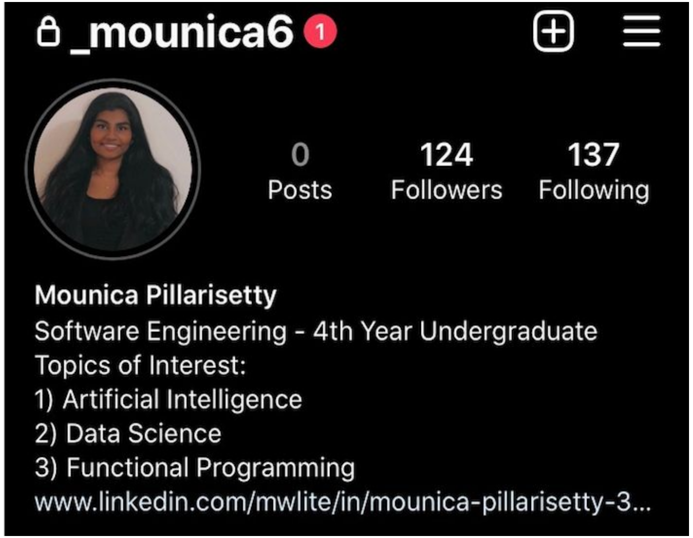
Carleton UNIVERSITY | FACULTY OF Engineering and Design

# Mitigating Inference Attacks on Social Networking Platforms

Mounica Pillarisetty
Sarah Lamonica
Shoana Sharma



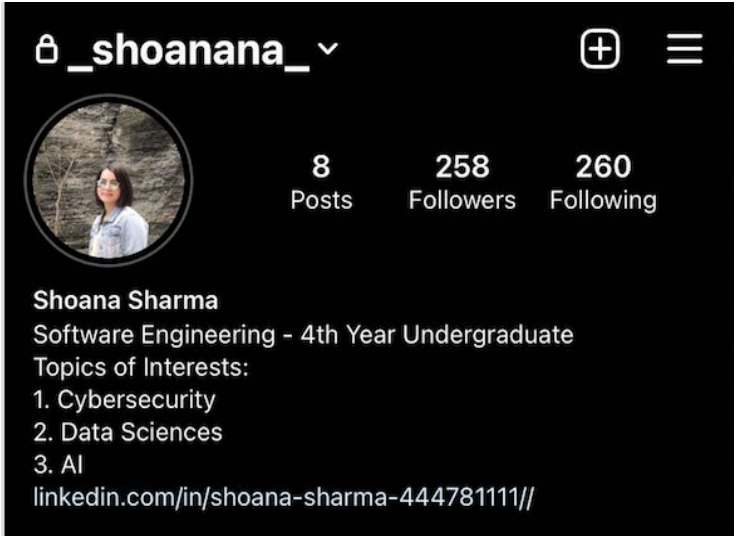
_mounica6

0 Posts

124 Followers

137 Following

**Mounica Pillarisetty**
Software Engineering - 4th Year Undergraduate
Topics of Interest:
1) Artificial Intelligence
2) Data Science
3) Functional Programming
www.linkedin.com/mwlite/in/mounica-pillarisetty-3...



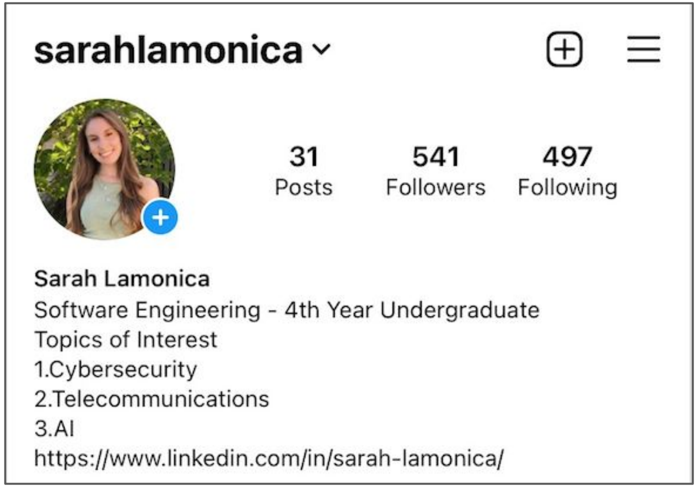
_shoanana_

8 Posts

258 Followers

260 Following

**Shoana Sharma**
Software Engineering - 4th Year Undergraduate
Topics of Interests:
1. Cybersecurity
2. Data Sciences
3. AI
linkedin.com/in/shoana-sharma-444781111//



sarahlamonica

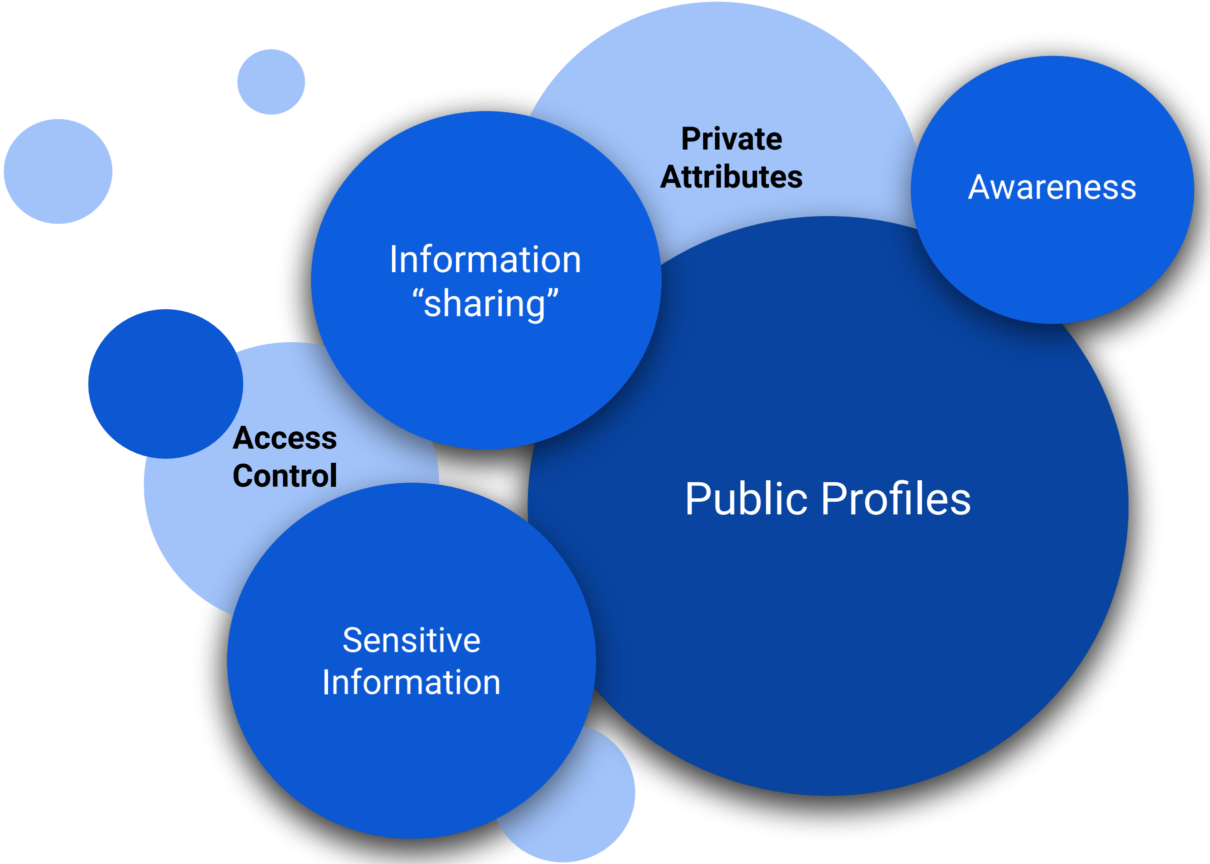
31 Posts

541 Followers

497 Following

**Sarah Lamonica**
Software Engineering - 4th Year Undergraduate
Topics of Interest
1.Cybersecurity
2.Telecommunications
3.AI
https://www.linkedin.com/in/sarah-lamonica/

