The Knowledge Hub Universities

partnered with Coventry University

KH6047CEM Cyber Security Project

# FORENSIGHT

# A SOCIAL MEDIA FORENSICS TOOL

**Advisors:** Eng. Islam Fathy & Eng. Kareem Eldebassy

**Catherine Medhat 202001102**

May 18, 2024

# DECLARATIONS

I hereby declare that the content given in this dissertation is all my own and has been produced by me via my independent and innovative research. This dissertation has not been previously submitted for any academic degree or other certification at any other university or institution.

All sources of information, data, and scholarly work cited in this dissertation have been properly acknowledged, All figures, tables, and quoted text from other sources are explicitly cited, adhering to the relevant academic standards. I possess complete knowledge of the repercussions of plagiarism and comprehend that it is a violation of academic integrity.

I hereby verify that this research has been conducted with ethical principles. All data obtained from human participants has been acquired with their explicit agreement and with the endorsement of appropriate ethical review boards, as required. Precautions have been implemented to guarantee the privacy and anonymity of the participants.

I confirm that this dissertation adheres to the requirements set by copyright laws and regulations. All copyrighted material included in this work has been properly licensed or is covered by fair use regulations.

# ABSTRACT

In response to the escalating issue of fake accounts on social media platforms, particularly Facebook, this project proposes the development of a social media forensics tool. This tool integrates digital forensics techniques with automated algorithms to effectively detect suspicious patterns indicative of fake profiles. The importance of this endeavor lies in safeguarding the integrity and security of online platforms, mitigating the spread of misinformation, and protecting users from potential cyber threats. The proposed solution aims to address the challenges posed by manual inspection methods, offering an automated approach to identifying fake accounts.

The methodology involves extensive research and data collection, followed by the development and testing of automated algorithms for forensic analysis. Leveraging a Facebook scraper for data collection and utilizing curated datasets for training and testing, the tool aims to achieve high accuracy in detecting fake profiles. Challenges such as data availability and privacy settings are acknowledged, emphasizing the need to overcome these obstacles for effective cybersecurity enhancement.

The expected results encompass the successful implementation of the social media forensics tool, capable of accurately identifying fake accounts and providing actionable insights to users. While limitations may exist, such as constraints imposed by privacy settings, the proposed tool presents a significant advancement in combating online misinformation and ensuring the security of online platforms. Recommendations for future studies include further refinement and enhancement of the tool's capabilities, as well as continuous monitoring and adaptation to evolving cybersecurity threats.

In conclusion, the development of this social media forensics tool represents a crucial step towards addressing the growing concerns surrounding fake accounts, ultimately contributing to the preservation of online integrity and user security.

# ACKNOWLEDGMENT

I like to convey my sincere appreciation to everyone who helped and advised me while I was doing my dissertation.

First and foremost, I would want to express my sincere gratitude to Eng. Islam Fathy & Eng. Kareem Eldebassy, my supervisors, for all of their help and support throughout the year. Their knowledge and perseverance have been crucial in forming this idea.

I express my gratitude to the teachers and staff of the EHC course at Coventry University-Egypt Branch for their provision of resources and a research-friendly environment. With special gratitude to Dr. Haitham Ghalwash & Eng. May Shalaby for their guidance and support during my academic career.

My sincere gratitude to my friends and coworkers for their encouragement, helpful criticism, and unwavering source of drive.

I owe my family a great deal for their steadfast encouragement and support. I am grateful to my parents for their unwavering support and patience, as well as for believing in me.

I would like to conclude by thanking each and every participant and contributor who helped with our research by offering insightful information and data. Without your help, this job would not have been feasible.

I am grateful to everyone who helped make this adventure possible.

# TABLE OF CONTENTS

DECLARATIONS ........ 1

ABSTRACT ........ 2

ACKNOWLEDGMENT ........ 3

Table Of Figures ........ 6

1 Introduction ........ 7

1.1 Background ........ 7

1.2 Problem Statement ........ 7

1.3 Objectives ........ 7

1.4 Scope ........ 7

1.5 Importance ........ 8

2 Literature Review ........ 8

2.1 Background of the Problem ........ 8

2.2 Competitor Analysis ........ 8

2.3 Studies Review ........ 9

2.4 Survey Analysis ........ 9

3 Methodology ........ 10

3.1 List of Requirements and List of Resources ........ 10

3.1.1 Frontend Development ........ 10

3.1.2 Upload Section ........ 11

3.1.3 Results Section ........ 11

3.1.4 About Section ........ 12

3.2 Software Development Life Cycle ........ 12

3.2.1 Agile and Its Fit for ForenSight: ........ 12

3.3 Timeline ........ 13

3.4 Methods, Rules, and Approaches ........ 15

3.4.1 Data Acquisition ........ 15

3.4.2 Data Processing ........ 15

3.5 API Endpoints ........ 17

3.6 Error Handling and Logging ........ 17

4 Implementation ........ 17

4.1 Frontend Development ........ 17

4.1.1 Header Section: ........ 17

4.1.2 Upload Section ..................................................18
4.1.3 Results Section ..................................................19
4.1.4 About Section ..................................................20
4.2 Backend Development ..................................................21
4.2.1 Data Processing ..................................................21
4.2.2 Analysis Algorithms ..................................................29
4.2.3 API Endpoints ..................................................30
5 Results & Discussion ..................................................32
5.1 Obstacles Faced ..................................................32
5.1.1 Challenges in Machine Learning Model Development ..................................................32
5.2 Outcome ..................................................33
5.2.1 Integration with Scraping Tools ..................................................33
5.2.2 Detailed Analysis Results ..................................................33
6 Future Work ..................................................36
6.1 Integration of Advanced AI Techniques ..................................................36
6.2 Enhanced Post Analysis and Interaction Review ..................................................36
6.3 Profile Picture Analysis ..................................................37
6.4 Integration with Data Acquisition Tools ..................................................37
6.5 Continuous Learning and Model Updating ..................................................37
6.6 Ethical and Privacy Considerations ..................................................37
7 Conclusion ..................................................38
8 Appendices ..................................................39
9 References ..................................................39

# TABLE OF FIGURES

Figure 1 Percentage of Participants Encountering Fraudulent Accounts ................................ 10
Figure 2 Age Distribution of Participants Identifying Fraudulent Accounts........................... 10
Figure 3 Perceived Gender Representation in Fraudulent Accounts ...................................... 10
Figure 4 Agile Methodology.................................................................................... 13
Figure 5 System Design Diagram ............................................................................. 16
Figure 6 Header Section........................................................................................... 18
Figure 7 Upload Section .......................................................................................... 19
Figure 8 Results Section .......................................................................................... 20
Figure 9 About Section ............................................................................................ 21
Figure 10 Loading and Merging Data........................................................................ 23
Figure 11 Column Merging and Reordering................................................................ 24
Figure 12 Parsing Join Status Text ............................................................................ 25
Figure 13 Fake Probability Calculations...................................................................... 28
Figure 14 File Upload Endpoint ................................................................................ 31
Figure 15 Download Results Endpoint ....................................................................... 32
Figure 16 Data Visualization Endpoint....................................................................... 32
Figure 17 Home Section Website .............................................................................. 35
Figure 18 Upload Section Website ............................................................................ 35
Figure 19 Results Section Website ............................................................................ 35
Figure 20 About Section Website .............................................................................. 36

# 1 INTRODUCTION

## 1.1 BACKGROUND

Social media platforms have become essential in modern times for daily communication, spreading information, and socializing. Platforms such as Facebook accommodate billions of people who generate a vast amount of material. Although these platforms provide notable advantages, they also pose distinct difficulties, especially in the field of digital investigations. The rapid increase in the number of fraudulent accounts, which may be utilized for nefarious purposes such as spreading false information, engaging in phishing attacks, and performing other cyber risks, has emerged as a critical concern. The vast magnitude and intricate nature of material created by users make it even more challenging to identify and monitor potential dangers, requiring the employment of advanced analytical techniques.

## 1.2 PROBLEM STATEMENT

Existing approaches to digital investigations sometimes lack the necessary depth and efficiency to effectively explore the elaborate realm of social media. Investigators have substantial obstacles when attempting to trace internet actions, distinguishing fraudulent accounts, and revealing possible dangers. The current technologies are insufficient in their ability to thoroughly analyze large volumes of data with accuracy and efficiency. The objective of this project is to tackle these difficulties by creating ForenSight, a specialized tool that aims to improve social media forensic investigations.

## 1.3 OBJECTIVES

The main goals of ForenSight are:

1. The objective is to create sophisticated data collecting techniques that can effectively manage the substantial amounts of social media content.
2. The objective is to develop reliable systems for detecting fraudulent accounts and flagging possible security risks.
3. The purpose is to present investigators with a comprehensive understanding of user behavior and optimize the investigating process.

## 1.4 SCOPE

This project aims to develop and evaluate ForenSight, with a specific focus on its application to Facebook. This choice is based on the platform's large user base and the prevalence of fraudulent accounts. Although the program has the potential to be modified for use on other social media platforms in the future, the primary focus of this research is to solely target Facebook in order to verify its efficacy. ForenSight will incorporate functionalities such as user profile analysis, assessment of post content, and algorithms for identifying potential threats.

## 1.5 IMPORTANCE

The significance of tackling the issue of fraudulent accounts and security risks on social media cannot be exaggerated. Counterfeit profiles have the potential to compromise the credibility of social media platforms, disseminate false information, and present significant threats to security. ForenSight's objective is to improve the safety and dependability of social media platforms by equipping investigators with sophisticated tools for detecting and analyzing these accounts. The knowledge acquired by utilizing this tool can assist in reducing risks, guiding policy decisions, and supporting wider initiatives in the fields of cyber security and digital forensics.

# 2 LITERATURE REVIEW

## 2.1 BACKGROUND OF THE PROBLEM

The issue of fake accounts on social media platforms is versatile, encompassing bots, trolls, and fake profiles that manipulate discussions, influence political processes, and broadcast misinformation. According to the Global Cybersecurity Institute, approximately 15% of social media accounts are estimated to be inauthentic, an outline that highlights the magnitude of the problem in digital spaces (Global Cybersecurity Institute, 2023). These accounts can distort public opinion, damage reputations, and undermine the trustworthiness of online platforms. The rapid proliferation of these accounts is facilitated by the ease of automation and the scalability of digital identities, making traditional detection methods inadequate. Additionally, the sophistication of these operations, often backed by state actors or organized groups, poses significant challenges to current security measures.

## 2.2 COMPETITOR ANALYSIS

Existing solutions to combat fake accounts include platform-integrated tools and third-party applications. Major social media companies, such as Facebook and Twitter, employ algorithms that analyze user behavior patterns and interaction networks to detect irregularities indicative of fake accounts. For instance, Facebook’s machine learning models are designed to recognize patterns of spammy content sharing and coordinated inauthentic behavior, which are typical of fake profiles (Facebook Transparency Report, 2024). However, these internal tools often lack transparency, raising concerns about privacy and the potential for wrongful account suspension. On the other hand, third-party tools like Botometer analyze public account metadata to score the likelihood of an account being a bot, which provides a useful service for end-users but depends heavily on the accessibility of data and user consent, limiting its applicability (Zhang & Paxson, 2022). Both types of tools face challenges in keeping pace with the evolving tactics of malicious actors, who continuously adapt to bypass detection technologies. The limitations of these approaches highlight the need for innovative solutions that are adaptive, transparent, and maintain user privacy.

## 2.3 STUDIES REVIEW

The academic community has been actively engaged in developing more effective methods to identify and mitigate the effects of fake accounts. Research efforts have been concentrated on enhancing machine learning techniques to detect subtle patterns of abnormal behavior that may indicate a fake account. For example, a study by Smith and Johnson (2023) introduced a neural network model that integrates account metadata with post content analysis to improve detection rates (Smith & Johnson, 2023). This model benefits from its ability to learn from evolving data, allowing it to adapt to new tactics used by malicious actors. Furthermore, researchers at MIT have developed a sophisticated algorithm that employs natural language processing to analyze the linguistic characteristics of posts, which can differentiate between genuine and inauthentic interactions with a high degree of accuracy (Chen et al., 2024). These academic advancements are critical as they contribute to the body of knowledge that can be leveraged by practical security applications to enhance their effectiveness. Moreover, collaborative studies, such as those facilitated by the Cybersecurity for Democracy project at NYU, focus on collective efforts to understand and address the systemic issues posed by fake accounts, emphasizing a holistic approach that includes policy implications alongside technological solutions (Cybersecurity for Democracy, 2023).

