Software Design

Document

for

A.I in Digital Forensics

**Group Members:**

| **Name** | **Enrollment Number** | **Email** |
| --- | --- | --- |
| Ahana Nair | BT22GCS303 | ahana.nair22@st.niituniversity.in |
| Archana Anto | BT22GCS219 | archana.anto22@st.niituniversity.in |
| Geetika Agrawal | BT22GCS106 | geetika.agrawal22@st.niituniversity.in |
| Jagriti Singh | BT22GCS145 | jagriti.singh22@st.niituniversity.in |

| **Instructor:** | **Manish Hurkat** |
| --- | --- |
| **Course:** | **Capstone Project 1** |
| **Date:** | **20 February, 2025** |

**TABLE OF CONTENTS**

**1.Introduction**…………………………………………………………………………………3

1.1 Purpose………………………………………………………………………………3

1.2 Scope………………………………………………………………………………...3

1.3 Reference Material………………………………………………………………….3

**2.System Overview**…………………………………………………………………………..3

**3.System Architecture**………………………………………………………………………4

3.1 Decomposition Description………………………………………………………...4

3.2 Process Flow Diagram……………………………………………………………..5

3.3 Wireframe Model..............................................................................................6

## 

## **1.Introduction:**

**1.1 Purpose**

This is a comprehensive software design document (SDD) which provides cues into implementation of the project - **AI in Digital Forensics**. The system aims at users from all backgrounds (i.e. technical and non-technical) for analyzing logs, images, and documents using artificial intelligence which can assist them in case of any suspected activity in their device and network. This document provides an overview on the implementation of the project.

**1.2 Scope**

The project aims to create a web application that can help users analyze logs, images and documents for detecting any suspicious activity, image tampering or malicious content in the document.

**1.3 Reference Material:**

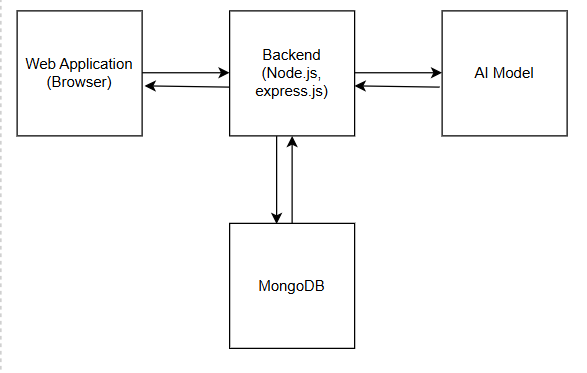
1. [*https://www.cameraforensics.com/blog/2020/03/06/a-quick-guide-to-digital-image-forensics-in-2020/*](https://www.cameraforensics.com/blog/2020/03/06/a-quick-guide-to-digital-image-forensics-in-2020/)
2. [*https://www.bluevoyant.com/knowledge-center/get-started-with-these-9-open-source-tools*](https://www.bluevoyant.com/knowledge-center/get-started-with-these-9-open-source-tools)
3. [*https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics*](https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics)

## **2.System Overview:**

The system will be a web application where users can analyze logs, images and documents for analyzing any suspicious activities in these files. The web application shall be user friendly and help users to understand the process of analysis through tutorials. For analysis the users will have to upload the file (i.e logs, images and documents) and then a comprehensive report will be generated and provided to the user.

## 

## **3.System Architecture:**



The Web Application firstly authenticates the user using the authentication details shared. It first checks and validates the details based on the data stored in the database. Once the users are authenticated the session is started. The user then according to the requirement starts the analysis by first uploading the file containing logs, images or documents. Once the file is uploaded and the AI model at the backend starts to analyze the data in the file for any malicious content or suspicious activity.

