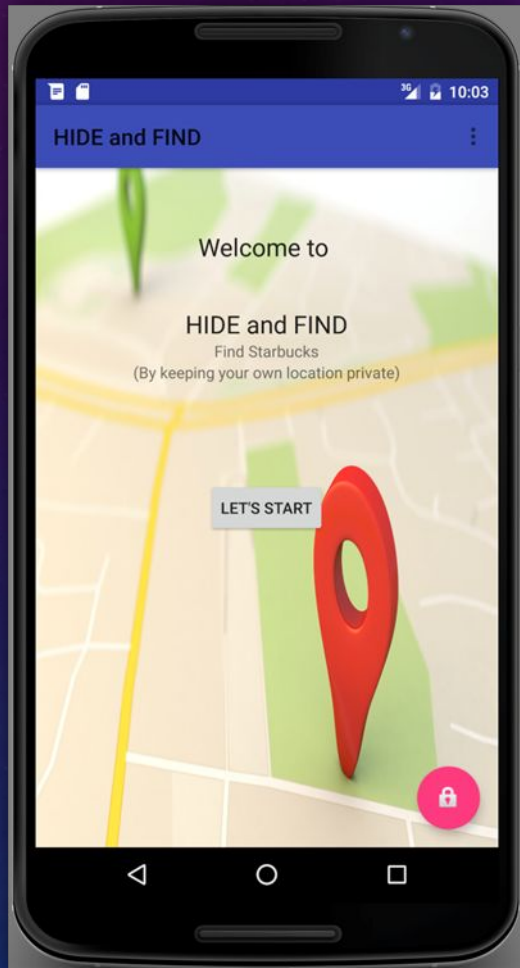
Tools and Programming language used

- Android Studio v.2.0 –JAVA and XML
- Google API

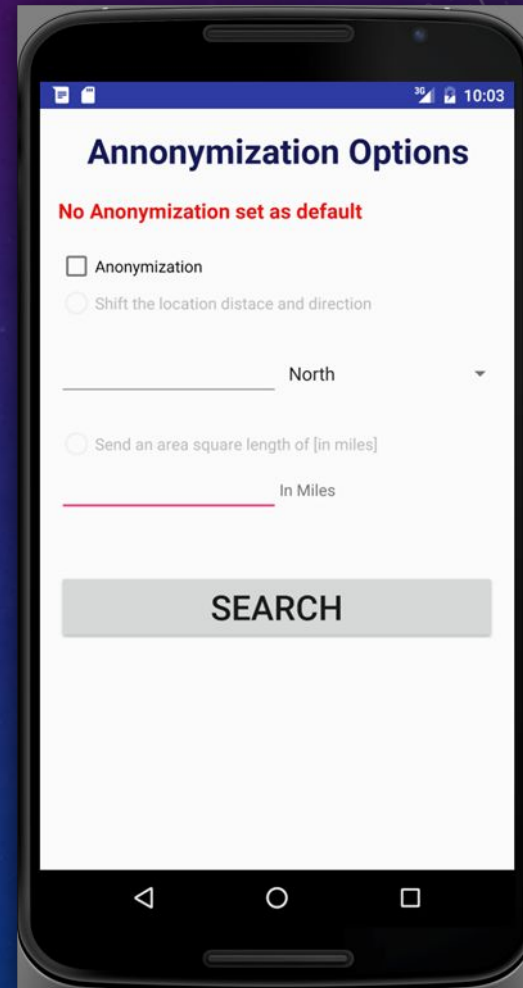
PROJECT ACCOMPLISHMENT

What we have done so far?