# Our Motivation



Private Attributes

Awareness

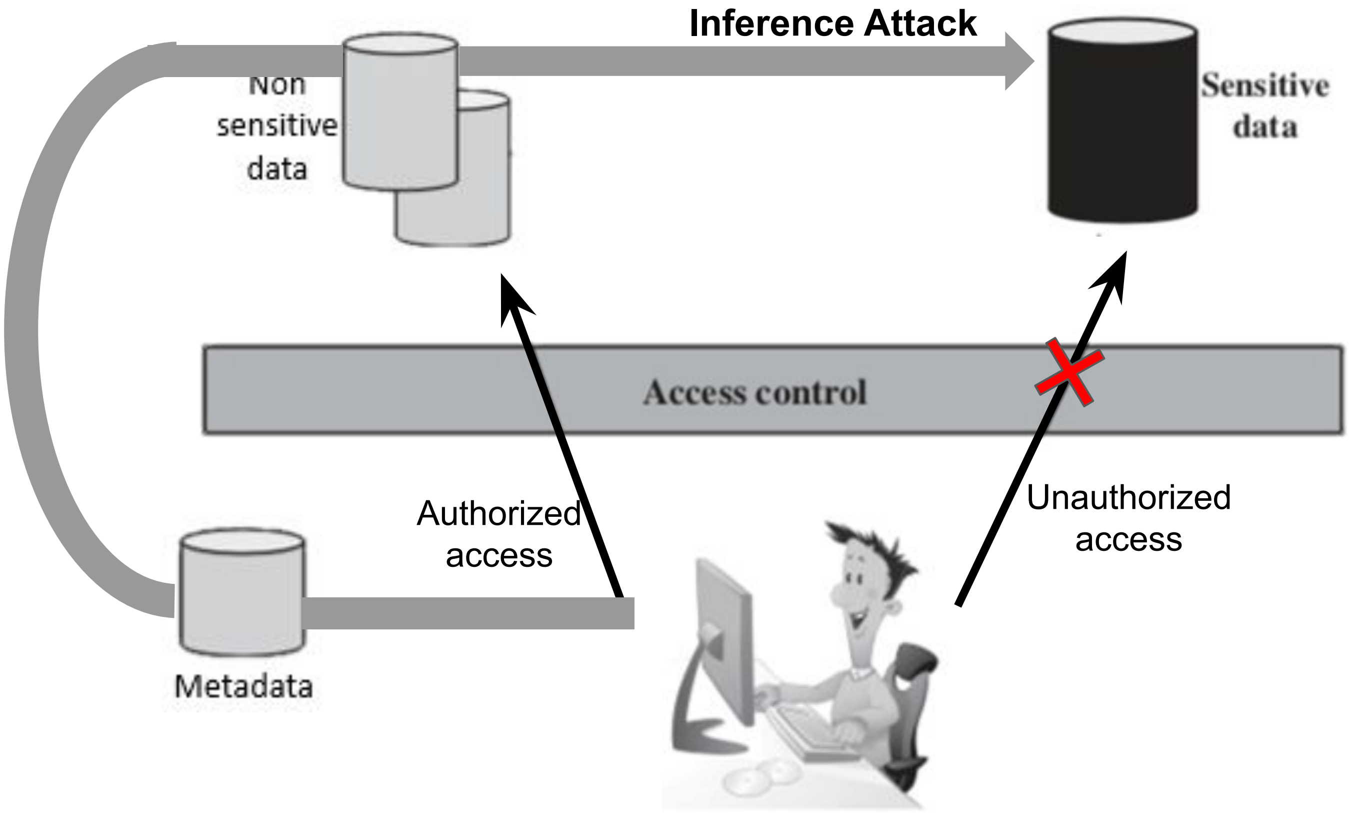
Information “sharing”

Public Profiles

Access Control

Sensitive Information

# Inference Attack



# Problem Statement

To build a system that can support **confidentiality preservation** in social media datasets by **identifying** when sensitive information can be inferred from such data using predefined **security policies**.

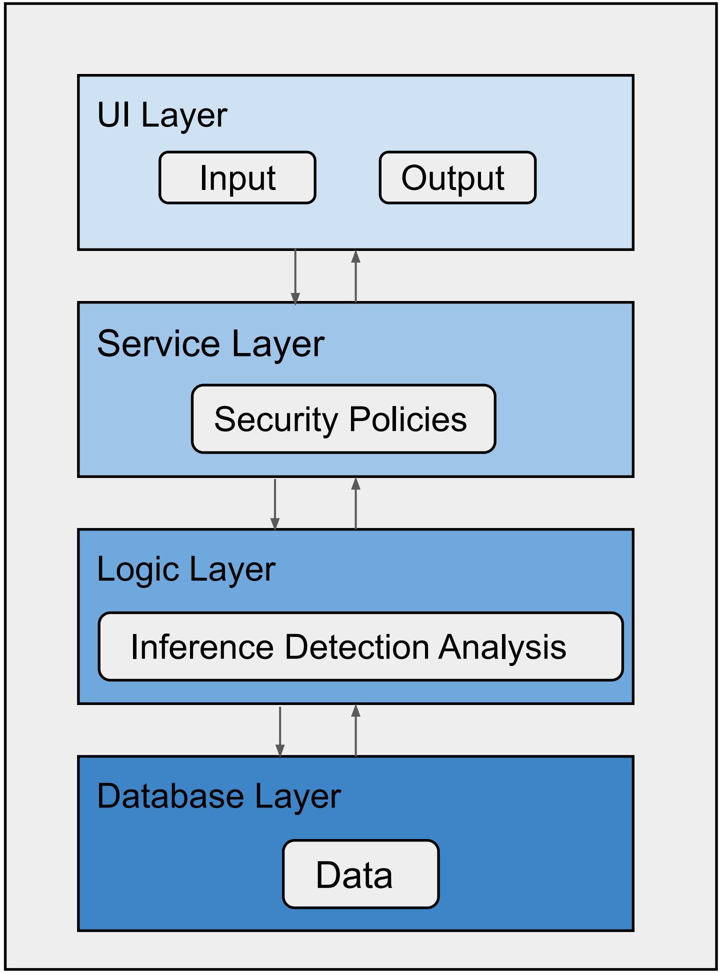
# Objective

Provide users with insightful information about their social media data and the various sensitive information that is prone to an inference attack

# Background

- Countermeasures:
  - Partitioning
  - Polyinstantiation
- Related Work:
  - Sina Weibo

