THE ANONYMISER HACKATHON

Supported by
Department of Information Technology and Electronics
Government of West Bengal

INIT2

Problem Statements

1. Surveillance cameras: Surveillance cameras are becoming ubiquitous in public spaces, leading to concerns about privacy violations and misuse of data. An AI-based anonymizer can be used to protect individuals' identities while allowing organizations to still use the footage for security and analysis purposes.

2. Financial Transactions: Financial institutions must process large amounts of sensitive customer data daily, making them prime targets for cyber attacks. An AI-based anonymizer can be used to protect customer data from theft or misuse.

Problem statement 1: Surveillance cameras

- Title: Protecting Privacy in Public Spaces with an AI-based Anonymizer
- Departments: Law Enforcement, Urban Development, Social Welfare
- How does this problem impact privacy? Share with an example: Surveillance cameras can capture sensitive information such as individuals' movements and activities, leading to privacy concerns. For example, if a person is caught on camera engaging in a controversial or illegal activity, their identity could be revealed and used against them.

How will an anonymizer help retain value of the data? Share with an example:

An AI-based anonymizer can help protect individuals' identities while still allowing organizations to use the footage for security and analysis purposes. For example, a city can use anonymized camera footage to analyze traffic patterns and improve public safety without compromising individuals' privacy.

How can conventional anonymization methods (e.g. masking known PII) not be useful here? Share with an example:

Conventional anonymization methods such as blurring or pixelating may not be effective in situations where individuals' movements and poses can still be used to re-identify them. For example, a person's unique gait or clothing may be enough to identify them, even if their face is blurred.

Solution Design:

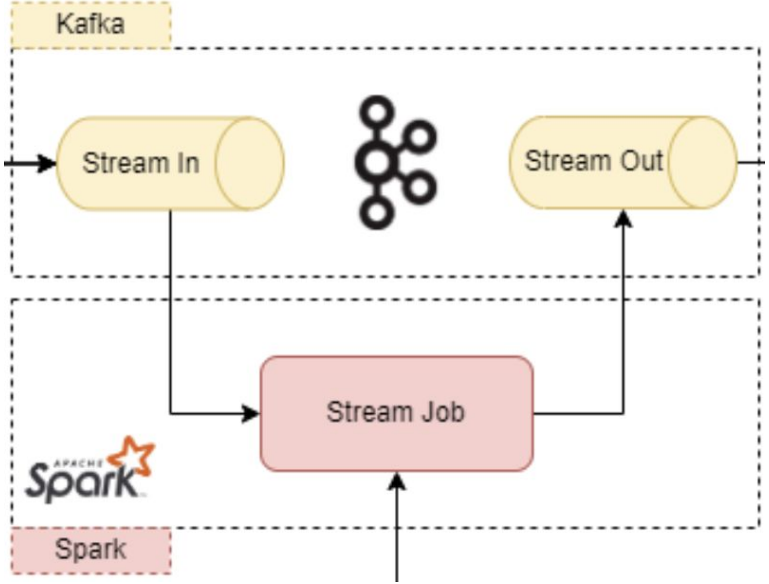
- Capture the surveillance camera footage
- Use computer vision techniques such as blurring or pixelating faces and other identifying features of individuals in the footage
- For situations where conventional techniques are not sufficient, use advanced AI techniques such as generative adversarial networks (GANs) to create synthetic data that can be used for analysis without compromising privacy
    - For this we will also have to develop precise video object detection models
    - Also in lots of use cases, we need not the exact data of the video but merely description of the event happening in the video.
    - A video event detection and video-summarizer model is also being proposed.
- Test the anonymized data to ensure individuals' identities have been successfully removed while preserving the data's utility

Implemented Solution:

The Developed Codebase impacts multiple variation of applications,

Face Blurring

- Dubbed SiamMask based approach
  - single bounding box initialisation
  - operates online
  - producing class-agnostic
  - object segmentation masks
  - rotated bounding boxes
- Kafka brokers and Spark library is utilized to operate on bounding boxes initializations