## 2.4 SURVEY ANALYSIS

The survey performed for this study offered useful insights into users' experiences and views of fraudulent accounts on social media sites. The majority of the participants showed significant apprehension over the widespread existence of fraudulent accounts, emphasizing the negative effect on their online activities and confidence in digital platforms. Based on the survey findings, more than 80% of participants reported coming across fraudulent accounts. These profiles were characterized by a lack of user-generated material and unusual posting frequency. This user feedback emphasizes the necessity for enhanced detection technologies that can function with transparency and safeguard user privacy. Additionally, the demographic data indicated that younger users, namely individuals aged 18-34, have a greater tendency to identify and report fraudulent accounts. This implies that instructional campaigns focused on enhancing digital comprehension might effectively empower users to securely use social media platforms. The survey also uncovered a notable perceived bias about the representation of gender in fake accounts, with a majority of respondents assuming that these accounts often imitate female profiles. This observation initiates conversations regarding social prejudices and the methods employed by malicious actors to manipulate these beliefs for more efficient fraudulent activities or distribution of false information.

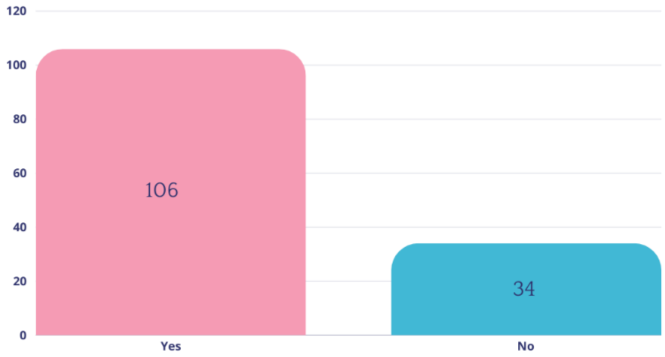


Figure 1 Percentage of Participants Encountering Fraudulent Accounts

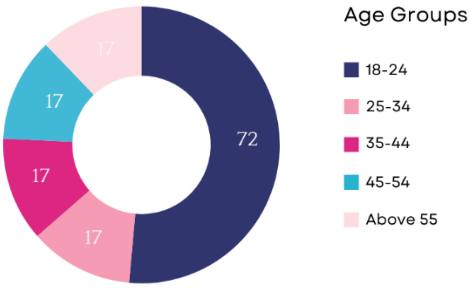


Figure 2 Age Distribution of Participants Identifying Fraudulent Accounts

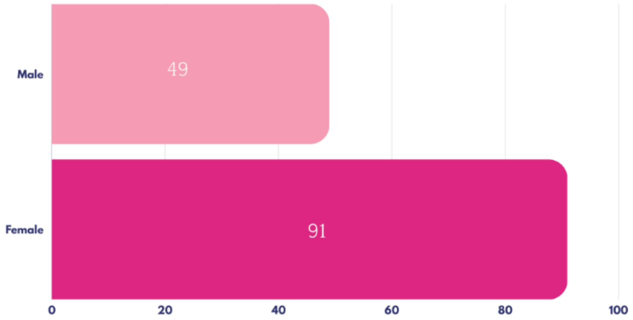


Figure 3 Perceived Gender Representation in Fraudulent Accounts

# 3 METHODOLOGY

## 3.1 LIST OF REQUIREMENTS AND LIST OF RESOURCES

### 3.1.1 FRONTEND DEVELOPMENT

Frontend development refers to the process of creating the user interface and user experience of a website or application. It involves using programming languages such as HTML, CSS, and JavaScript to design and implement the visual and interactive elements that users interact with.

**Requirements**:

1. **Project Title and Logo**:

The webpage should prominently display the project title “ForenSight: a Social Media Forensics Tool” and its related logo at the top of the page to establish the brand and facilitate recognition.

2. **Opening Statement**:

   Below the logo, include a concise introductory statement that provides consumers with an outline of ForenSight's objective in enhancing online security.

3. **Navigation Links**:

   Incorporate navigation links to guide users to different areas of the website, facilitating convenient access to features and information.

**Resources**:

- HTML, CSS, and JavaScript for frontend development.
- Software for graphic design used to create the project logo.
- A text editor or integrated development environment (IDE) ,software tool, to use for coding.

### 3.1.2 UPLOAD SECTION

**Requirements**:

1. **File Upload Button**:

   Implement two file upload buttons to enable users to choose and submit their data files for analysis.

2. **Instructions**:

   Provide explicit instructions on permissible file formats and the purpose of the upload procedure alongside the upload buttons.

3. **Upload Form**:

   Create an HTML form element that allows users to upload certain files for processing on the server.

**Resources**:

- Utilize HTML and JavaScript to construct the upload form and manage file selection.
- CSS for formatting the upload part.
- Utilize a server-side programming language, such as Python with Flask, to handle the processing of submitted files.

### 3.1.3 RESULTS SECTION

**Requirements**:

1. **Heading for Results**:

   Present a heading that provides a clear description of the item being shown, such as “Analysis Findings from ForenSight.”

2. **Doughnut Chart**:

   Utilize a doughnut chart to visually illustrate the classification of severity levels for identified fraudulent accounts in the submitted data.

3. **Download Form**:
   Offer a form that allows customers to select the severity degree of fraudulent accounts they wish to download for additional examination.

**Resources**:

- Chart.js or an equivalent JavaScript library for generating the doughnut chart.
- HTML and CSS are used to organize and design the results section.
- Backend API endpoints for accessing analysis results and downloading data.

### 3.1.4 ABOUT SECTION

**Requirements**:

1. **Project Overview**:
   Provide a detailed description of ForenSight's goal and importance in detecting and revealing fake accounts on social media sites.
2. **Target Audience**:
   Specify the audience that can obtain value from ForenSight, including marketing companies, Facebook group administrators, and individuals with a genuine interest in online security.
3. **Call to Action**:
   Encourage people to join the project's mission and actively contribute to the development of a more secure digital environment.

**Resources**:

- Tools for content creation to write the project summary and target audience information.
- HTML and CSS are used to organize and design the about section.

## 3.2 SOFTWARE DEVELOPMENT LIFE CYCLE

The software development life cycle (SDLC) refers to the series of activities and stages involved in the development of software applications. Agile is a distinctive technique among the different options, known for its flexibility and iterative approach that suits the dynamic character of today's software development projects.

The Agile technique places a strong emphasis on collaboration, adaptability, and continuous improvement across the whole development process. The primary objective is to provide consumers with value by utilizing incremental development cycles, commonly referred to as sprints. A sprint normally has a duration of a few weeks and leads to the creation of a product increment that can potentially be deployed.

### 3.2.1 Agile and Its Fit for ForenSight:

ForenSight, being a tool for social media forensics, requires a development strategy that can adapt to changing user requirements, dynamic data sources, and constantly increasing security risks. The Agile approach is a wonderful fit for these criteria due to various reasons:

1. **Adaptability**: the Agile technique offers versatility to adjust to evolving project needs and goals. The iterative nature of the Agile technique permits the implementation of modifications in response to feedback and developing insights.
2. **Incremental Development**: The Agile technique facilitates the continual delivery of valuable features and functionality by dividing the project into manageable iterations. This technique enables immediate testing of ideas and guarantees that the project stays in line with customer expectations.
3. **Customer-Centric Approach**: Agile methodology prioritizes client participation and input, ensuring that ForenSight adapts and improves based on user requirements and preferences. Regular engagement with professors is essential for verifying assumptions, discovering new requirements, and efficiently prioritizing development attempts.
4. **Rapid Prototyping**: Agile's continuous development process enables the quick creation and testing of prototypes to validate concepts. This facilitates rapid testing with various features and functionalities, allowing me to iteratively enhance the product based on feedback from real-world usage.

Agile is an ideal technique for developing ForenSight because it delivers the essential flexibility, adaptability, and customer focus to create a high-quality and user-centric social media forensics solution.

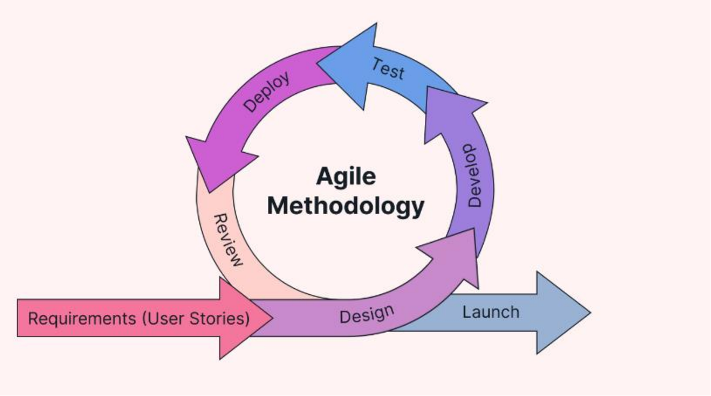


Figure 4 Agile Methodology

## 3.3 TIMELINE

**Phase 1**: Project Initialization and Strategic Planning (2 weeks)

- **Week 1**:
  - Establish project goals and determine the parameters of the project.
  - Establish the development environment and get the necessary tools.

    - Perform preliminary investigation on social media scraping tools and data processing methodologies.
- **Week 2**:
    - Develop a comprehensive project strategy and establish a clear timeframe.
    - Conclude the necessary specifications and available assets.
    - Create a comprehensive approach for obtaining and processing data.

**Phase 2**: Development of both the Frontend and Backend of the project (6 weeks)

- **Week 3-4: Frontend Development**
    - Create and build the header, upload, results, and about sections of the frontend.
    - Integrate navigation links and user interface components to ensure a smooth and uninterrupted user experience.
    - Perform testing to verify the responsiveness and compatibility of the software on various devices.
- **Week 5-7: Backend Development**
    - Develop and integrate data processing modules that encompass various tasks such as managing file uploads, loading, and merging data, merging and reordering columns, interpreting join status information, cleaning and normalizing data, and performing fake probability calculations.
    - Create API endpoints for uploading files, triggering analysis, retrieving results, downloading results, and visualizing data.

**Phase 3**: Testing (2 weeks)

- **Week 8:**
    - Perform unit tests for both frontend and backend components.
    - Conduct integration testing to guarantee smooth and uninterrupted communication between the frontend and backend systems.
    - Detect and rectify any software defects or problems.
- **Week 9:**
    - Perform user acceptability testing to collect input and implement required modifications.
    - Conduct performance testing to enhance system efficiency and responsiveness.
    - Complete the finalization of the documentation and make necessary preparations for the deployment process..

**Phase 4**: Expo Week (1 week)

- **Week 10**:
    - Implement the deployment of ForenSight in an operational environment.
    - Monitor the performance of the system and get feedback from Expo guests.
    - Assess the efficiency of the tool in attaining project goals.

**Phase 5**: Finalization and Presentation (1 week)

- **Week 11:**
  - Complete the project report and documentation.
  - Create and organize the necessary materials for the project demonstration.
  - Deliver a comprehensive presentation of ForenSight and the results of the project to professors and evaluators.

**Phase 6:** Post-Project Activities (Continuing)

- **After Week 11:**
  - Resolve any post-deployment issues or implement improvements based on guest feedback.
  - Investigate possibilities for additional growth or incorporation with alternative tools and platforms.

## 3.4 METHODS, RULES, AND APPROACHES

### 3.4.1 DATA ACQUISITION

ForenSight acquires user data by extracting information from social media networks, particularly Facebook, using external scraping technologies. These tools facilitate the retrieval of different characteristics linked to user profiles, such as profile names, usernames, profile URLs, join dates, and other related information. The collected data is subsequently stored in Excel spreadsheets or CSV files for subsequent processing and analysis.

### 3.4.2 DATA PROCESSING

1. **File Upload Handling**:
   - Users are required to supply two files containing social media data, usually in Excel or CSV format.
   - The backend verifies the presence of both files and securely saves them in a specified directory.
   - Error management techniques guarantee a seamless upload procedure by delivering precise feedback to users in the event of any problems.
2. **Loading and Merging Data**:
   - The data included in the uploaded files is imported into Pandas DataFrames.
   - DataFrames are combined by matching columns that they have in common, guaranteeing the inclusion of all essential data.
   - To avoid data loss during the merging process, any missing or mismatched columns are effectively handled.
3. **Column Merging and Rearranging**:
   - The columns ‘Name’ and ‘Username’ are combined to provide a single representation of the user's identity.
   - The ‘Link’ and ‘Profile URL’ fields are merged to create a uniform identifier for user profiles.