# Layer Pattern



UI Layer

Input

Output

Service Layer

Security Policies

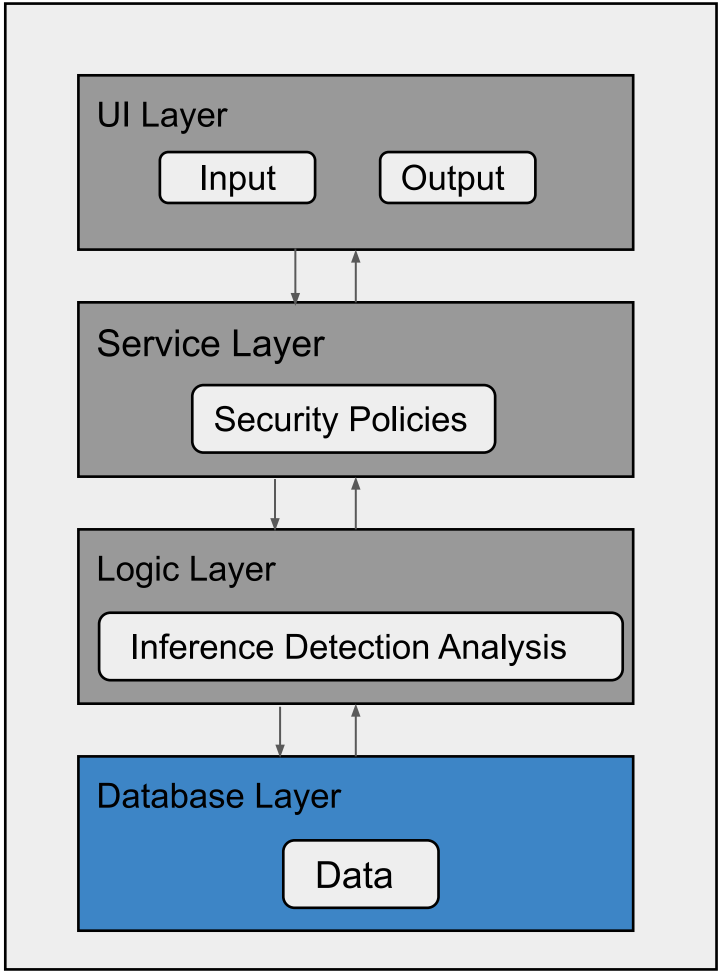
Logic Layer

Inference Detection Analysis

Database Layer

Data

# Layer Pattern



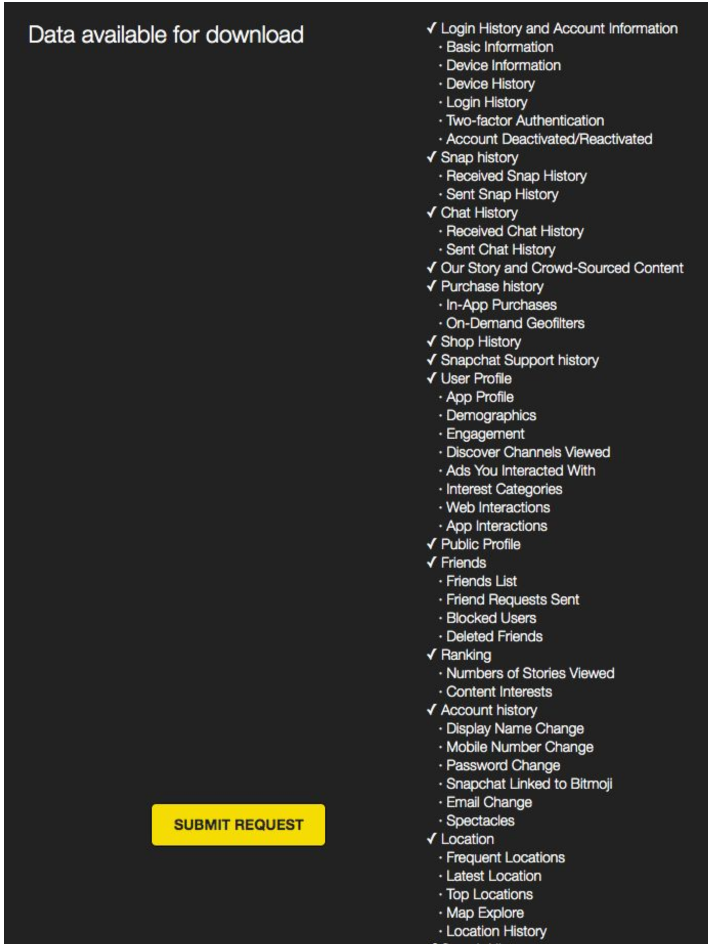
# Data Collection

- Person data is collected through **three social media sites**:

- Requested individually for each member
  - Enough data to conduct a thorough analysis

# Snapchat

- Snap History
- Chat History
- User Profile
- Friends
- Location History

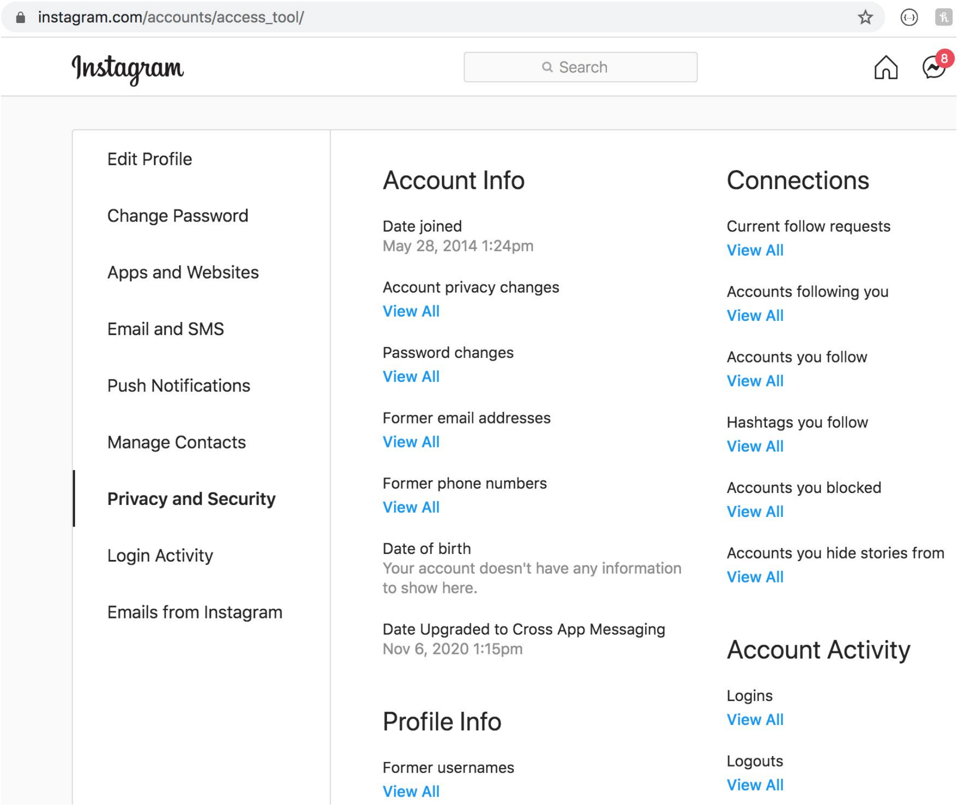


Data available for download

✓ Login History and Account Information
· Basic Information
· Device Information
· Device History
· Login History
· Two-factor Authentication
· Account Deactivated/Reactivated
✓ Snap history
· Received Snap History
· Sent Snap History
✓ Chat History
· Received Chat History
· Sent Chat History
✓ Our Story and Crowd-Sourced Content
✓ Purchase history
· In-App Purchases
· On-Demand Geofilters
✓ Shop History
✓ Snapchat Support history
✓ User Profile
· App Profile
· Demographics
· Engagement
· Discover Channels Viewed
· Ads You Interacted With
· Interest Categories
· Web Interactions
· App Interactions
✓ Public Profile
✓ Friends
· Friends List
· Friend Requests Sent
· Blocked Users
· Deleted Friends
✓ Ranking
· Numbers of Stories Viewed
· Content Interests
✓ Account history
· Display Name Change
· Mobile Number Change
· Password Change
· Snapchat Linked to Bitmoji
· Email Change
· Spectacles
✓ Location
· Frequent Locations
· Latest Location
· Top Locations
· Map Explore
· Location History

# Instagram

- Logins
- Logouts
- Accounts Following
- Messages



instagram.com/accounts/access_tool/

Edit Profile

Change Password

Apps and Websites

Email and SMS

Push Notifications

Manage Contacts

**Privacy and Security**

Login Activity

Emails from Instagram

## Account Info

Date joined
May 28, 2014 1:24pm

Account privacy changes
View All

Password changes
View All

Former email addresses
View All

Former phone numbers
View All

Date of birth
Your account doesn't have any information to show here.

Date Upgraded to Cross App Messaging
Nov 6, 2020 1:15pm

## Profile Info

Former usernames
View All

## Connections

Current follow requests
View All

Accounts following you
View All

Accounts you follow
View All

Hashtags you follow
View All

Accounts you blocked
View All

Accounts you hide stories from
View All

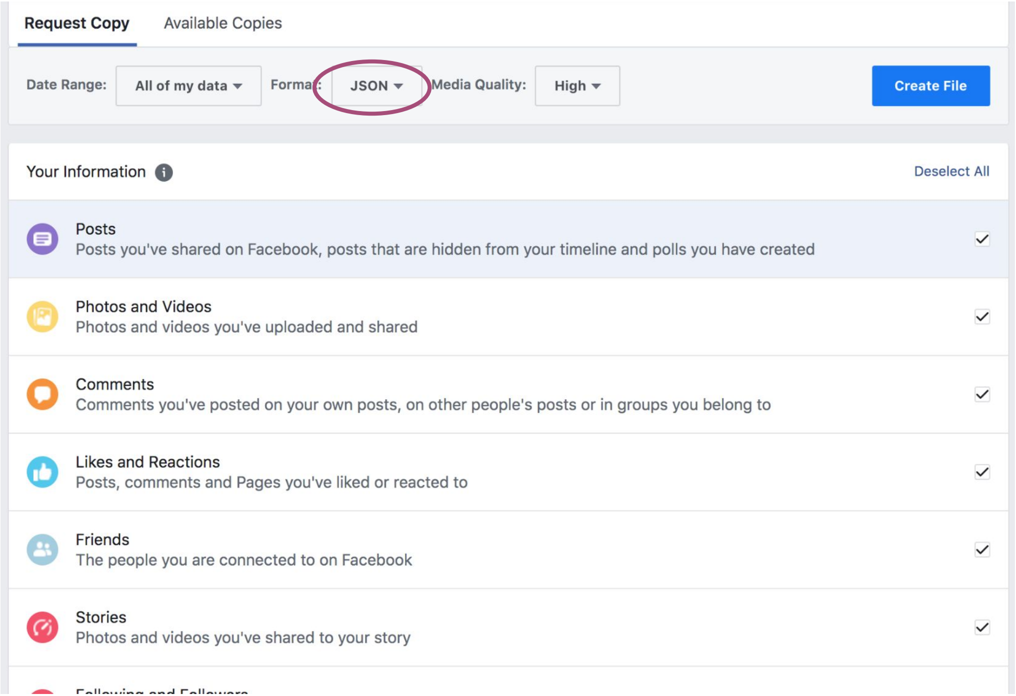
## Account Activity

Logins
View All

Logouts
View All

# Facebook

- Location History
- Events
- Messages
- Friends
- Logins
- Logouts



Request Copy   Available Copies

Date Range: All of my data ▾   Format: JSON ▾   Media Quality: High ▾   Create File

Your Information   Deselect All

Posts
Posts you've shared on Facebook, posts that are hidden from your timeline and polls you have created ✓