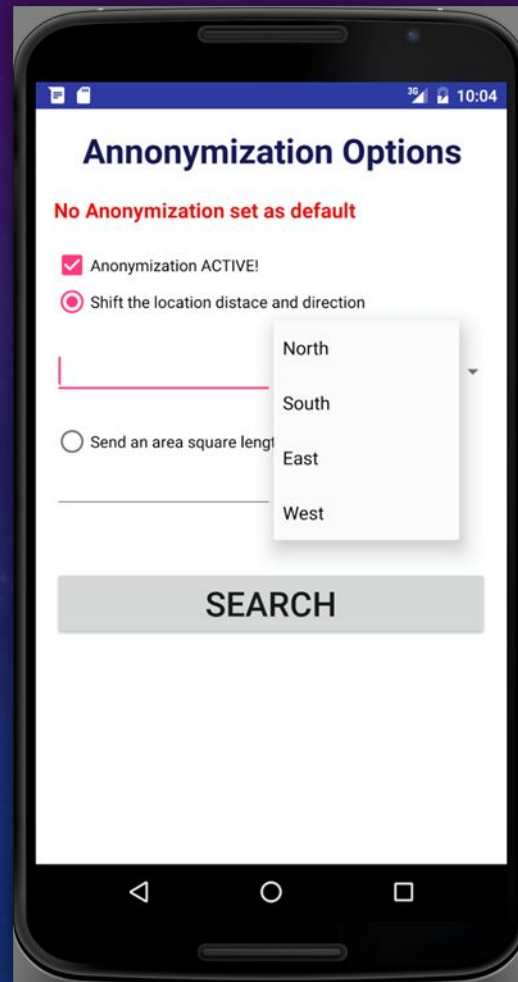
FRONT PAGE OF THE APP



NO ANONYMIZATION SELECTED (AS DEFAULT)



Shifting the location distance and direction towards North, South, East or West (user inputs the data)



SENDING A SQUARE RADIUS TO GET THE NEAREST LOCATIONS

10:04

Anonymization Options

No Anonymization set as default

☒ Anonymization ACTIVE!

☐ Shift the location distance and direction

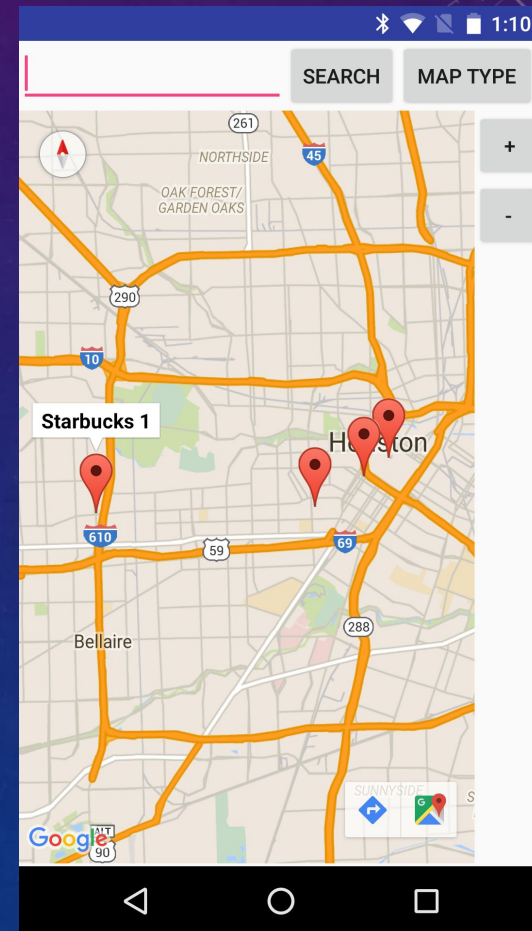
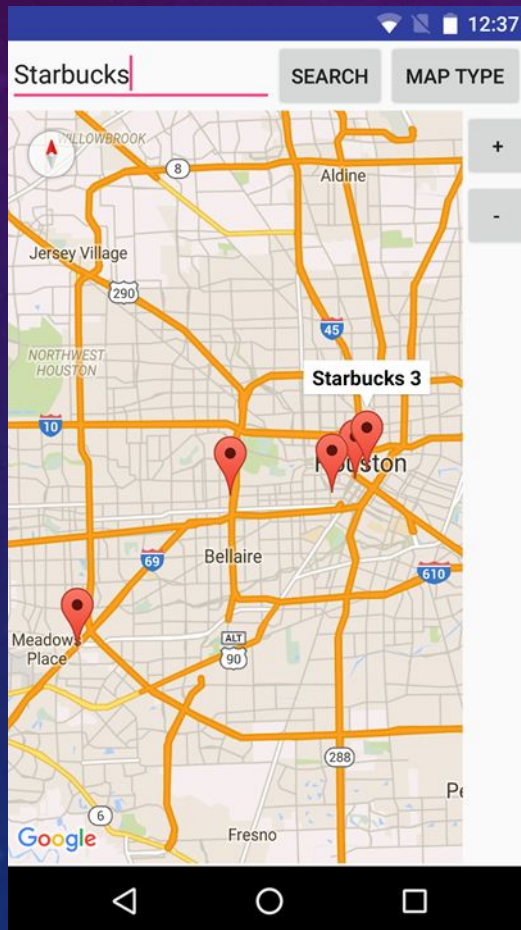
North