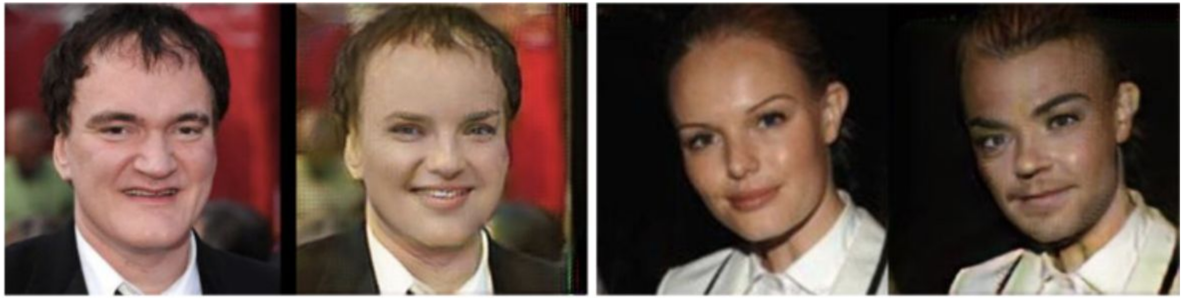


Implemented Solution:

The Developed Codebase impacts multiple variation of applications,

Attribute preserving face anonymization

- The task of removing the identifying characteristics of faces in videos while retaining the useful information for downstream tasks such as detection or tracking.
    - GANs based approach is used, where two competing systems fight:
        - (1) a video anonymizer which remove privacy-sensitive information
        - (2) a discriminator that tries to extract privacy-sensitive information
    - pixel-level modifications to anonymize each person's face



Problem statement 2: Financial Transactions

- Title: Securing Financial Transactions with an AI-based Anonymizer
- Departments: Law Enforcement, Finance
- How does this problem impact privacy? Share with an example: If a financial institution's customer data is not adequately protected, it could be used for identity theft or other fraudulent activities, leading to financial losses and reputational damage for the customers. For example, if a cybercriminal obtains a customer's financial data, they could use it to make unauthorized purchases or access their bank account.

How will an anonymizer help retain value of the data? Share with an example:

An anonymizer can protect sensitive financial data while allowing the financial institution to retain the necessary information for analysis and processing. For example, a bank can analyze anonymized customer data to identify spending patterns and offer personalized financial advice to customers.

How can conventional anonymization methods (e.g. masking known PII) not be useful here? Share with an example:

Conventional anonymization methods may not be sufficient to protect sensitive financial data. For example, masking PII such as name and address may not be enough to protect a customer's financial history and account details.

Solution Design:

- Collect the financial transaction data
- Identify the PII (e.g. name, address, social security number, bank account number)
- Use an AI-based anonymizer to de-identify the data while retaining the valuable information.
- Test the anonymized data to ensure the PII has been successfully removed while preserving the data's utility.

Version 1.1

- Many times, different organizations want data to do analysis but giving the data directly may invade their privacy.
- In this implementation we aim to anonymize proper nouns in the data set in such a manner that personally identifiable information are shadowed while maintaining the integrity of the dataset. This includes
  - **name, last_name, first_name, email, zip_code**
  - **street, street_address, number, text, sentences**
- **Demo:**

Version 1.2

- In certain scenarios, we may want the referential property of different files to be retained to maintain the integrity of data, so that it serves valuable insights all while being anonymized. With this in mind, previous approach was extended to include multiple csv files.
- **DEMO:**

Version 2.0

For our final version, we were planning to add K-anonymity and L-diversity and merge all the different versions together and ship it but were unable to do so due to time constraints;

- We however, implemented K-anonymity and L-diversity algorithms and made visualization script as well
- **DEMO;**
    -

Our github repo: Here

THANK YOU :)