Photos and Videos
Photos and videos you've uploaded and shared ✓

Comments
Comments you've posted on your own posts, on other people's posts or in groups you belong to ✓

Likes and Reactions
Posts, comments and Pages you've liked or reacted to ✓

Friends
The people you are connected to on Facebook ✓

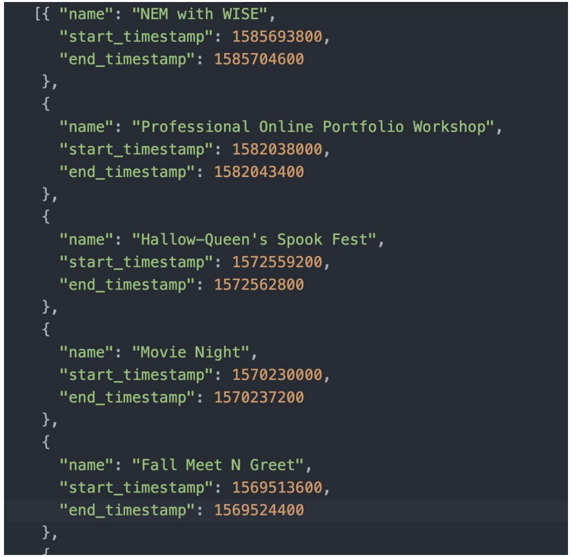
Stories
Photos and videos you've shared to your story ✓

Following and Followers

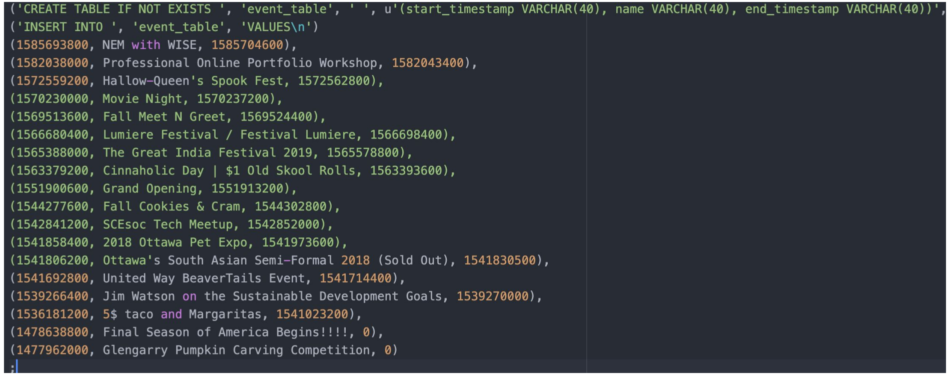
# Data Cleansing

- Data type: Json files
  - Large file sets

- Created Scripts
  - Removes extra spaces
  - Same headers for all social media sites
    - Same queries can be utilised



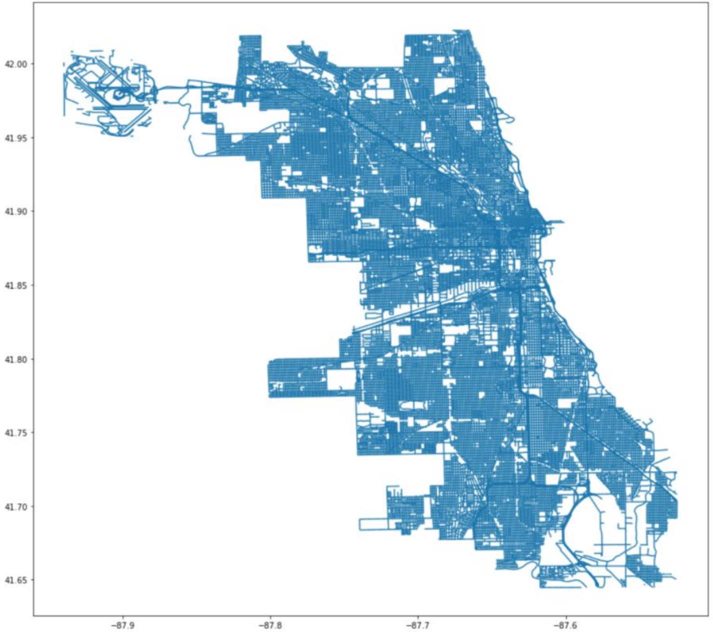
```
[{ "name": "NEM with WISE",
    "start_timestamp": 1585693800,
    "end_timestamp": 1585704600
  },
  {
    "name": "Professional Online Portfolio Workshop",
    "start_timestamp": 1582038000,
    "end_timestamp": 1582043400
  },
  {
    "name": "Hallow-Queen's Spook Fest",
    "start_timestamp": 1572559200,
    "end_timestamp": 1572562800
  },
  {
    "name": "Movie Night",
    "start_timestamp": 1570230000,
    "end_timestamp": 1570237200
  },
  {
    "name": "Fall Meet N Greet",
    "start_timestamp": 1569513600,
    "end_timestamp": 1569524400
  },
```



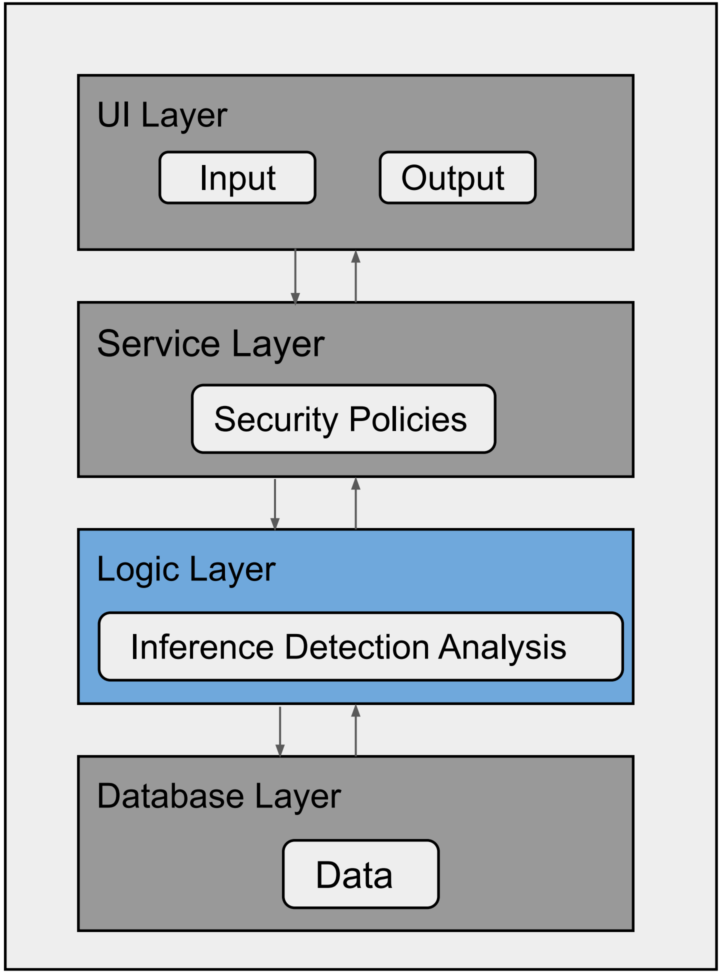
```
('CREATE TABLE IF NOT EXISTS ', 'event_table', ' ', u'(start_timestamp VARCHAR(40), name VARCHAR(40), end_timestamp VARCHAR(40))',
('INSERT INTO ', 'event_table', 'VALUES\n')
(1585693800, NEM with WISE, 1585704600),
(1582038000, Professional Online Portfolio Workshop, 1582043400),
(1572559200, Hallow-Queen's Spook Fest, 1572562800),
(1570230000, Movie Night, 1570237200),
(1569513600, Fall Meet N Greet, 1569524400),
(1566680400, Lumiere Festival / Festival Lumiere, 1566698400),
(1565388000, The Great India Festival 2019, 1565578800),
(1563379200, Cinnaholic Day | $1 Old Skool Rolls, 1563393600),
(1551900600, Grand Opening, 1551913200),
(1544277600, Fall Cookies & Cram, 1544302800),
(1542841200, SCEsoc Tech Meetup, 1542852000),
(1541858400, 2018 Ottawa Pet Expo, 1541973600),
(1541806200, Ottawa's South Asian Semi-Formal 2018 (Sold Out), 1541830500),
(1541692800, United Way BeaverTails Event, 1541714400),
(1539266400, Jim Watson on the Sustainable Development Goals, 1539270000),
(1536181200, 5$ taco and Margaritas, 1541023200),
(1478638800, Final Season of America Begins!!!!, 0),
(1477962000, Glengarry Pumpkin Carving Competition, 0)
;
```

# Pandas

- Converts JSON data easily into a database
- Query the database
- Metrics
- Tabulate results