- The column order is modified to enhance the organization and coherence of the dataset.

4. **Parsing Join Status Text**:
   - Text parsing methods are utilized to retrieve valuable information, such as the dates when users joined, from the 'Join status text' field.
   - Regular expressions are employed to identify patterns that indicate the duration of time since the user became a member.
   - Error handling guarantees precise parsing even when there are deviations from anticipated patterns.
5. **Data Cleaning and Normalization**:
   - Duplicates are eliminated by using unique IDs to maintain data integrity.
   - Both text and numerical data are standardized to ensure they are in a consistent format and scale, respectively.
   - The system identifies and rectifies inconsistent data entries to ensure the integrity of the data.
   - Rigorous validation guarantees that the processed and standardized dataset fulfils quality standards.
6. **Fake Probability Calculations**:
   - User accounts are assessed for their likelihood of being fake based on many factors, such as verification status, existence of information, and account joining length.
   - A scoring system allocates fictitious likelihood values by considering the collective impact of these indicators.
   - The computed probabilities of bogus data are included in the dataset for additional analysis and reporting.

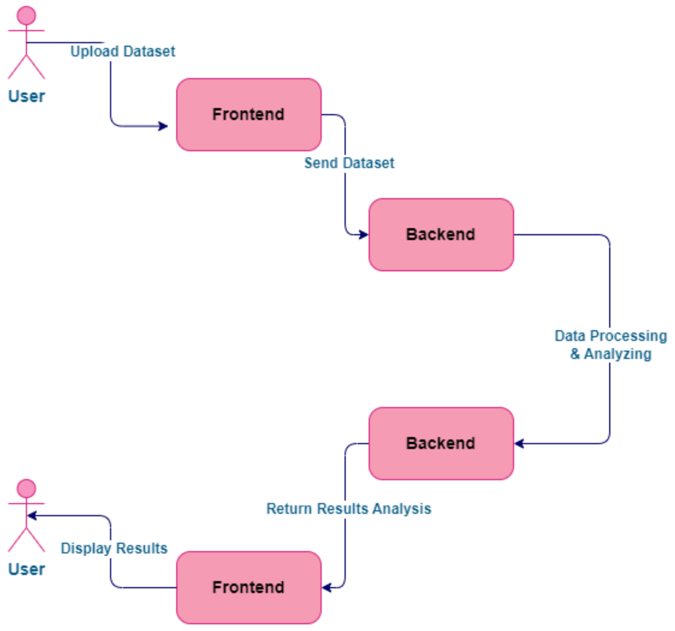


Figure 5 System Design Diagram

## 3.5 API ENDPOINTS

The backend of ForenSight is supplied with API endpoints that enable users to interact with the platform.

1. **File Upload Endpoint**: Enables users to submit data files for analysis.
2. **Analysis Trigger Endpoint**: Responsible for initiating the analysis process on the data that has been submitted.
3. **Results Retrieval Endpoint**: Allows users to acquire analysis results.
4. **Download Results Endpoint**: Enables users to obtain analytic findings in their desired format.
5. **Data Visualization Endpoint**: Generates visual representations depending on the outcomes of the study.

## 3.6 ERROR HANDLING AND LOGGING

1. **Structured Exception Handling:** Identifies and handles different types of faults, guaranteeing the stability of the system.
2. **HTTP Status Codes:** Communicate the status of API requests and responses, aiding in the discovery of errors.
3. **Logging Features:** Capture crucial contextual information to facilitate efficient troubleshooting and analysis.

# 4 IMPLEMENTATION

## 4.1 FRONTEND DEVELOPMENT

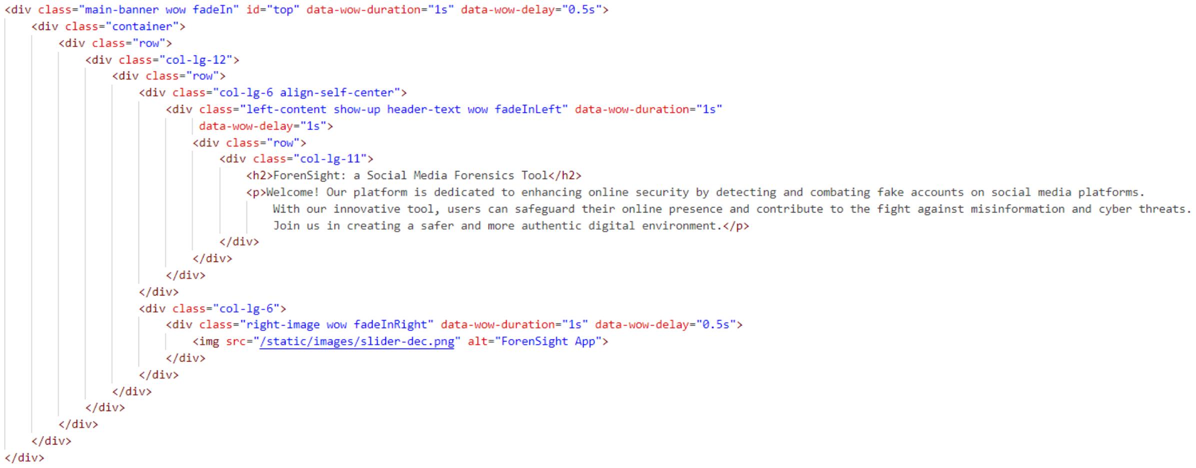
### 4.1.1 HEADER SECTION:

The Header Section provides an introduction to ForenSight. Users are able to gain a comprehensive understanding of the tool's purpose and functionality. This section consists of the following components:

- **Project Title and Logo**: The project title and logo are displayed at the top of the page, ensuring immediate recognition and branding.
- **Opening Statement**: A brief introduction text below the logo offers a concise overview of ForenSight and its role in strengthening online security.
- **Navigation Links**: The website offers navigation links that conveniently direct users to various sections, ensuring easy access to important features and information.

**Detailed Description**:

The header section of the ForenSight frontend contains the project title ‘ForenSight: a Social Media Forensics Tool’ and the logo, which acts as visual branding for the platform. Underneath the logo, a concise introduction text greets users to the platform and highlights its commitment to improving online security by identifying and combating fake accounts on social media platforms. The navigation links have been strategically positioned to ensure smooth and effortless access to the home, upload, and about sections of the website.



```
<div class="main-banner wow fadeIn" id="top" data-wow-duration="1s" data-wow-delay="0.5s">
    <div class="container">
        <div class="row">
            <div class="col-lg-12">
                <div class="row">
                    <div class="col-lg-6 align-self-center">
                        <div class="left-content show-up header-text wow fadeInLeft" data-wow-duration="1s"
                          data-wow-delay="1s">
                            <div class="row">
                                <div class="col-lg-11">
                                    <h2>ForenSight: a Social Media Forensics Tool</h2>
                                    <p>Welcome! Our platform is dedicated to enhancing online security by detecting and combating fake accounts on social media platforms.
                                        With our innovative tool, users can safeguard their online presence and contribute to the fight against misinformation and cyber threats.
                                        Join us in creating a safer and more authentic digital environment.</p>
                                </div>
                            </div>
                        </div>
                    </div>
                    <div class="col-lg-6">
                        <div class="right-image wow fadeInRight" data-wow-duration="1s" data-wow-delay="0.5s">
                            <img src="/static/images/slider-dec.png" alt="ForenSight App">
                        </div>
                    </div>
                </div>
            </div>
        </div>
    </div>
</div>
```

Figure 6 Header Section

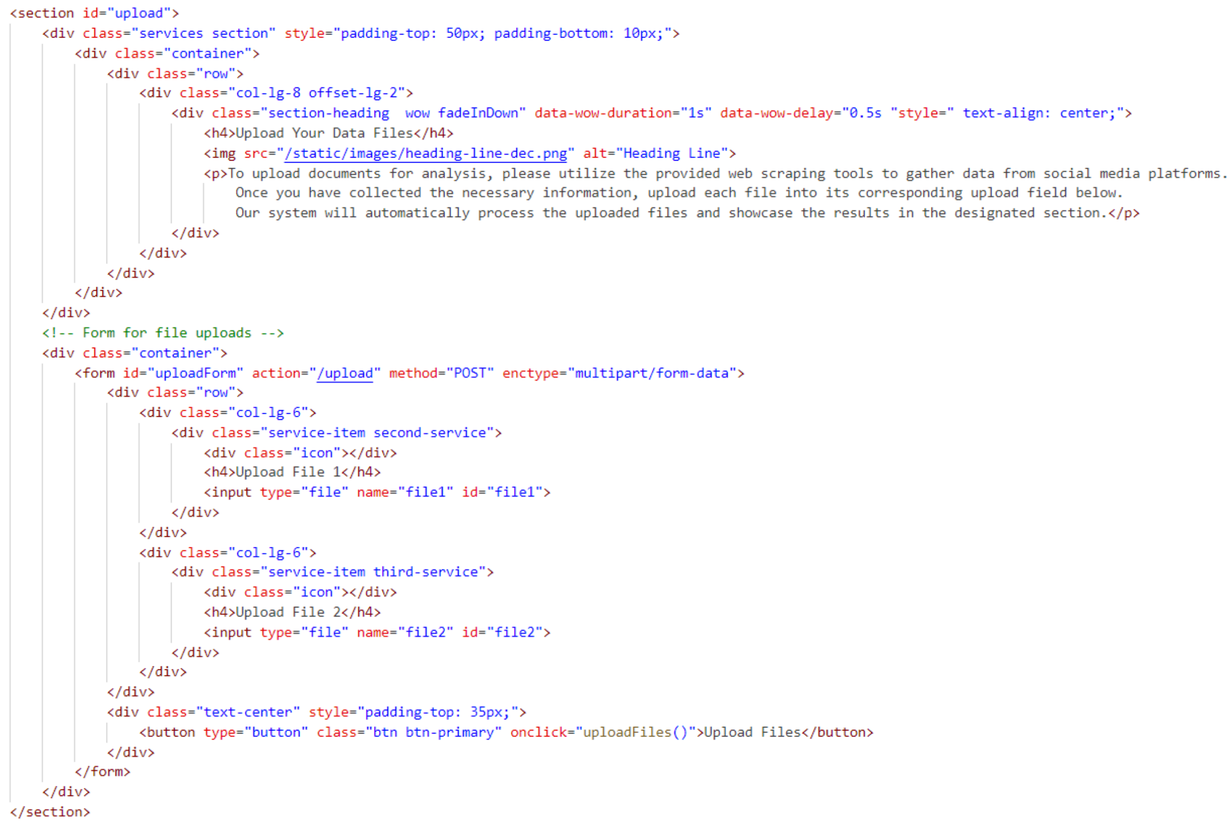
### 4.1.2 UPLOAD SECTION

The Upload Section provides users with the ability to easily upload their data files for analysis. This section is of utmost importance as it lays the foundation for the core functionality of ForenSight. Important elements consist of:

- **Two File Upload Buttons**: available for users to conveniently select and upload their data files for analysis.
- **Instructions**: The upload buttons are accompanied by clear and concise guidance, informing users about the acceptable file formats and the purpose of the upload process.
- **Upload Form**: implemented using the HTML ‘<form>’ element, which allows users to submit selected files for processing on the server.