**3.1 Decomposition Description:**

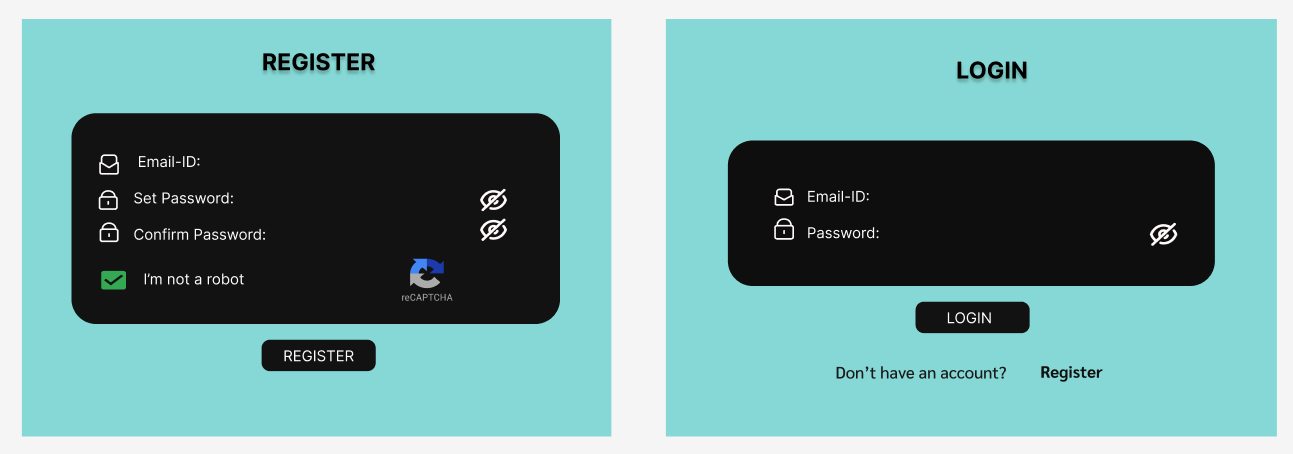
1. MongoDB: Stores the data about the user and stores the previous analysis performed.
2. Web Application: An interactive interface for the user to perform the required analysis.
3. Backend (Node.js, Express.js): Data received from the web application is further processed as required.
4. AI Model: For analyzing the file given by the user i.e logs, images or documents.