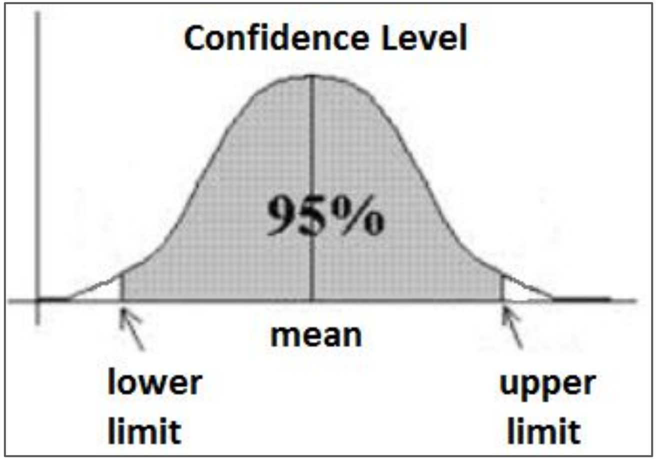


# Layer Pattern

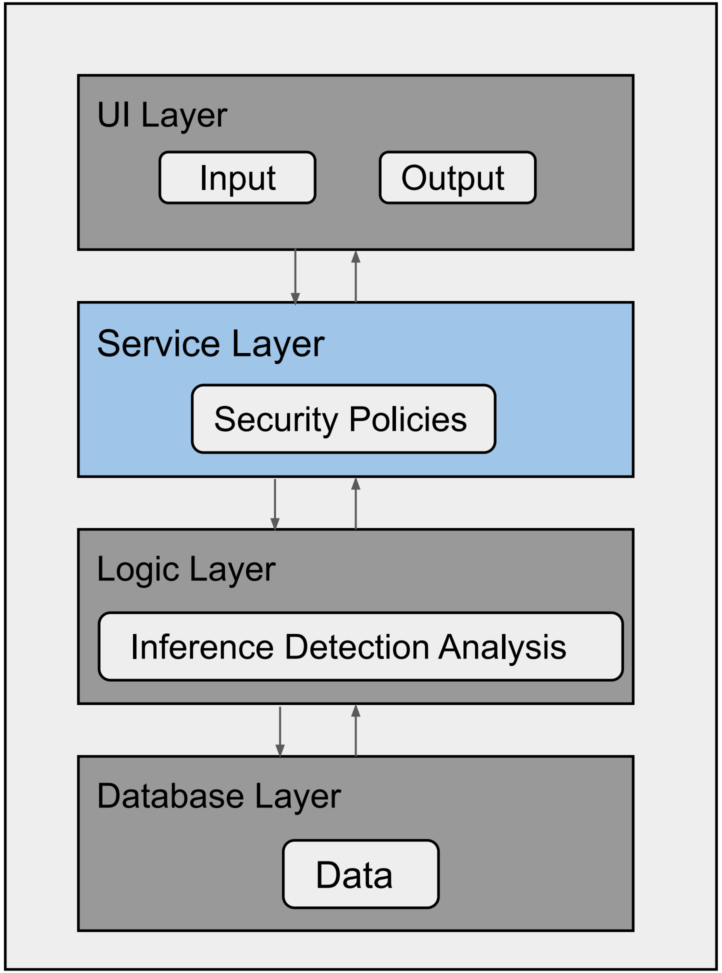


# Inference Detection Analysis

- Metrics
  - Confidence Intervals: Percentage based on the sample space for true mean
  - Analysing Results through queries

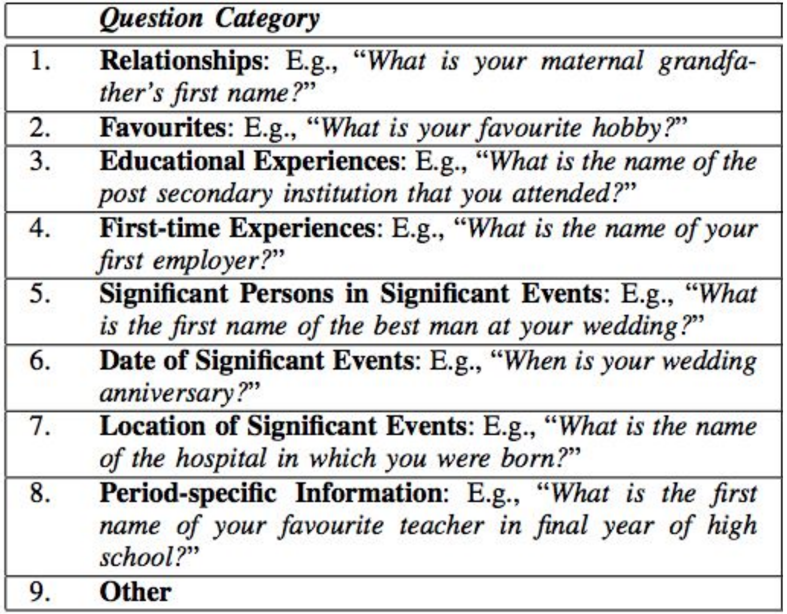


# Layer Pattern



# Preliminary Research

- Top security questions
  - Research paper from University of Calgary
  - Google search
  - Personal experiences



| | *Question Category* |
|---|---|
| 1. | **Relationships**: E.g., "*What is your maternal grandfather's first name?*" |
| 2. | **Favourites**: E.g., "*What is your favourite hobby?*" |
| 3. | **Educational Experiences**: E.g., "*What is the name of the post secondary institution that you attended?*" |
| 4. | **First-time Experiences**: E.g., "*What is the name of your first employer?*" |
| 5. | **Significant Persons in Significant Events**: E.g., "*What is the first name of the best man at your wedding?*" |
| 6. | **Date of Significant Events**: E.g., "*When is your wedding anniversary?*" |
| 7. | **Location of Significant Events**: E.g., "*What is the name of the hospital in which you were born?*" |
| 8. | **Period-specific Information**: E.g., "*What is the first name of your favourite teacher in final year of high school?*" |
| 9. | **Other** |

- Location information
  - Longitude - Latitude

# Security Policies

| Security Policy | Queries |
|---|---|
| Common Security Question: The hometown of an individual is determined based on location during Christmas day | dataframe[dataframe['Time'].str.contains("12/25")] |
| Common Security Question: The hometown of an individual is determined based on location during Thanksgiving day | dataframe[dataframe['Time'].str.contains("10/12")] |
| The home address of an individual is determined based on most frequent location | dataframe['Latitude, Longitude'].value_counts().idxmax() |
| The work address of an individual is determined based on secondary most frequent location | dataframe['Latitude, Longitude'].value_counts().idxmax() |
| Common Security Question: The hobby of an individual is determined based on most common nouns used | [word for word, word_count in Counter(nouns).most_common(3)] |
| Special occasions are determined based on typical congratulatory conversation on important dates | [word for word, word_count in Counter(nouns).most_common(3)] |
| Common Security Question: The pet name of an individual is determined based on most common nouns used | [word for word, word_count in Counter(nouns).most_common(3)] |
| Relationships between individuals is determined based on nouns extracted from conversation | [word for word, word_count in Counter(nouns).most_common(3)] |

**Security Policy #1:** The hometown of an individual is determined based on location during Christmas day

### Why is it deemed sensitive information?

- Common security question
  - Inferred family home
  - Inferred family relationship

### Query Representation:

```
dataframe[dataframe['Time'].str.contains("12/25")]
```

Christmas day

**Security Policy #2:** The hometown of an individual is determined based on location during Thanksgiving day

**Why is it deemed sensitive information?**

- Common security question
  - Inferred Family home
  - Inferred Family relationship

**Query Representation:**

```
dataframe[dataframe['Time'].str.contains("10/12")]
```

Thanksgiving day for 2020

**Security Policy #3:** The home address of an individual is determined based on most frequent location

**Why is it deemed sensitive information?**

- Inferred home address
  - Most data hits through location history

**Query Representation:**

dataframe['Latitude, Longitude'].value_counts().idxmax()

**Security Policy #4:** The work address of an individual is determined based on <u>secondary most frequent location</u>

**Why is it deemed sensitive information?**

- Inferred from second most data hits of location history
- From 9 A.M. to 5 P.M.