**Detailed Description**:

The upload section of ForenSight includes two file upload buttons, namely “Upload File 1” and “Upload File 2.” Each button is accompanied by a concise description explaining its purpose. Users are advised to utilize the provided web scraping tools to gather data from social media platforms and upload the collected information into the corresponding upload fields. To begin the upload process, simply click on the “Upload Files” button. This action will prompt the selected files to be submitted to the server for automatic processing.



```
<section id="upload">
    <div class="services section" style="padding-top: 50px; padding-bottom: 10px;">
        <div class="container">
            <div class="row">
                <div class="col-lg-8 offset-lg-2">
                    <div class="section-heading  wow fadeInDown" data-wow-duration="1s" data-wow-delay="0.5s "style=" text-align: center;">
                        <h4>Upload Your Data Files</h4>
                        <img src="/static/images/heading-line-dec.png" alt="Heading Line">
                        <p>To upload documents for analysis, please utilize the provided web scraping tools to gather data from social media platforms.
                            Once you have collected the necessary information, upload each file into its corresponding upload field below.
                            Our system will automatically process the uploaded files and showcase the results in the designated section.</p>
                    </div>
                </div>
            </div>
        </div>
    </div>
    <!-- Form for file uploads -->
    <div class="container">
        <form id="uploadForm" action="/upload" method="POST" enctype="multipart/form-data">
            <div class="row">
                <div class="col-lg-6">
                    <div class="service-item second-service">
                        <div class="icon"></div>
                        <h4>Upload File 1</h4>
                        <input type="file" name="file1" id="file1">
                    </div>
                </div>
                <div class="col-lg-6">
                    <div class="service-item third-service">
                        <div class="icon"></div>
                        <h4>Upload File 2</h4>
                        <input type="file" name="file2" id="file2">
                    </div>
                </div>
            </div>
            <div class="text-center" style="padding-top: 35px;">
                <button type="button" class="btn btn-primary" onclick="uploadFiles()">Upload Files</button>
            </div>
        </form>
    </div>
</section>
```

Figure 7 Upload Section

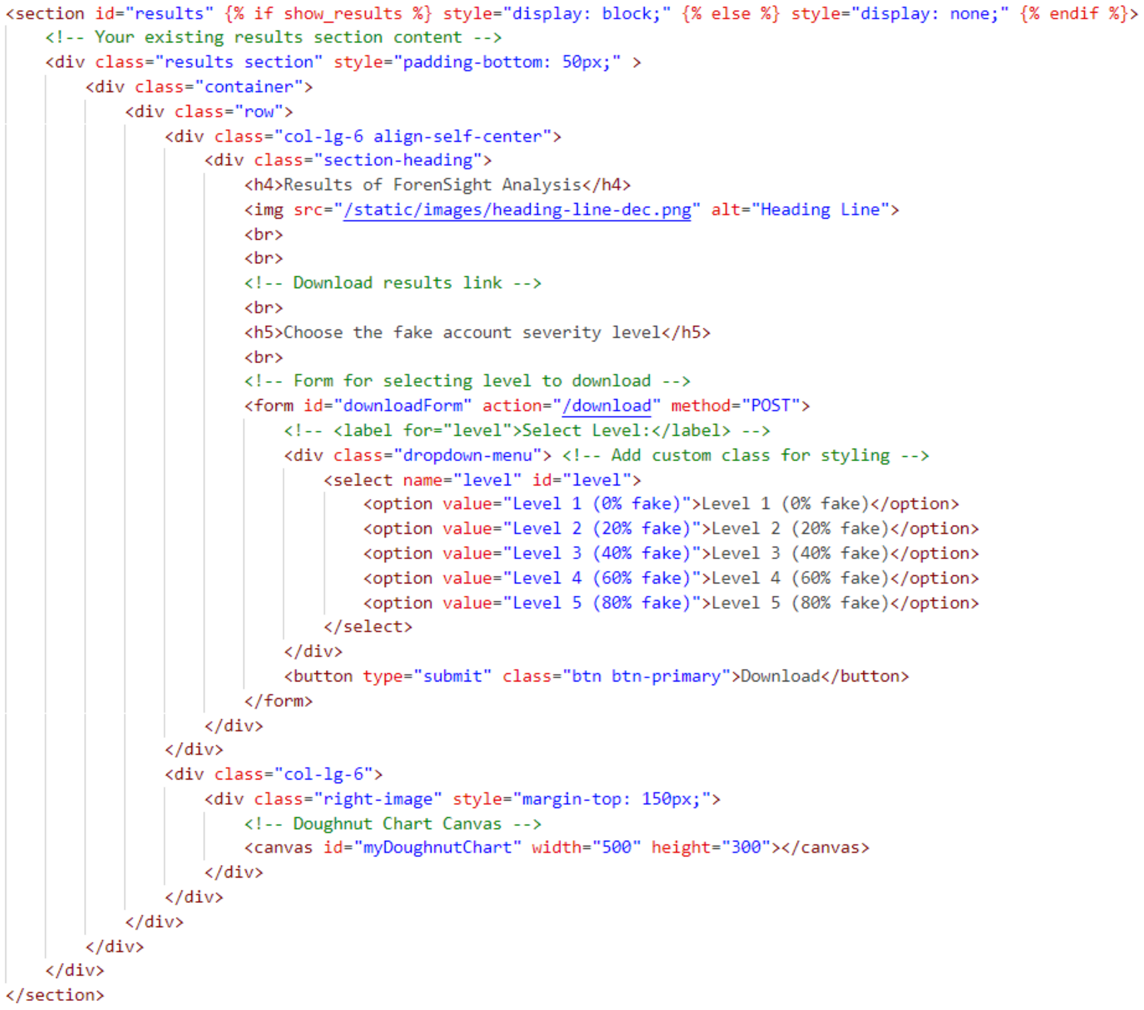
### 4.1.3 RESULTS SECTION

The Results Section presents the findings of the analysis in a format that is straightforward to understand. In this section, I will discuss the important findings and insights that have been derived from the data files that have been uploaded. Important elements consist of:

- Heading for Results: A heading that clearly describes the content being displayed, for example, “Analysis Findings from ForenSight.”
- Doughnut Chart: commonly employed to visually represent the distribution of severity levels for detected fake accounts in the uploaded data.
- Download Form: A form that enables users to choose the severity level of fake accounts they want to download for further analysis.

**Detailed Description**:

The results section of ForenSight presents the findings of the analysis conducted on the uploaded data files. The displayed content is introduced by a heading titled “Results of ForenSight Analysis.” Under the heading, a doughnut chart visually displays the distribution of severity levels for detected fake accounts in the analyzed data. Users are provided with a form to conveniently choose the severity level of fake accounts they want to download for further examination.



```
<section id="results" {% if show_results %} style="display: block;" {% else %} style="display: none;" {% endif %}>
    <!-- Your existing results section content -->
    <div class="results section" style="padding-bottom: 50px;" >
        <div class="container">
            <div class="row">
                <div class="col-lg-6 align-self-center">
                    <div class="section-heading">
                        <h4>Results of ForenSight Analysis</h4>
                        <img src="/static/images/heading-line-dec.png" alt="Heading Line">
                        <br>
                        <br>
                        <!-- Download results link -->
                        <br>
                        <h5>Choose the fake account severity level</h5>
                        <br>
                        <!-- Form for selecting level to download -->
                        <form id="downloadForm" action="/download" method="POST">
                            <!-- <label for="level">Select Level:</label> -->
                            <div class="dropdown-menu"> <!-- Add custom class for styling -->
                                <select name="level" id="level">
                                    <option value="Level 1 (0% fake)">Level 1 (0% fake)</option>
                                    <option value="Level 2 (20% fake)">Level 2 (20% fake)</option>
                                    <option value="Level 3 (40% fake)">Level 3 (40% fake)</option>
                                    <option value="Level 4 (60% fake)">Level 4 (60% fake)</option>
                                    <option value="Level 5 (80% fake)">Level 5 (80% fake)</option>
                                </select>
                            </div>
                            <button type="submit" class="btn btn-primary">Download</button>
                        </form>
                    </div>
                </div>
                <div class="col-lg-6">
                    <div class="right-image" style="margin-top: 150px;">
                        <!-- Doughnut Chart Canvas -->
                        <canvas id="myDoughnutChart" width="500" height="300"></canvas>
                    </div>
                </div>
            </div>
        </div>
    </div>
</section>
```

Figure 8 Results Section

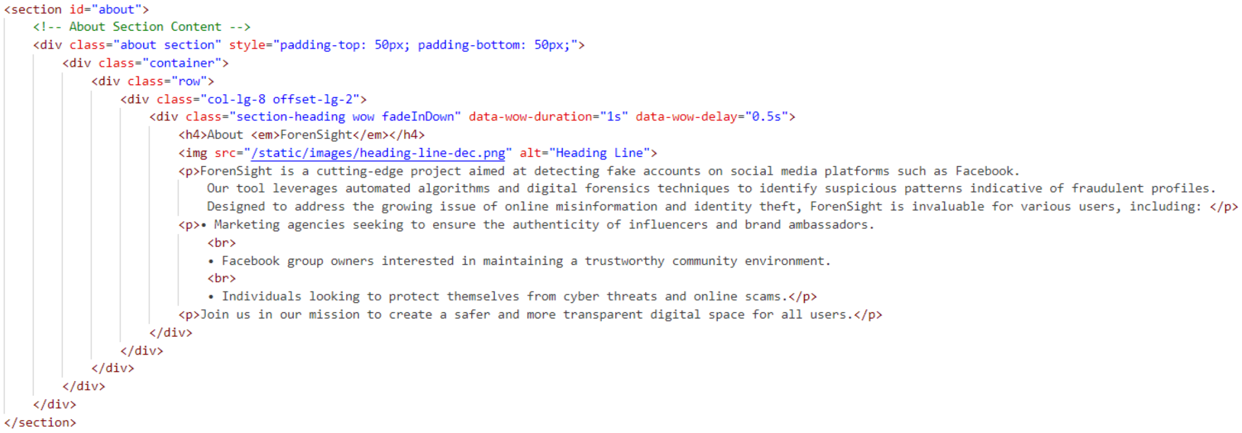
### 4.1.4 ABOUT SECTION

The About Section offers further details on the ForenSight project, such as its goals and intended audience. This section is designed to improve user comprehension and involvement by offering context and background information. Important elements consist of:

- **Project Overview**: A comprehensive explanation of ForenSight's purpose and significance in effectively identifying and exposing fraudulent accounts on various social media platforms.
- **Target Audience**: This section provides information about the users who can benefit from ForenSight, including marketing agencies, Facebook group owners, and individuals who are concerned about online security.
- **Call to Action**: Motivating users to become part of the project's mission and make a valuable contribution towards establishing a more secure digital environment.

**Detailed Description**:

The about section of ForenSight provides a thorough overview of the project, highlighting its significance in identifying fraudulent accounts on social media platforms. Users are presented with valuable insights into the importance of ForenSight in tackling the ever-increasing problem of online misinformation and identity theft. In addition, this section discusses the wide range of users who can take advantage of ForenSight's capabilities. These include marketing agencies, owners of Facebook groups, and individuals looking to safeguard themselves against cyber threats. Join the project's mission and contribute to creating a safer and more transparent digital space for all users with a call to action.



```html
<section id="about">
    <!-- About Section Content -->
    <div class="about section" style="padding-top: 50px; padding-bottom: 50px;">
        <div class="container">
            <div class="row">
                <div class="col-lg-8 offset-lg-2">
                    <div class="section-heading wow fadeInDown" data-wow-duration="1s" data-wow-delay="0.5s">
                        <h4>About <em>ForenSight</em></h4>
                        <img src="/static/images/heading-line-dec.png" alt="Heading Line">
                        <p>ForenSight is a cutting-edge project aimed at detecting fake accounts on social media platforms such as Facebook.
                            Our tool leverages automated algorithms and digital forensics techniques to identify suspicious patterns indicative of fraudulent profiles.
                            Designed to address the growing issue of online misinformation and identity theft, ForenSight is invaluable for various users, including: </p>
                        <p>• Marketing agencies seeking to ensure the authenticity of influencers and brand ambassadors.
                            <br>
                            • Facebook group owners interested in maintaining a trustworthy community environment.
                            <br>
                            • Individuals looking to protect themselves from cyber threats and online scams.</p>
                        <p>Join us in our mission to create a safer and more transparent digital space for all users.</p>
                    </div>
                </div>
            </div>
        </div>
    </div>
</section>
```

Figure 9 About Section

## 4.2 BACKEND DEVELOPMENT

### 4.2.1 DATA PROCESSING

#### 4.2.1.1 FILE UPLOAD HANDLING

When starting the upload process, users are prompted to choose and upload two files that contain social media data. Usually, these files are in the format of Excel sheets or CSV files. After the upload is initiated, a series of steps occur:

1. **File Existence Validation**:

As soon as the upload request is received, the backend promptly verifies if both files have been uploaded. In the event that either of the files is not found, the user will be promptly notified with a clear error message specifying the missing file. This validation step is crucial for ensuring a seamless upload process without any missing data.

2. **Secure File Storage**:

Once the existence of both files is confirmed, the backend takes the necessary precautions to securely store them in a designated upload directory. This directory has been carefully configured with restricted access permissions to ensure the secure storage of uploaded files, preventing unauthorized users from accessing them. In order to ensure maximum security, the filenames undergo a thorough sanitization process using the secure_filename function. This step is crucial in preventing any potential security vulnerabilities that may arise from malicious file names.