☒ Send an area square length of [in miles]

In Miles

SEARCH

RESULTS SHOWING STARBUCKS LOCATIONS NEARBY HOUSTON



CHALLENGES

- Configuring Google API with current versions of Android OS
- Creating server-client connection using tomcat8 and android studio
- Creating database using tomcat8 (using xamp would have been much easier)

CONCLUSION

- ❑ Location privacy is a major obstacle in ubiquitous deployment of location-based services
- ❑ Major privacy threats with real life scenarios are currently taking place due to the use of location-detection devices
- ❑ Several social studies indicate that users become more aware about their privacy

CONCLUSION (CONTINUE)

- ❑ Location privacy is significantly different from database privacy as the aim to protect incoming data and queries not the stored data
- ❑ Three main architectures for location anonymization: client-server architecture, third trusted party architecture, and peer-to-peer architecture.
- ❑ Probabilistic query processors and querying uncertain data approaches can be utilized to support privacy-aware query processors.
- ❑ Using the methods discussed we can successfully blur the user location so that the attacker can not find the exact location of the user because users location is blurred in to the mix of other users using POI based services.

FUTURE WORK :

- Search feature to search all destinations. Navigation within the application.
- Option to securely send the current location and directions to other known person.
- Option to save map offline for desired time duration.
- Implement algorithm to check the integrity of installed android application database periodically to ensure that it is not been corrupted and hacked by other applications.
- A formal definition for the optimal spatial cloaked regions
- Developing workload benchmark to be used for comparison of various anonymization techniques.

FUTURE WORK : (CONTINUED)

- Measures of comparison would be scalability, efficiency in terms of time, close-to-optimal cloaked regions
- Developing new algorithms that support various user requirements
- Making the anonymization process ubiquitous within the user device by utilizing cached data at the user side
- Adding more anonymization options
 1. Low privacy
 2. Medium privacy. Using the internet for loading map data and GPS for location.
 3. High privacy- offline maps with multiple queries to get the direction to the desired POI.

REFERENCES

- <http://developer.android.com/develop/index.html>
- ABI Research. GPS-Enabled Location-Based Services (LBS) Subscribers Will Total 315 Million in Five Years. <http://www.abiresearch.com/abiprdisplay.jsp?pressid=731> September, 27, 2006.
- Osman Abul, Francesco Bonchi, Mirco Nanni: Never Walk Alone: Uncertainty for Anonymity in Moving Objects Databases. ICDE 2008: 376-385
- Linda Ackerman, James Kempf, and Toshio Miki. Wireless location privacy: A report on law and policy in the united states, the european union, and japan. Technical Report DCL-TR2003-001, DoCoMo Communication Laboratories, USA, 2003.
- Mikhail J. Atallah and Keith B. Frikken. Privacy-Preserving Location-Dependent Query Processing. In Proceeding of the IEEE/ACS International Conference on Pervasive Services, ICPS, pages 9–17, Beirut, Lebanon, July 2004.
- Bhuvan Bamba, Ling Liu, Péter Pesti, Ting Wang: Supporting anonymous location queries in mobile environments with privacy grid. WWW 2008: 237-246.

SO ... DO YOU HAVE ANY
QUESTIONS FOR ME?