**Query Representation:**
dataframe['Latitude, Longitude'].value_counts().idxmax()

**Security Policy #5:** The hobby of an individual is determined based on most common nouns used

**Why is it deemed sensitive information?**

- Common security question
- Natural Language Processing:
  - Branch of artificial intelligence
  - Deals with the human computer interaction through natural language
  - Noun extraction

**Query Representation:**

```
[word for word, word_count in Counter(nouns).most_common(3)]
```

**Security Policy #6:** Special occasions are determined based on typical congratulatory conversation on important dates

**Why is it deemed sensitive information?**

- Common security question
- Natural Language Processing
  - Noun extraction
- Inferred birthdays of spouses, children or anniversaries

**Query Representation:**

```
[word for word, word_count in Counter(nouns).most_common(3)]
```

**Security Policy #7:** The pet name of an individual is determined based on most common nouns used

**Why is it deemed sensitive information?**

- Common security question
- Natural Language Processing
  - Noun Extraction
- Inferred pet name through conversation, liked pages or profile tags

**Query Representation:**

```
[word for word, word_count in Counter(nouns).most_common(3)]
```

**Security Policy #8:** Relationships between individuals is determined based on nouns extracted from conversation

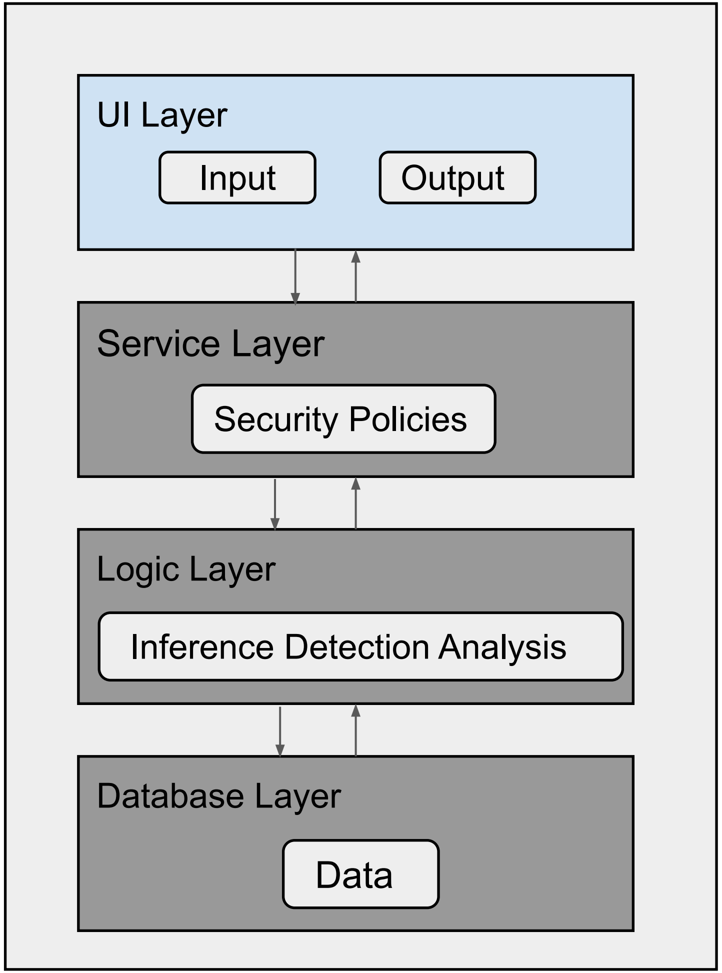
**Why is it deemed sensitive information?**

- Common security question
- Natural Language Processing
  - Noun Extraction
- Inferred through conversation, tagged profile, relationship status

**Query Representation:**

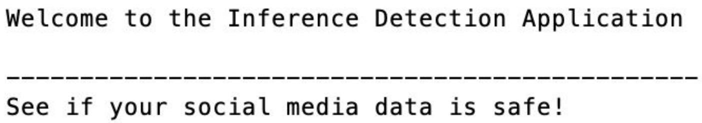
[word for word, word_count in Counter(nouns).most_common(3)]

# Layer Pattern



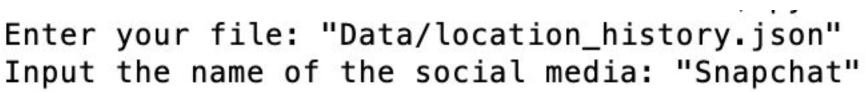
# Interface

Step 1:



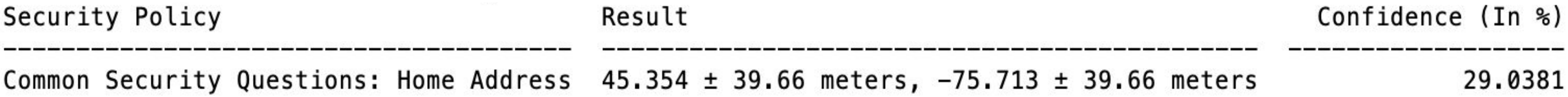
```
Welcome to the Inference Detection Application

-----------------------------------------------
See if your social media data is safe!
```

Step 2:



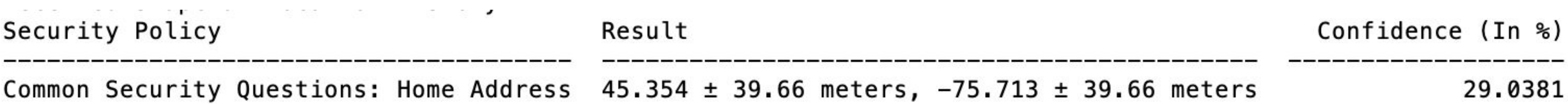
```
Enter your file: "Data/location_history.json"
Input the name of the social media: "Snapchat"
```

Step 3:



```
Security Policy                        Result                                          Confidence (In %)
-------------------------------------  ----------------------------------------------  ------------------
Common Security Questions: Home Address  45.354 ± 39.66 meters, -75.713 ± 39.66 meters              29.0381
```

# Analysis of Results

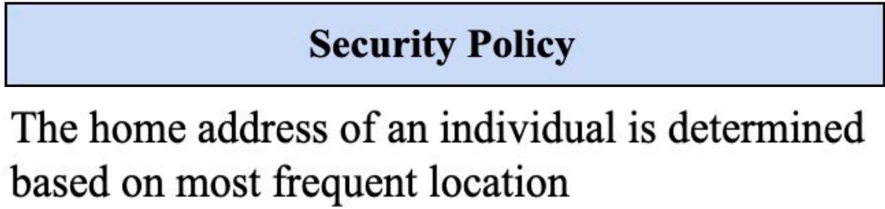


```
Security Policy                             Result                                              Confidence (In %)
-----------------------------------------   -------------------------------------------------   --------------------
Common Security Questions: Home Address     45.354 ± 39.66 meters, -75.713 ± 39.66 meters                    29.0381
```

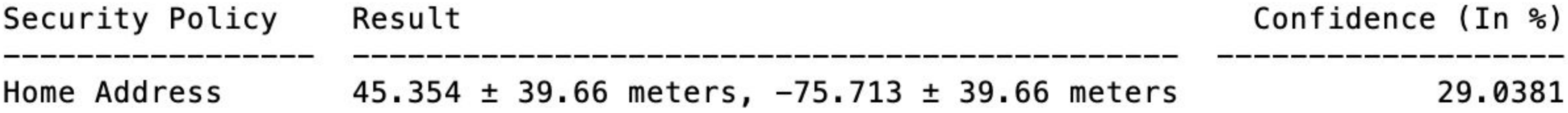
- A **result** is shown to demonstrate to the user exactly what the program has found when they perform a query on the data set.
- A **confidence value** is shown as a percentage. It is a metric to demonstrate to the user how confident the system is in determining the result.
  - Confidence = (Accepted Value) / (Total Values) x 100
- **Goal**: Inform the user when unauthorized information can be inferred by unauthorized parties.

# Demo

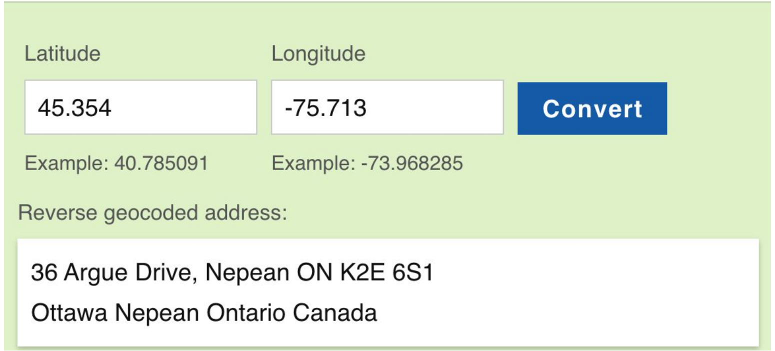
# Demo Result #1



| Security Policy |
|---|
| The home address of an individual is determined based on most frequent location |



```
Security Policy      Result                                          Confidence (In %)
-----------------    ---------------------------------------------   -------------------
Home Address         45.354 ± 39.66 meters, -75.713 ± 39.66 meters              29.0381
```