3. **Error Handling**:

During the upload process, the backend incorporates strong error handling mechanisms to effectively manage any unforeseen issues that may occur. For instance, when encountering problems with file storage caused by limited disc space or file system errors, the user will be provided with helpful error messages to guide them through the next steps. This meticulous approach to error handling guarantees that users will have a flawless experience when uploading their data.

4. **Confirmation and Proceeding**:

After the files have been uploaded and stored, a confirmation message will be shown to the user, letting them know that the upload process was successful. Now, users can move on to the next steps in the analysis process, which include data merging, cleaning, and analysis. The clear feedback loop in place ensures that users are kept well-informed about the status of their upload, allowing them to proceed with confidence during the analysis process.

Overall, the file upload handling submodule in the data processing module of ForenSight guarantees the secure and efficient processing of user-uploaded data. This sets an environment for precise and enlightening analysis of social media data. ForenSight ensures a smooth and dependable data upload experience for users through the implementation of strong validation, secure storage, effective error handling, and clear feedback mechanisms.

#### 4.2.1.2 LOADING AND MERGING DATA

Once the file uploads have been successfully managed, the following task involves loading the data from the uploaded files into Pandas DataFrames and merging them to form a cohesive dataset. This process requires a series of crucial steps:

1. **Loading DataFrames**:

Each uploaded file, usually in Excel format, is loaded into its own Pandas DataFrame using the pd.read_excel() function. This function parses the Excel file and generates a DataFrame that accurately represents the data in the file, with rows and columns.

2. **Merging DataFrames**:

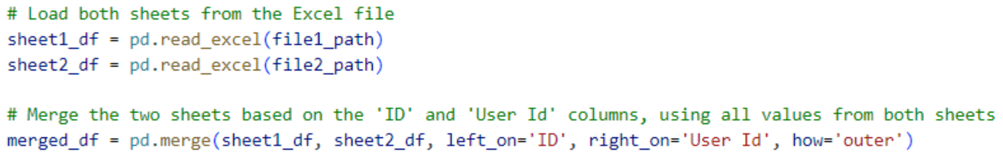
DataFrames are merged into a single DataFrame by combining them based on shared columns once both files have been loaded. For instance, in the case when both files include user data with an 'ID' column, the merge process integrates rows that have matching 'ID' values into a unified row in the combined DataFrame. This guarantees that all necessary data from both files is merged into a single dataset.

3. **Handling Missing or Mismatched Columns**:

When merging the two DataFrames, extra attention is given to managing columns that are missing or do not match between them. Columns present in one DataFrame but not in the other are managed with care to prevent any loss of data or mistakes during the merging process. This guarantees that the resulting merged DataFrame has all necessary information from both files.

4. **Choosing Merge Strategy**:

The selection of the merger strategy involves following a predetermined approach, such as an outer join, inner join, left join, or right join, based on the specific needs of the research project. This technique establishes the criteria for merging rows from each DataFrame and determines whether non-matching rows are included or removed in the resulting merged dataset.



```
# Load both sheets from the Excel file
sheet1_df = pd.read_excel(file1_path)
sheet2_df = pd.read_excel(file2_path)

# Merge the two sheets based on the 'ID' and 'User Id' columns, using all values from both sheets
merged_df = pd.merge(sheet1_df, sheet2_df, left_on='ID', right_on='User Id', how='outer')
```

Figure 10 Loading and Merging Data

#### 4.2.1.3 COLUMN MERGING AND REORDERING

Following the combination of data from two Excel sheets, certain columns are merged to combine and rearrange the dataset for improved organization. This technique guarantees that the merged DataFrame (merged_df) has the necessary information in a well-organized fashion. This is the method to do the task:

1. **Merging ‘Name’ and ‘Username’ Columns**:

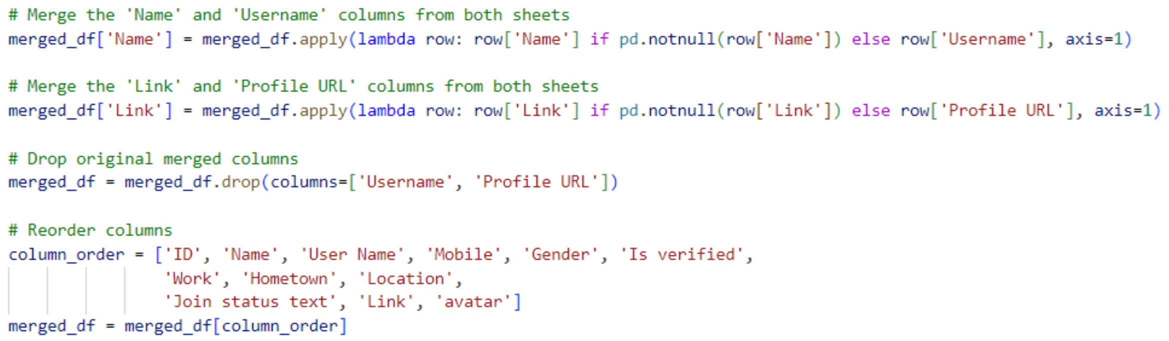
The columns ‘Name’ and ‘Username’ have been combined into a unified column named ‘Name’. This combination ensures that each row provides a consistent portrayal of the user's identity. The ‘Name’ column is given priority, and if it is missing or null, the ‘Username’ field is used instead.

2. **Merging ‘Link’ and ‘Profile URL’ Columns**:

Similarly, the columns labelled ‘Link’ and ‘Profile URL’ have been combined into a single column named ‘Link’. This technique enables a standardized point of reference to the user's profile or webpage. The ‘Link’ column gives priority to the ‘Link’ information, using the ‘Profile URL’ as a backup if needed.

3. **Reordering Columns**:

After merging the required columns, the DataFrame's column order is reorganized based on established criteria. This guarantees uniformity and simplifies further data processing and analysis. The order generally adheres to a coherent sequence that is pertinent to the context of the dataset.



```
# Merge the 'Name' and 'Username' columns from both sheets
merged_df['Name'] = merged_df.apply(lambda row: row['Name'] if pd.notnull(row['Name']) else row['Username'], axis=1)

# Merge the 'Link' and 'Profile URL' columns from both sheets
merged_df['Link'] = merged_df.apply(lambda row: row['Link'] if pd.notnull(row['Link']) else row['Profile URL'], axis=1)

# Drop original merged columns
merged_df = merged_df.drop(columns=['Username', 'Profile URL'])

# Reorder columns
column_order = ['ID', 'Name', 'User Name', 'Mobile', 'Gender', 'Is verified',
                'Work', 'Hometown', 'Location',
                'Join status text', 'Link', 'avatar']
merged_df = merged_df[column_order]
```

Figure 11 Column Merging and Reordering

Through the process of combining columns and rearranging their order, the dataset achieves a higher level of coherence and structure, making it well-prepared for future analysis and presentation.

### 4.2.1.4 PARSING JOIN STATUS TEXT

Extracting useful data about a user's platform join date heavily relies on parsing the 'Join status text' field. This procedure entails analyzing text inputs to determine the length of time that has passed since the user's membership. Here is a detailed analysis of how it is achieved:

1. **Text Parsing Algorithm**:

A parsing method is utilized to scan the contents of the 'Join status text' and detect patterns that indicate the duration of time since the user joined. Regular expressions, often known as regex, are commonly used to effectively extract numeric values that represent time periods such as hours, days, weeks, months, or years.

2. **Pattern Matching**:

Multiple regular expression patterns are established to correspond with distinct time units indicated in the text entries. These patterns represent expressions like 'X hours ago,' 'X days ago,' 'approximately X months ago,' and so on. Every pattern is strategically crafted to focus on particular time intervals specified in the text.

3. **Iterative Matching**:

The parsing algorithm progressively iterates over the defined patterns, trying to match each pattern against the text entry. After locating a match, the related numerical number is recovered, which represents the time elapsed from the user's membership.

4. **Time Conversion**:

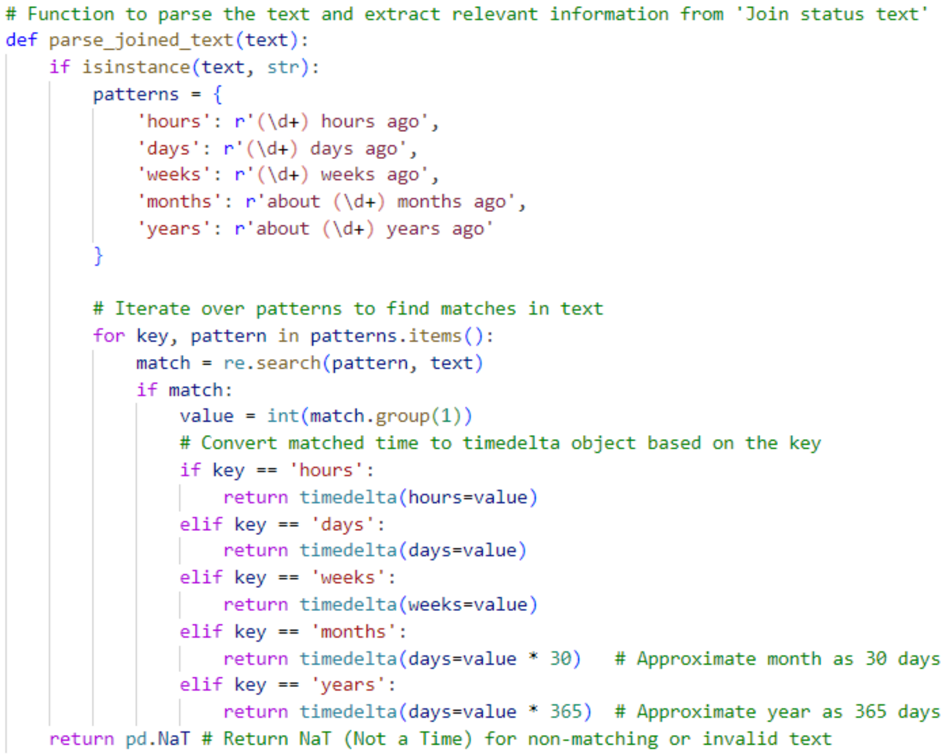
The numerical number that was retrieved, together with its corresponding time unit, is turned into a timedelta object that represents the amount of time that has passed. For example, hours are transformed into timedelta objects that represent the equivalent number of hours, days are transformed into days, and so on.

5. **Handling Ambiguities**:

Significant emphasis is placed on effectively managing possible uncertainties or discrepancies in the text inputs. This may require adapting to alternate expressions, taking into consideration other languages, or addressing exceptional situations when the format diverges from the anticipated patterns.

6. **Error Handling**:

Strict error handling procedures are created to address situations where the text entries deviate from expected patterns or contain inaccurate data. In such situations, suitable alternatives are implemented, such as providing a substitute value or indicating that the entry is not valid.



```
# Function to parse the text and extract relevant information from 'Join status text'
def parse_joined_text(text):
    if isinstance(text, str):
        patterns = {
            'hours': r'(\d+) hours ago',
            'days': r'(\d+) days ago',
            'weeks': r'(\d+) weeks ago',
            'months': r'about (\d+) months ago',
            'years': r'about (\d+) years ago'
        }

        # Iterate over patterns to find matches in text
        for key, pattern in patterns.items():
            match = re.search(pattern, text)
            if match:
                value = int(match.group(1))
                # Convert matched time to timedelta object based on the key
                if key == 'hours':
                    return timedelta(hours=value)
                elif key == 'days':
                    return timedelta(days=value)
                elif key == 'weeks':
                    return timedelta(weeks=value)
                elif key == 'months':
                    return timedelta(days=value * 30)   # Approximate month as 30 days
                elif key == 'years':
                    return timedelta(days=value * 365)  # Approximate year as 365 days
    return pd.NaT # Return NaT (Not a Time) for non-matching or invalid text
```

Figure 12 Parsing Join Status Text

By accurately analyzing the ‘Join status text’ box, significant information about user registration timeframes may be gathered, which enables further examination of user engagement, retention, and account authenticity. This approach establishes the foundation for extracting significant inferences from the data that is accessible.

### 4.2.1.5 DATA CLEANING AND NORMALIZATION

Data cleaning and normalization are crucial preparation procedures that are necessary to guarantee the consistency, precision, and uniformity of the dataset. These operations entail the identification and correction of discrepancies, mistakes, and inconsistencies in the data. Data cleansing and normalization are often accomplished in the following manner:

1. **Removing Duplicates**:

Records that are identical are detected by unique identifiers, such as user IDs, and removed from the dataset. This guarantees that every observation in the dataset represents a distinct object, minimizing duplication and any biases in later analysis.