## **3.2 Process Flow Diagram:**

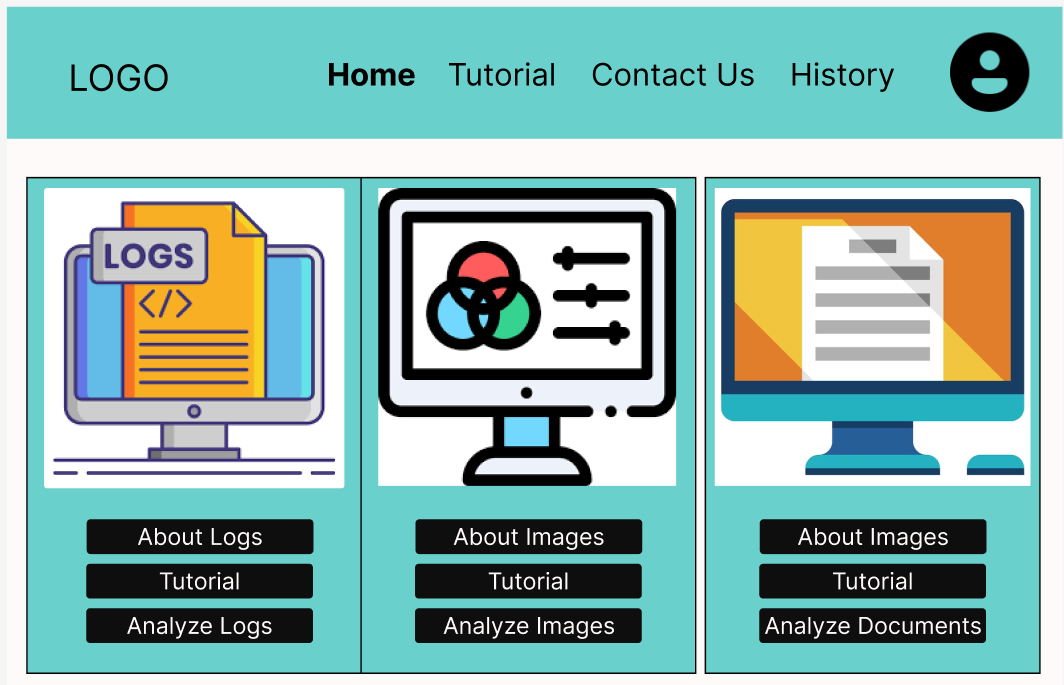
## 

## **3.3 Wireframe Model:**

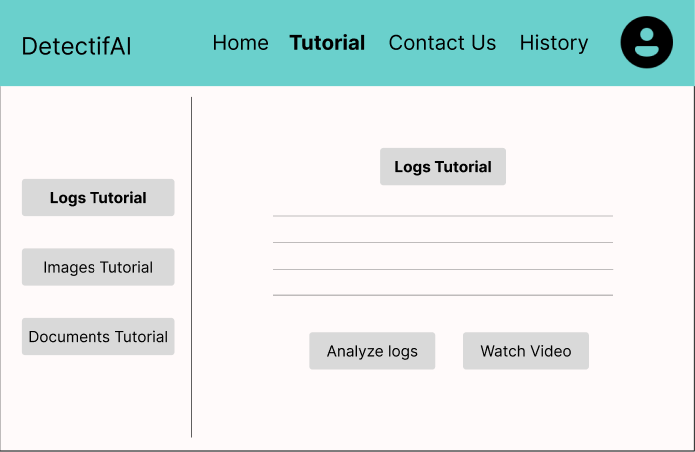
* The registration and login page

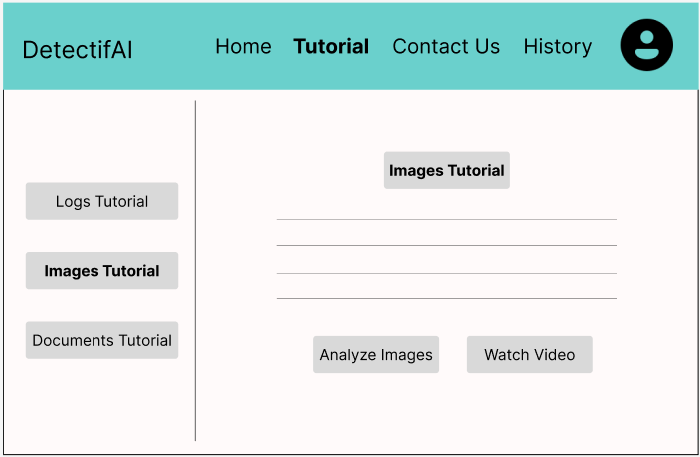


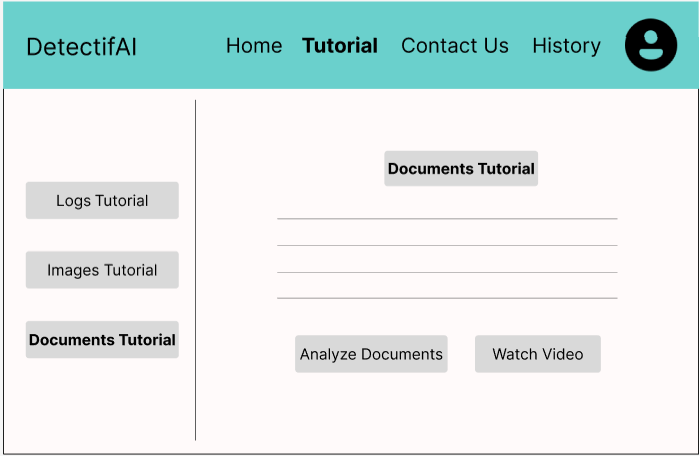
* Home page



* Tutorial Page







* Contact Us Page