Latitude: 45.354

Example: 40.785091

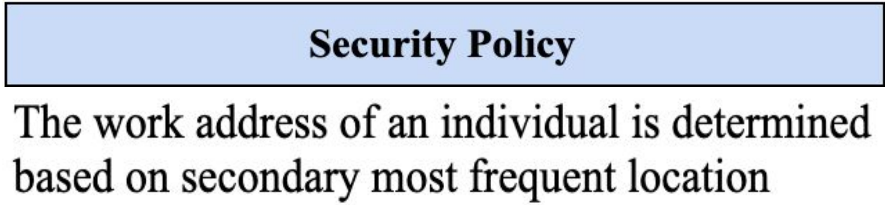
Longitude: -75.713

Example: -73.968285

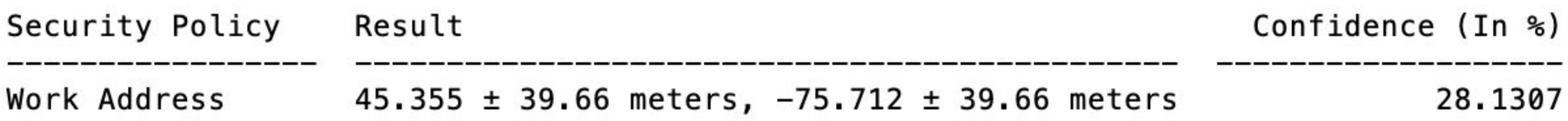
Reverse geocoded address:

36 Argue Drive, Nepean ON K2E 6S1
Ottawa Nepean Ontario Canada

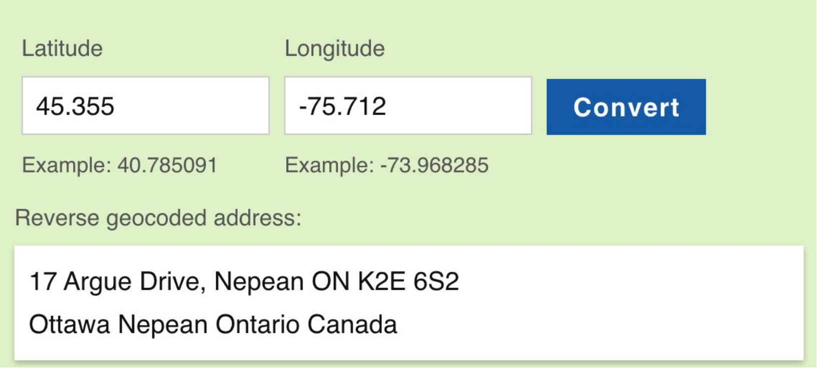
# Demo Result #2



| Security Policy |
|---|
| The work address of an individual is determined based on secondary most frequent location |



```
Security Policy    Result                                             Confidence (In %)
-----------------  -------------------------------------------------  -------------------
Work Address       45.355 ± 39.66 meters, -75.712 ± 39.66 meters                  28.1307
```



Latitude: 45.355

Longitude: -75.712

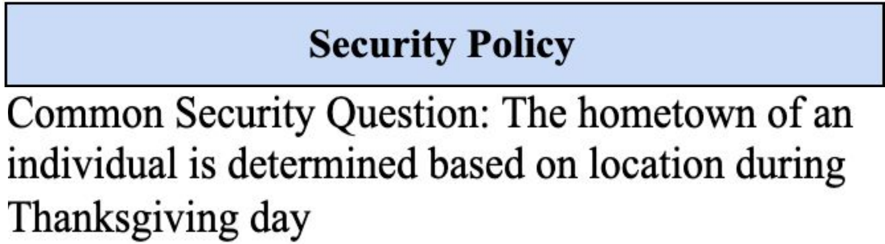
Example: 40.785091

Example: -73.968285

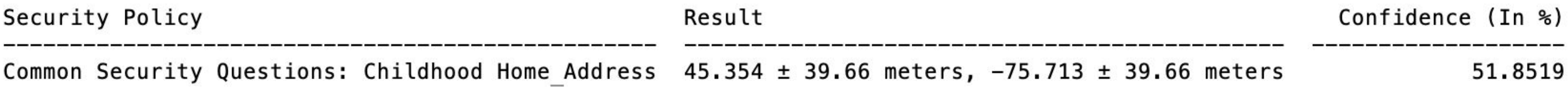
Reverse geocoded address:

17 Argue Drive, Nepean ON K2E 6S2
Ottawa Nepean Ontario Canada

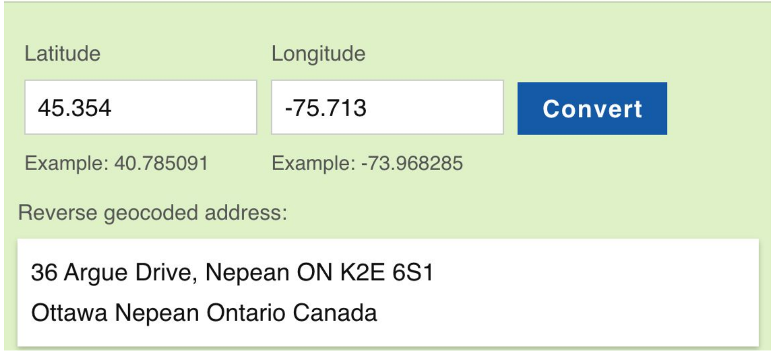
# Demo Result #3



| Security Policy |
|---|
| Common Security Question: The hometown of an individual is determined based on location during Thanksgiving day |



```
Security Policy                                    Result                                           Confidence (In %)
-------------------------------------------------  ---------------------------------------------  -------------------
Common Security Questions: Childhood Home_Address  45.354 ± 39.66 meters, -75.713 ± 39.66 meters              51.8519
```



Latitude: 45.354

Longitude: -75.713

Example: 40.785091

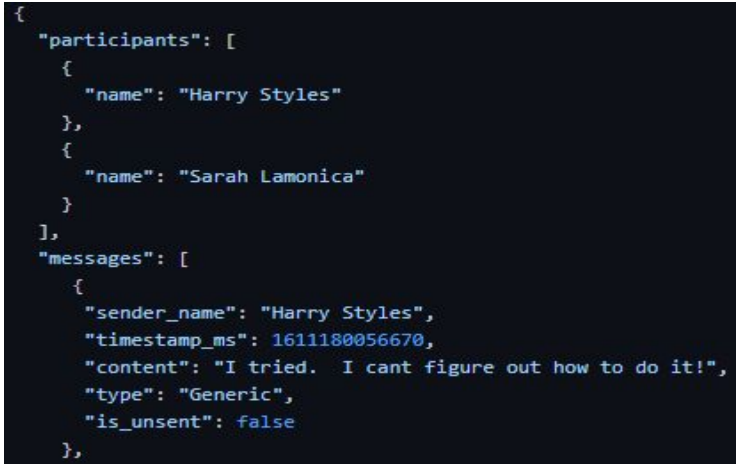
Example: -73.968285

Reverse geocoded address:

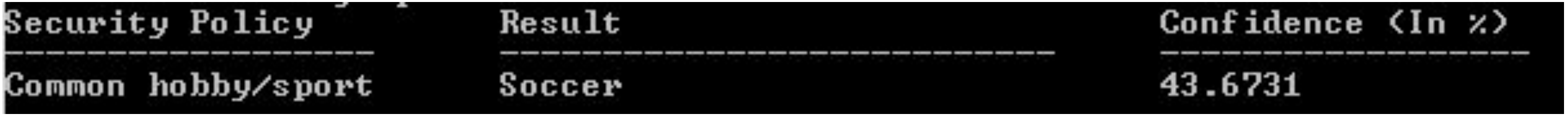
36 Argue Drive, Nepean ON K2E 6S1
Ottawa Nepean Ontario Canada

# Natural Language Processing

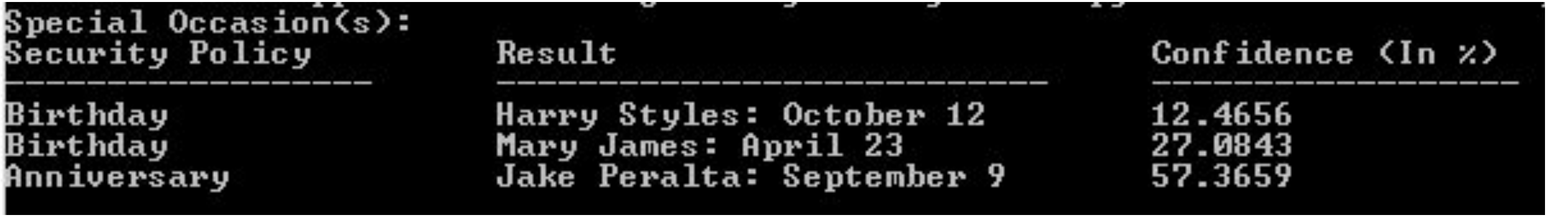
- Common security questions addressed:
  - Favourite hobby or sport
  - Special occasions
- Natural Language Toolkit



```
{
  "participants": [
    {
      "name": "Harry Styles"
    },
    {
      "name": "Sarah Lamonica"
    }
  ],
  "messages": [
     {
      "sender_name": "Harry Styles",
      "timestamp_ms": 1611180056670,
      "content": "I tried.  I cant figure out how to do it!",
      "type": "Generic",
      "is_unsent": false
    },
```