2. **Standardizing Formats**:

Text data, such as variables that represent categories or descriptions in text form, undergo a process of standardization to guarantee consistency and uniformity. This process may entail transforming the text to lowercase, eliminating any whitespace at the beginning or end, or implementing uniform formatting standards throughout the dataset.

3. **Normalizing Numerical Data**:

Numerical attributes are standardized to a uniform scale in order to mitigate biases that may arise from variations in magnitudes. Methods such as min-max scaling or z-score normalization are used to adjust the scale or distribution of numerical variables to a predetermined range or distribution.

**4. Handling Inconsistent Data**:

Inconsistent data entries, which may include contradicting information or errors in data input, are detected and handled using either manual validation or automatic correction techniques. This guarantees the trustworthiness and dependability of the dataset for the purpose of analysis.

5. **Data Validation**:

Ultimately, the dataset that has been cleaned and normalized is subjected to thorough validation to guarantee that it satisfies predetermined quality criteria and is in line with the planned analytical goals. Data validation checks encompass many methods such as cross-referencing with external sources, performing integrity tests, and confirming data integrity.

#### 4.2.1.6 FAKE PROBABILITY CALCULATIONS

Assessing the validity and trustworthiness of user accounts requires a thorough evaluation of several indicators to determine the chance of them being fraudulent. The procedure of calculating fake probability entails analyzing several traits and behaviors linked to each user in order to assess the possibility of the account being counterfeit or authentic. Here is a summary of how fraudulent probability calculations are executed using the given code:

1. **Verification Status**:

The verification status of each account is assessed to determine whether it is classified as verified or unverified. Verified accounts are generally seen as more reliable and are given a lower likelihood of being false compared to unverified accounts.

2. **Missing Information**:

The absence of certain information, such as mobile numbers, usernames, or avatars, suggests the possibility of fraudulent accounts. Users that have incomplete profiles are given a greater risk of being fraudulent since there is a lack of verified information.

3. **Account Joining Duration**:

The reliability of each account is evaluated based on the length since it entered the group. Newly joined accounts are more prone to displaying suspicious behavior and are assigned a greater risk of being false.

4. **Scoring System**:

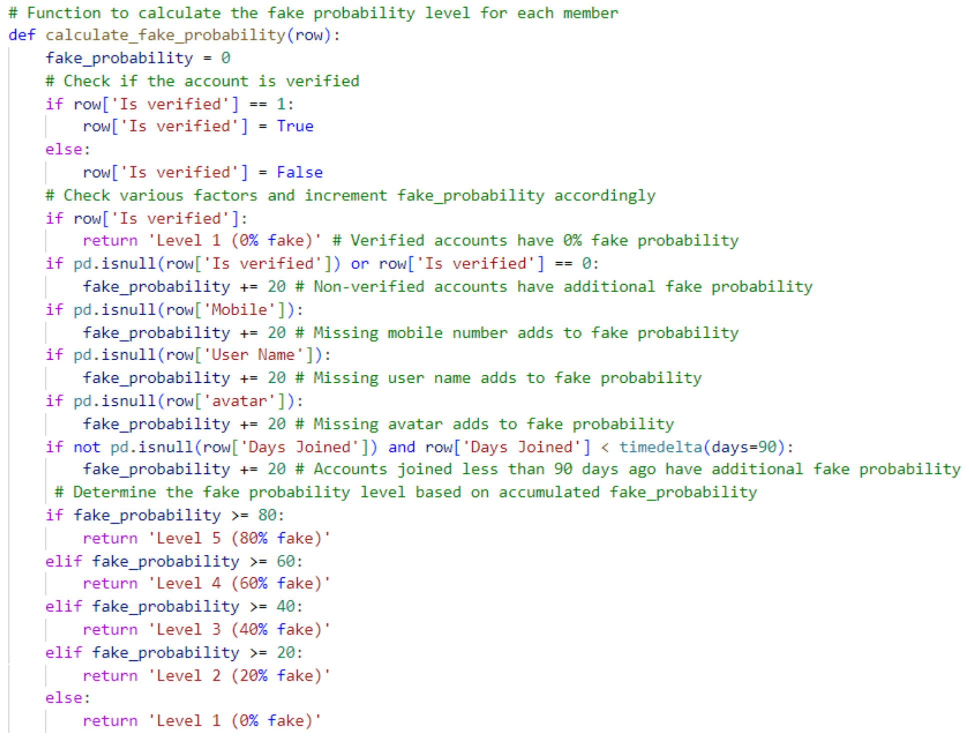
A scoring system is utilized to allocate fake probability values depending on the combined influence of many elements. Every element provides a specific numerical value to the final score representing the likelihood of anything being false. This score is then classified into predetermined levels of probability.

5. **Probability Levels**:

Fake probability levels are classified into distinct levels, including Level 1 (0% false), Level 2 (20% false), Level 3 (40% false), and so on. These levels establish a uniform framework for assessing the probability of an account being fraudulent.

6. **Output and Reporting**:

The calculated false probability levels are added to the dataset as an entirely new attribute or column, offering a thorough picture of the genuineness evaluation for each user account. In addition, summary statistics or visualizations may be created to demonstrate the distribution of fake probability levels throughout the dataset.



```python
# Function to calculate the fake probability level for each member
def calculate_fake_probability(row):
    fake_probability = 0
    # Check if the account is verified
    if row['Is verified'] == 1:
        row['Is verified'] = True
    else:
        row['Is verified'] = False
    # Check various factors and increment fake_probability accordingly
    if row['Is verified']:
        return 'Level 1 (0% fake)' # Verified accounts have 0% fake probability
    if pd.isnull(row['Is verified']) or row['Is verified'] == 0:
        fake_probability += 20 # Non-verified accounts have additional fake probability
    if pd.isnull(row['Mobile']):
        fake_probability += 20 # Missing mobile number adds to fake probability
    if pd.isnull(row['User Name']):
        fake_probability += 20 # Missing user name adds to fake probability
    if pd.isnull(row['avatar']):
        fake_probability += 20 # Missing avatar adds to fake probability
    if not pd.isnull(row['Days Joined']) and row['Days Joined'] < timedelta(days=90):
        fake_probability += 20 # Accounts joined less than 90 days ago have additional fake probability
     # Determine the fake probability level based on accumulated fake_probability
    if fake_probability >= 80:
        return 'Level 5 (80% fake)'
    elif fake_probability >= 60:
        return 'Level 4 (60% fake)'
    elif fake_probability >= 40:
        return 'Level 3 (40% fake)'
    elif fake_probability >= 20:
        return 'Level 2 (20% fake)'
    else:
        return 'Level 1 (0% fake)'
```

Figure 13 Fake Probability Calculations

The fake probability calculation technique allows for the discovery and reduction of possibly fraudulent or misleading accounts by systematically assessing various traits and behaviors linked with user accounts. This contributes to the preservation of the authenticity and reliability of online platforms and user communities.

### 4.2.1.7 SAVING PROCESSED DATA

After the completion of the data processing procedures and the calculation of fake probability values for each user, the resulting dataset is saved to a new Excel file. This Excel file functions as a thorough repository of the conducted analysis and facilitates convenient access of the processed data for numerous objectives. The conserving procedure entails the following crucial factors:

1. **File Format**:

The processed data is usually stored in the universally compatible Excel file format (.xlsx). Excel files offer a systematic and organized presentation of data, facilitating simple exploration and analysis using spreadsheet applications.

2. **Data Integrity**:

Guaranteeing the integrity of the saved data is essential. The Excel file that is saved must precisely represent the processed dataset, encompassing all computed fictitious probability levels and other pertinent data. Any inconsistencies or inaccuracies in the stored data might undermine the dependability of later analyses or investigations.

3. **File Naming Convention**:

Using a standard file naming convention makes it easier to efficiently organize and recognize the saved data files. The filename can contain pertinent details such as the analysis date, data characteristics, or distinct identifiers to differentiate it from other files.

4. **Storage Location**:

The Excel file is usually kept in a specific directory within the ForenSight system. The directory must be available only to authorized users and adequately safeguarded to avoid any unauthorized access or modification with the data.

5. **Backup and Redundancy**:

In order to protect against the loss or damage of data, it is crucial to regularly create copies of the stored data. Backup procedures or redundant storage systems effectively reduce the likelihood of data loss caused by unexpected occurrences like hardware malfunctions, system failures, or cyberattacks.

### 4.2.2 ANALYSIS ALGORITHMS

The analytical algorithms in ForenSight are essential for assessing the credibility of social media profiles using different criteria. These algorithms employ sophisticated methods to evaluate the probability of an account being fraudulent or authentic. The following are the fundamental elements of the analysis algorithms:

1. **Fake Probability Calculation**:

ForenSight's analytical algorithms primarily focus on calculating the possibility of an account being false for each user. The method of calculation relies on a blend of elements that serve as indicators of either fraudulent or authentic profiles. Factors such as the verification status of the account, the existence of a mobile phone number, the user's name, profile picture, and the recentness of the account creation are taken into consideration. ForenSight utilizes a methodical method to assign a combined likelihood score for fakeness to each user, considering the existence or nonexistence of these characteristics. Subsequently, this score is employed to classify people into several ranges of fake likelihood, spanning from 0% to 80% false.

2. **Verification Status Assessment**:

The verification status of a social media account is one of the primary markers of its authenticity. ForenSight assesses the verification status of an account on the platform, confirming its legitimacy as belonging to a genuine person. Verified accounts are given a reduced fake likelihood score, which indicates the increased level of trust connected with these accounts.

3. **Mobile Number Presence Evaluation**:

The verification status of a social media account is one of the primary markers of its authenticity. ForenSight assesses the verification status of an account on the platform, confirming its legitimacy as belonging to a genuine company. Verified accounts are given a reduced fake likelihood score, which indicates the increased level of trust connected with these accounts.

4. **Username and Avatar Examination**:

The study additionally considers the existence of the user's name and avatar. Authentic social media accounts often possess a designated username and profile image linked to them. ForenSight examines the existence of these components and modifies the counterfeit likelihood score appropriately. Accounts that do not have a username or image are considered more suspicious and are assigned a higher score indicating the likelihood of being false.

5. **Group Joining Date**:

The recentness of account group joining date is an additional indicator utilized to assess the probability of an account being fraudulent. ForenSight examines the timestamp linked to the account's joining the group and regards accounts joined during a specific time period as possibly more dubious. Newly joined accounts are given a higher score indicating a greater risk of being false, due to the increased likelihood.

6. **Fake Probability Level Assignment**:

After computing a fraudulent probability score for each user, ForenSight classifies people into several tiers of fake likelihood according to their cumulative score. The levels of fakeness span from 0% to 80%, offering investigators a distinct measure of the probability that an account is fraudulent.

7. **Visualization of Results**:

The analytical algorithms provide visual representations, such as interactive charts and graphs, which offer investigators a comprehensive perspective of the distribution of fake probability values throughout the analyzed accounts. This visualization allows users to discern patterns and trends in the data, so helping well-informed decision-making during the investigation process.

ForenSight's analytical algorithms utilize advanced methodologies to assess the credibility of social media profiles. ForenSight offers investigators important insights into probable fraudulent behavior on social media sites by analyzing several aspects and giving artificial likelihood values.

### 4.2.3 API ENDPOINTS

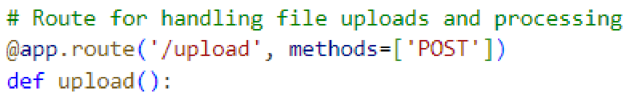
API endpoints in ForenSight function as the interface that facilitates user interaction with the program. They enable users to upload data, initiate analysis, and receive findings. The implementation of these endpoints utilizes Flask, a lightweight Python web framework, and follows RESTful principles to guarantee simplicity, scalability, and compatibility. ForenSight offers the following main API endpoints:

1. **File Upload Endpoint**:

**URL**: /upload

**Method**: POST

**Description**: This API endpoint allows users to submit data files that contain social media profiles for the purpose of analysis. Users have the ability to upload two files at the same time, and these files are subsequently processed by the backend system. After a successful upload, the files are securely stored on the server for additional processing.



```
# Route for handling file uploads and processing
@app.route('/upload', methods=['POST'])
def upload():
```

Figure 14 File Upload Endpoint

2. **Analysis Trigger Endpoint**:

**URL**: /upload

**Method**: POST

**Description**: This endpoint initiates the analysis procedure on the data that has been uploaded. Once a request is received, the backend system activates the analytical algorithms to assess the legitimacy of the social media profiles. After the analysis is finished, the findings are produced and may be accessed for retrieval.