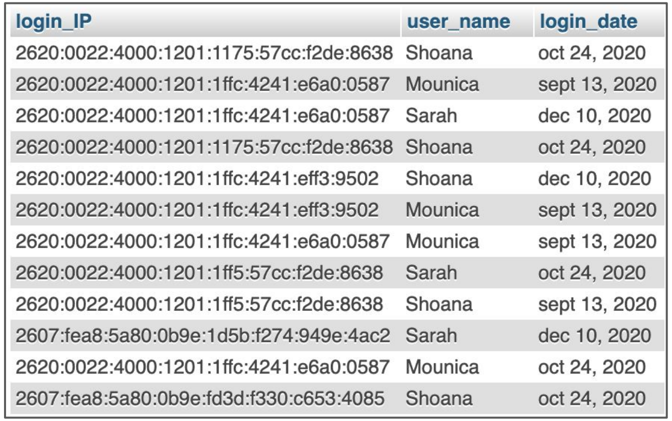
```
Security Policy         Result                            Confidence (In %)
---------------         ----------------------------      ------------------
Common hobby/sport      Soccer                            43.6731
```



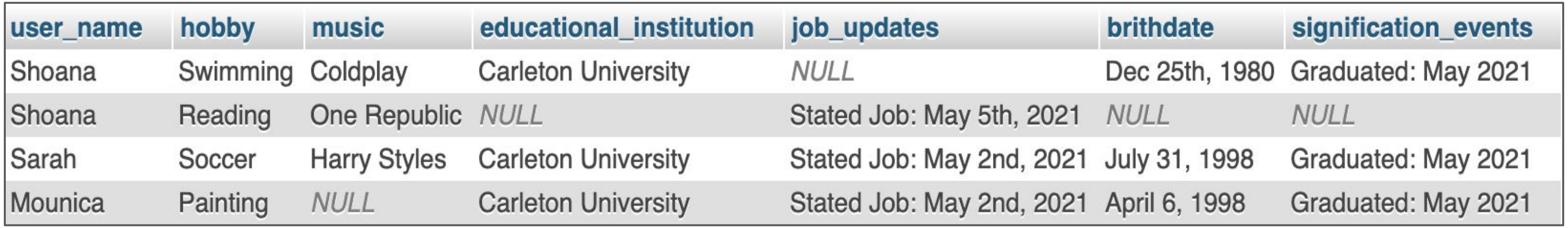
```
Special Occasion(s):
Security Policy         Result                            Confidence (In %)
---------------         ----------------------------      ------------------
Birthday                Harry Styles: October 12          12.4656
Birthday                Mary James: April 23              27.0843
Anniversary             Jake Peralta: September 9         57.3659
```

# Testing & Validation

- Dummy database
  - Used for testing
- Testing with different datasets
  - 3 Distinct Users
- Multiple data points
  - More data points = More accurate results
- Confidence interval
  - Determine how confident the system is in determining the result



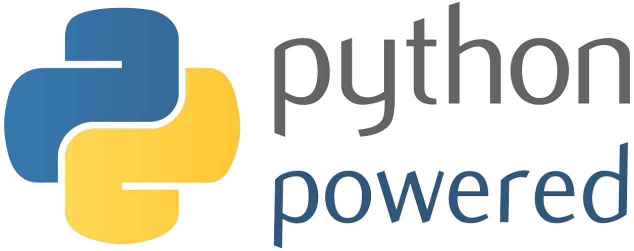
| login_IP | user_name | login_date |
|---|---|---|
| 2620:0022:4000:1201:1175:57cc:f2de:8638 | Shoana | oct 24, 2020 |
| 2620:0022:4000:1201:1ffc:4241:e6a0:0587 | Mounica | sept 13, 2020 |
| 2620:0022:4000:1201:1ffc:4241:e6a0:0587 | Sarah | dec 10, 2020 |
| 2620:0022:4000:1201:1175:57cc:f2de:8638 | Shoana | oct 24, 2020 |
| 2620:0022:4000:1201:1ffc:4241:eff3:9502 | Shoana | dec 10, 2020 |
| 2620:0022:4000:1201:1ffc:4241:eff3:9502 | Mounica | sept 13, 2020 |
| 2620:0022:4000:1201:1ffc:4241:e6a0:0587 | Mounica | sept 13, 2020 |
| 2620:0022:4000:1201:1ff5:57cc:f2de:8638 | Sarah | oct 24, 2020 |
| 2620:0022:4000:1201:1ff5:57cc:f2de:8638 | Shoana | sept 13, 2020 |
| 2607:fea8:5a80:0b9e:1d5b:f274:949e:4ac2 | Sarah | dec 10, 2020 |
| 2620:0022:4000:1201:1ffc:4241:e6a0:0587 | Mounica | oct 24, 2020 |
| 2607:fea8:5a80:0b9e:fd3d:f330:c653:4085 | Shoana | oct 24, 2020 |



| user_name | hobby | music | educational_institution | job_updates | brithdate | signification_events |
|---|---|---|---|---|---|---|
| Shoana | Swimming | Coldplay | Carleton University | *NULL* | Dec 25th, 1980 | Graduated: May 2021 |
| Shoana | Reading | One Republic | *NULL* | Stated Job: May 5th, 2021 | *NULL* | *NULL* |
| Sarah | Soccer | Harry Styles | Carleton University | Stated Job: May 2nd, 2021 | July 31, 1998 | Graduated: May 2021 |
| Mounica | Painting | *NULL* | Carleton University | Stated Job: May 2nd, 2021 | April 6, 1998 | Graduated: May 2021 |

# Accomplishments

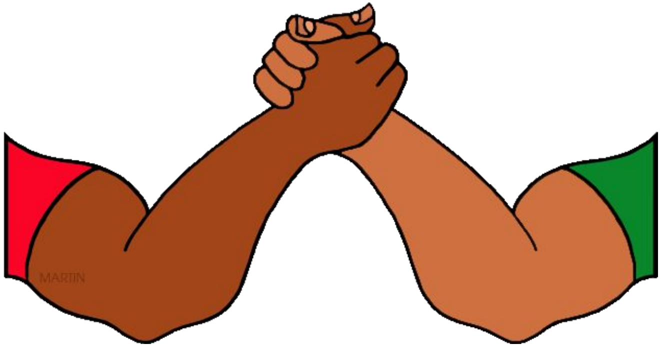
- A security policy
- Database model
- Command-line interface
- Queries designed to infer data
- Data parsing script to clean data
- Providing statistical metrics to the user



```
print("Hello, world!")
```

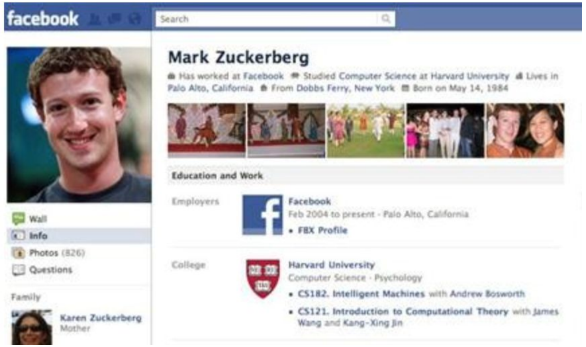
# Challenges

- Database selection (SQL vs. SQLite vs. Pandas Dataframe)
- User Interface Implementation - (Web UI vs. Command Line Interface)
- Implementation of multiple data sets
    - Data consistency and Data cleansing
- Security Policy Development
- Automation



# Future advancements

- Include publicly available data from user profiles
- Automate the runs
- Web Interface
- Association Rules - Can we predict patterns?
- Scale to include more social media websites
- Scale to allow the user to input many different social media data files at the same time



Mark Zuckerberg

Has worked at Facebook · Studied Computer Science at Harvard University · Lives in Palo Alto, California · From Dobbs Ferry, New York · Born on May 14, 1984

Education and Work

Employers: Facebook
Feb 2004 to present · Palo Alto, California
- FBX Profile

College: Harvard University
Computer Science · Psychology
- CS182. Intelligent Machines with Andrew Bosworth
- CS121. Introduction to Computational Theory with James Wang and Kang-Xing Jin

Family
Karen Zuckerberg
Mother

# Conclusion

Provide users with insightful information about their social media data and the various sensitive information that is prone to an inference attack

View
Jason Jaskolka
Mounica Pillarisetty
Mostafa Taha
Shoana Sharma
Sarah Lamonica
Mute
Stop Video
5
Participants
Chat
Share Screen
Record
Reactions
Leave