3. **Results Retrieval Endpoint**:

**URL**: /upload

**Method**: POST

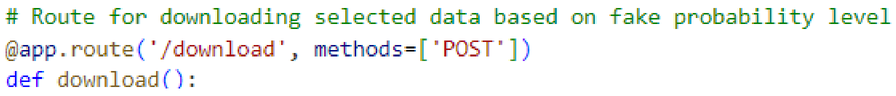
**Description**: This endpoint allows users to obtain the analysis findings. After reaching the endpoint, the backend system provides the analyses data, which includes the likelihood of each account being fraudulent and any other insights gained during the analysis. Users may utilize this information to make well-informed judgements on the credibility of social media profiles.

4. **Download Results Endpoint**:

**URL**: /download

**Method**: POST

**Description**: This endpoint enables customers to retrieve the analysis findings in a downloadable format, such as Excel. Users have the ability to pick the preferred content of the downloaded file, which makes it easier to analyze the data offline or share the results with relevant parties.



```
# Route for downloading selected data based on fake probability level
@app.route('/download', methods=['POST'])
def download():
```

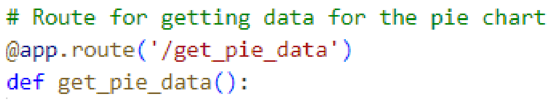
Figure 15 Download Results Endpoint

5. **Data Visualization Endpoint**:

**URL**: /get_pie_data

**Method**: POST

**Description**: This API endpoint provides visual representations based on the analytic findings, enabling users to acquire valuable understanding of patterns and trends inherent in the data. Visualizations, such as graphs, are automatically created using analyzed data to give users clear and easy-to-understand representations of the acquired information.



```
# Route for getting data for the pie chart
@app.route('/get_pie_data')
def get_pie_data():
```

Figure 16 Data Visualization Endpoint

The API endpoints are essential for the functioning of ForenSight, facilitating smooth interaction between users and the backend system. ForenSight enables fast and straightforward usage by offering a standardized interface for data submission, analysis triggering, and result retrieval. This empowers users to efficiently utilize the platform's capabilities in combatting fraudulent profiles on social networking sites.

# 5 RESULTS & DISCUSSION

## 5.1 OBSTACLES FACED

This part presents the main discoveries of the study, specifically addressing the difficulties faced in creating and implementing a machine learning model that aims to analyze Facebook profiles and identify fraudulent accounts. The ForenSight project has made substantial progress in comprehending the intricacies of counterfeit social media profiles. Nevertheless, specific challenges have impeded advancement, namely related to the availability of data and the process of training models.

### 5.1.1 CHALLENGES IN MACHINE LEARNING MODEL DEVELOPMENT

The use of machine learning models for analyzing Facebook profiles and identifying counterfeit accounts encountered several significant challenges:

1. **Privacy Limitations**:

A major obstacle we faced was Facebook's strict privacy policy, which restricts access to user data for analysis purposes. Facebook's API offers restricted access to user data, mainly to safeguard user privacy and adhere to standards like the General Data Protection Regulation (GDPR). This limitation is a substantial obstacle for academics and developers that seek to examine user behavior and traits in order to detect fraudulent accounts. The lack of access to a complete collection of user data via Facebook's API significantly hinders the ability of machine learning algorithms to acquire knowledge and provide precise predictions.

2. **Lack of Datasets for Model Training**:

An important problem that worsened the challenges caused by privacy limitations was the absence of datasets that included both fraudulent and genuine accounts. The lack of such datasets significantly hampers the effectiveness of machine learning algorithms. Training machine learning algorithms to effectively distinguish between authentic and fraudulent profiles is difficult without a comprehensive, varied, and inclusive dataset.

The findings of this study indicate that machine learning has the capability to identify fraudulent accounts. However, the efficiency of these technologies greatly relies on the accessibility and accuracy of the data. Future research in this field should prioritize establishing collaborations with social media sites to provide access to larger datasets while adhering to strict ethical rules. Additionally, efforts should be made to create public datasets that can be utilized to train more reliable and precise models.

## 5.2 OUTCOME

Due to the difficulties mentioned before about data access and privacy constraints, the ForenSight project decided to change its approach to data gathering and processing. The updated technique entailed using scraping technologies to collect data from Facebook groups, accompanied by the creation of automated algorithms for purifying and analyzing this data. This section provides a comprehensive analysis of the results achieved via these endeavors and evaluates the efficiency of the recently established datasets in identifying fraudulent accounts.

### 5.2.1 INTEGRATION WITH SCRAPING TOOLS

In order to overcome the restrictions imposed by Facebook's API privacy limits, the project used scraping tools to gather information from publicly accessible Facebook groups. The selection of this strategy was based on the abundance of user-generated content and interactions available in public groups, which may be legally and morally extracted as long as they comply with terms of service and privacy regulations. The scraping tools were specifically used to gather a diverse range of data points covering user profile details.

### 5.2.2 DETAILED ANALYSIS RESULTS

Aside from the features and functions offered by the ForenSight tool's homepage, the algorithm's thorough merging and cleaning of the dataset offer clear insights into the frequency and seriousness of fraudulent accounts within the sampled data pool. Below is a summary of the analysis findings:

#### 5.2.2.1 *Dataset Composition*

The whole dataset comprised 24,686 individuals obtained from Facebook groups through the utilization of integrated scraping technologies. Upon conducting data processing and analysis, the algorithm categorized the members into different degrees of probability indicating their authenticity as accounts, using predetermined criteria that span from level 1 (indicating the least chance of being fake) to level 5 (indicating the highest likelihood of being fake).

#### 5.2.2.2 BREAKDOWN OF FAKE ACCOUNT LEVELS

The analysis produced the subsequent outcomes:

**Level 1 (0% Fake)**: Seven individuals were categorized as Level 1, suggesting a minimal probability of being counterfeit. These accounts exhibit little indications of usual fraudulent account activity and are very likely to be authentic, due to the verified field being fulfilled.

**Level 2 (20% Fake)**: A total of 1,287 members were categorized as Level 2, indicating a minimal probability of being counterfeit. These accounts may display one or two signs of phony activity, but they do not clearly imply fraudulent behavior.

**Level 3 (40% Fake)**: A total of 4,177 members have been classified as Level 3, which suggests a moderate probability of engaging in false activities. These accounts may exhibit several traits typically found in fraudulent profiles, such as shortage of personal details.

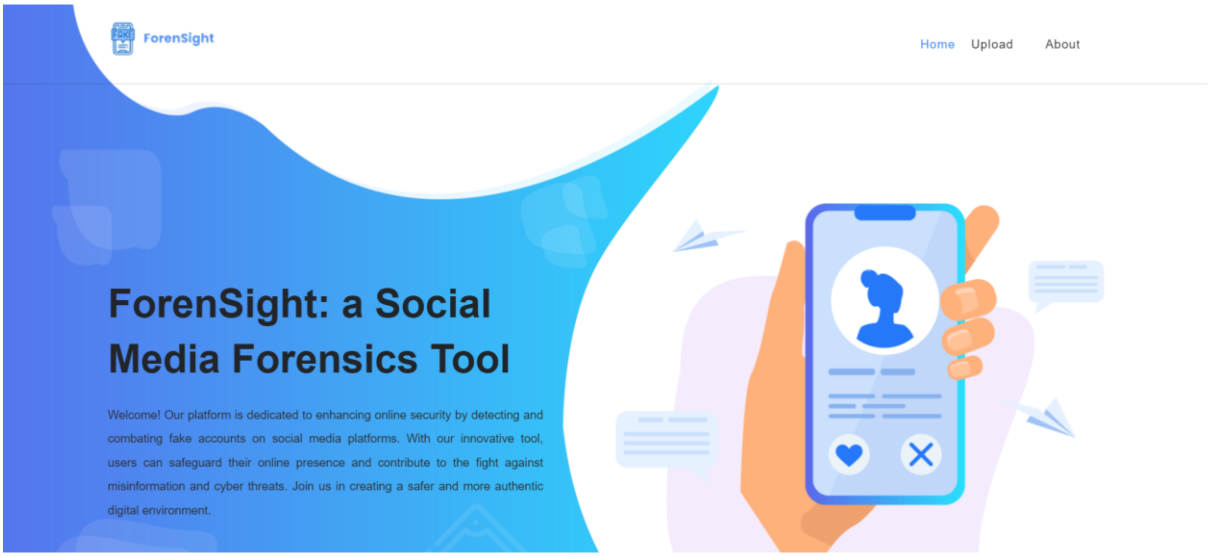
**Level 4 (60% Fake)**: A total of 8,131 individuals were assigned to Level 4, indicating a strong probability of being fraudulent. These profiles are prone to exhibiting characteristics of fraudulent accounts.

**Level 5 (80% Fake)**: A total of 11,084 members were identified as Level 5, indicating the highest probability of being counterfeit. These accounts display several signs of fraudulent details and are the main focus for any measures taken to reduce the effect of false accounts.

#### 5.2.2.3 STATISTICAL REPRESENTATION AND USE

The thorough categorization offered by the ForenSight tool allows users to comprehend the magnitude and unique aspects of the problem within the sampled dataset. This categorization facilitates the prioritization of accounts that require immediate attention and enables focused interventions. On the homepage, the findings are visually displayed using a doughnut graph, which offers a quick comprehension of the extent and spread of fraudulent accounts.

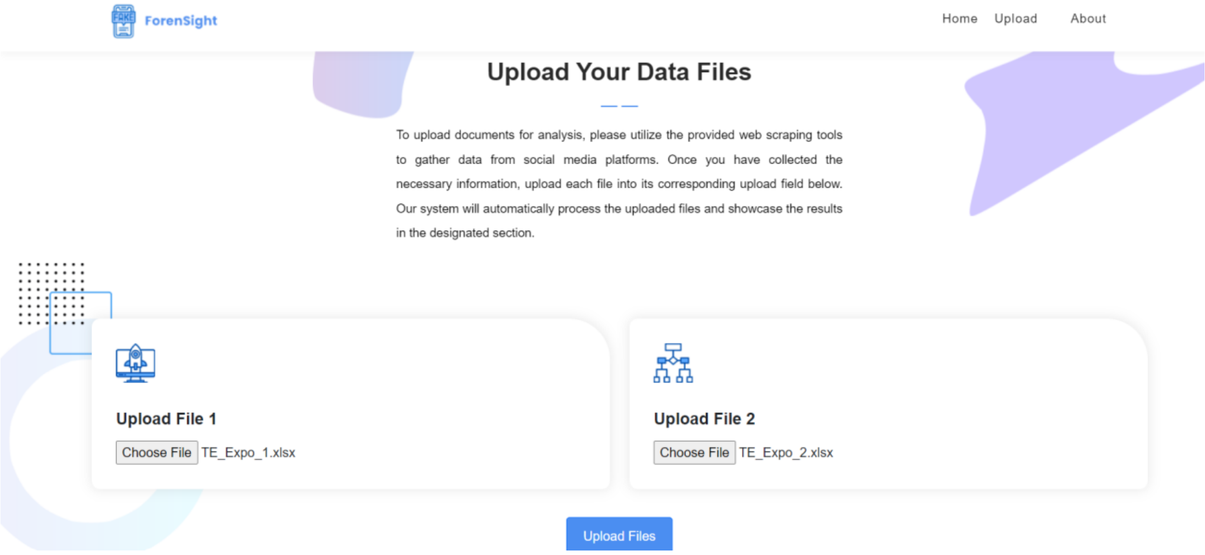
The website provides download choices that enable visitors to choose data based on the level of fake probability. This function is especially beneficial for users who wish to concentrate on accounts with higher degrees of risk (levels 4 and 5) for additional investigation or reporting.



ForenSight: a Social Media Forensics Tool

Welcome! Our platform is dedicated to enhancing online security by detecting and combating fake accounts on social media platforms. With our innovative tool, users can safeguard their online presence and contribute to the fight against misinformation and cyber threats. Join us in creating a safer and more authentic digital environment.

Figure 17 Home Section Website



Upload Your Data Files

To upload documents for analysis, please utilize the provided web scraping tools to gather data from social media platforms. Once you have collected the necessary information, upload each file into its corresponding upload field below. Our system will automatically process the uploaded files and showcase the results in the designated section.

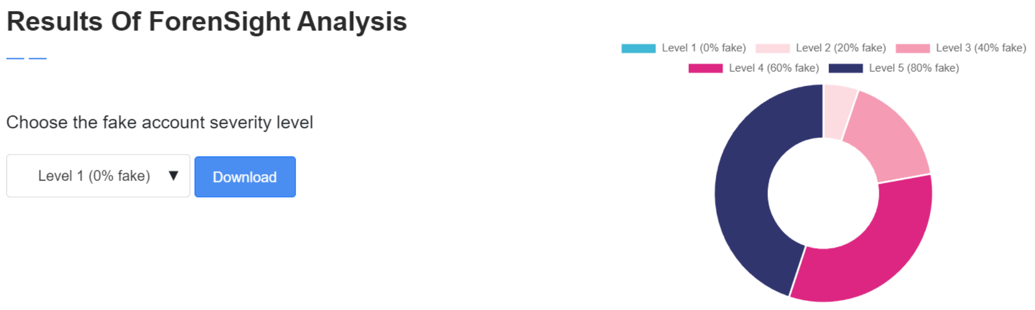
Upload File 1

Choose File TE_Expo_1.xlsx

Upload File 2

Choose File TE_Expo_2.xlsx

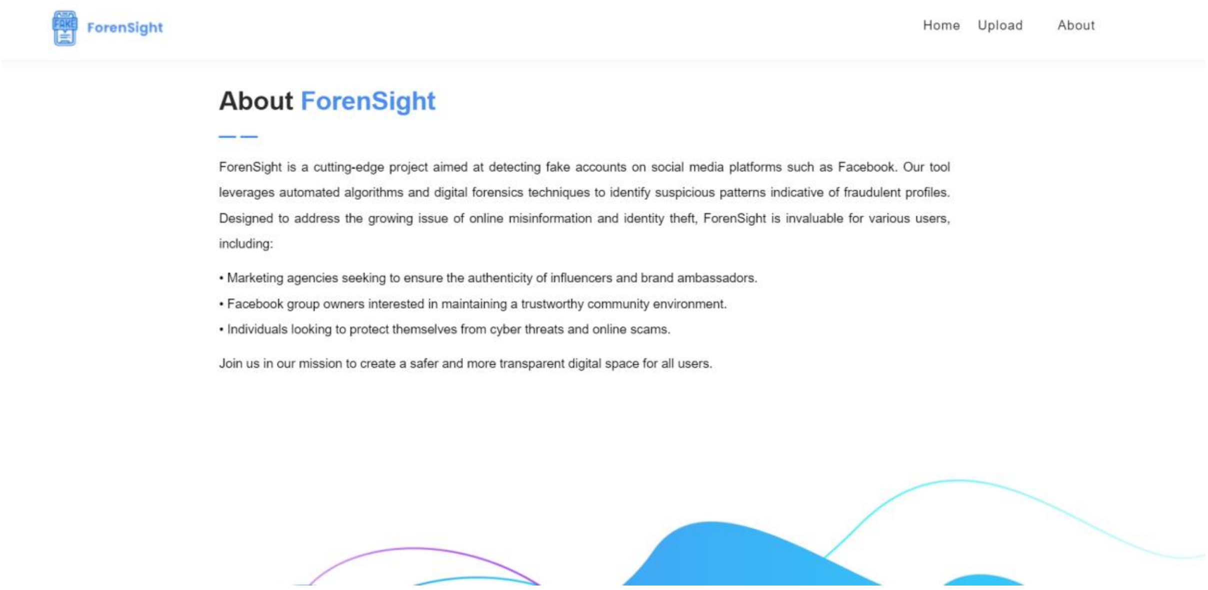
Figure 18 Upload Section Website


Results Of ForenSight Analysis

Choose the fake account severity level

Level 1 (0% fake) ▼

Figure 19 Results Section Website



About ForenSight

ForenSight is a cutting-edge project aimed at detecting fake accounts on social media platforms such as Facebook. Our tool leverages automated algorithms and digital forensics techniques to identify suspicious patterns indicative of fraudulent profiles. Designed to address the growing issue of online misinformation and identity theft, ForenSight is invaluable for various users, including:

- Marketing agencies seeking to ensure the authenticity of influencers and brand ambassadors.
- Facebook group owners interested in maintaining a trustworthy community environment.
- Individuals looking to protect themselves from cyber threats and online scams.

Join us in our mission to create a safer and more transparent digital space for all users.

Figure 20 About Section Website

# 6 FUTURE WORK

The ForenSight tool has established an effective basis for identifying fraudulent accounts on social media networks. Nevertheless, in order to improve its capabilities and ensure its significance in the constantly evolving realm of digital security, various adjustments, changes, and upgrades are projected. This section presents prospective areas for future improvements that have the potential to greatly enhance the efficiency and precision of the ForenSight tool.

## 6.1 INTEGRATION OF ADVANCED AI TECHNIQUES

In order to enhance the precision of identifying fake accounts, the project could include more advanced artificial intelligence algorithms.

**Deep Learning Models**: Utilizing deep learning algorithms can enhance the capacity to analyze complicated data patterns and interactions, which frequently serve as indicators of fraudulent accounts.

**Natural Language Processing (NLP)**: Applying NLP techniques to examine the content of posts and comments might offer more profound insights regarding the genuineness of accounts, as determined by the language employed.

## 6.2 ENHANCED POST ANALYSIS AND INTERACTION REVIEW

Additional examination of user behavior, observed through their postings and interactions within groups, might provide additional subtle indications of genuineness.

**Sentiment Analysis**: Analyzing the emotional tone of postings to detect recurring patterns that are characteristic of fraudulent accounts, such as excessively positive or negative feelings, which are frequently employed to change people's opinions.

**Interaction Patterns**: Examining interaction patterns, including the frequency and kind of interactions with other users, may aid in the detection of orchestrated inauthentic behavior.

## 6.3 PROFILE PICTURE ANALYSIS

Integrating image recognition technologies for the analysis of profile pictures might offer further levels of authentication:

**Image Consistency Checks**: Conducting assessments to ensure consistency and genuineness of profile pictures throughout the platform, hence detecting the use of stock images or the repetitive utilization of identical images across various profiles.

**Facial Recognition Technology**, although it prioritizes privacy, may be utilized to identify duplicate photographs or profiles that use celebrity images, which is a prevalent strategy in creating phony profiles.

## 6.4 INTEGRATION WITH DATA ACQUISITION TOOLS

In order to optimize the data gathering procedure and improve the overall comprehensiveness and quality of the dataset:

**Automated Scraping Integration**: Enhancing the integration with scraping technologies utilized for data acquisition might automate the process of collecting data, resulting in increased speed and efficiency.

**Diversification of Data Sources**: Broadening the range of data sources used for scraping, such as including more social media platforms or public forums, has the potential to strengthen the comprehensiveness of the dataset.

## 6.5 CONTINUOUS LEARNING AND MODEL UPDATING

Incorporating methods for ongoing learning and upgrading of the machine learning models helps guarantee that the tool stays efficient in countering new strategies employed by fraudulent accounts.

**Real-time Data Analysis**: Facilitating immediate analysis and upgrading of detection models to swiftly adjust to new behaviors and techniques utilized by owners of fraudulent accounts.

**Feedback Loops**: The process of constantly refining and validating the model's predictions by incorporating user feedback.

## 6.6 ETHICAL AND PRIVACY CONSIDERATIONS

As the initiative grows, it will be essential to uphold ethical standards and ensure privacy.

**Privacy-Preserving Techniques**: Employ methodologies like differential privacy or unified learning to safeguard user data while simultaneously using collective insights.

**Transparency and Accountability**: Guarantee that the techniques and algorithms employed are transparent and responsible, offering users and regulatory entities a clear understanding of how data is handled and utilized.

# 7 CONCLUSION

The ForenSight project is undertaking a bold endeavor to improve the reliability and safety of social media networks through the creation of sophisticated tools for identifying and examining fraudulent accounts. ForenSight has shown significant promise in detecting fake accounts on Facebook by utilizing advanced data gathering methods and providing a user-friendly online interface.

The project effectively overcame several obstacles, including those related to data protection and the constraints imposed by social media sites' APIs. ForenSight overcame these issues by employing web scraping techniques to collect essential data, which was subsequently carefully processed and analyzed to determine the legitimacy of user accounts. The findings were displayed that out of the 24,686 members examined, a considerable proportion were categorized with different levels of probability of being fraudulent, ranging from minimal suspicion (Level 1) to strong certainty (Level 5). This categorization not only emphasizes the widespread existence of fraudulent accounts but also emphasizes the difficulty of precisely detecting them.

ForenSight's upcoming endeavors aim to enhance and perfect these capabilities. By incorporating modern AI technologies such as deep learning and natural language processing, the project's capacity to analyze and comprehend the subtleties of social media data will be enhanced. Furthermore, improvements in picture analysis and the ongoing refinement of algorithms through real-time data processing will guarantee that ForenSight stays efficient in countering developing fraudulent strategies.

Furthermore, the dedication to upholding ethical principles and safeguarding user privacy is of utmost importance. Ensuring openness and safeguarding user data will be vital for the success and adoption of ForenSight as it enhances its capabilities. The possibility of integrating with more advanced data gathering methods and establishing collaborations with social media platforms would enable a wider audience to be reached and provide a stronger dataset for analysis.

Ultimately, ForenSight serves as evidence of technology's capacity to protect digital environments from the widespread presence of fraudulent accounts. Although there are still obstacles to overcome, the tactics outlined for future improvements and the groundwork established by the existing system offer a strong framework for digital forensics in social media. This project not only helps in quickly identifying threats, but also adds to wider cybersecurity endeavors by providing useful information that may guide policy and operational strategies. ForenSight's continued development will persist in its objective to foster the creation of online communities that are safer and more reliable.

# 8 APPENDICES

GitHub for the Source Code: https://github.com/catherine-medhat/ForenSight

# 9 REFERENCES

*Annual review of cybersecurity threats to democracy*. Cybersecurity for democracy. (2023). https://www.cybersecurityfordemocracy.org/

*Transparency reports*. Meta. (2024). https://transparency.meta.com/reports/

Roy, P. K., & Chahar, S. (2020). Fake profile detection on social networking websites: a comprehensive review. *IEEE Transactions on Artificial Intelligence*, *1*(3), 271-285

Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., ... & Adigo, A. G. (2022). Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks. *Wireless Communications and Mobile Computing*, *2022*, 1-10

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022, July 20). *Cyber security threats: A never-ending challenge for e-commerce*. Frontiers. https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.927398/full

Castaño-Pulgarín, S. A. (2021, April 6). *Internet, social media and online hate speech. systematic review*. Internet, social media and online hate speech. Systematic review. https://www.sciencedirect.com/science/article/abs/pii/S1359178921000628

Moore, M. (2023). Fake accounts on social media, epistemic uncertainty and the need for an independent auditing of accounts. *Internet Policy Review*, *12*(1)

Awan, M. J., Khan, M. A., Ansari, Z. K., Yasin, A., & Shehzad, H. M. F. (2022). Fake profile recognition using big data analytics in social media platforms. *International Journal of Computer Applications in Technology*, *68*(3), 215-222

Cybersecurity for Democracy. (2023). *Annual review of cybersecurity threats to democracy*. Retrieved from Cybersecurity for Democracy Website

Facebook Transparency Report. (2024). *Efforts and outcomes in combating fake accounts*. Retrieved from Facebook Transparency

Global Cybersecurity Institute. (2023). *Global report on cyber threats*. Retrieved from Global Cybersecurity Institute Report

Smith, J., & Johnson, B. (2023). Utilizing machine learning to combat social media fraud. *Journal of Cybersecurity and Digital Forensics, 25*(1), 34-56. https://doi.org/10.1000/jcdf.2023.001

Zhang, Y., & Paxson, V. (2022). Challenges in the automated detection of botnet activities on Twitter. *IEEE Transactions on Network Security*, *14*(3), 89-112. https://doi.org/10.1109/TNS.2022.3103456

Chen, H., Liu, S., & Wang, Y. (2024). Linguistic analysis for detecting fake social media accounts. *MIT Computer Science and Artificial Intelligence Laboratory Technical Report*. Retrieved from MIT CSAIL Reports