Software Requirements Specification

for

A.I in Digital Forensics

**Prepared by:**

**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:** | **23 February, 2025** |

**Contents**

**j**[**1 Introduction 1**](#_heading=h.2et92p0)

[1.1 Document Purpose 1](#_heading=)

[1.2 Product Scope 1](#_heading=)

[1.3 Intended Audience and Document Overview 1](#_heading=)

[1.4 Definitions, Acronyms and Abbreviations 1](#_heading=)

[1.5 Document Conventions 2](#_heading=)

[1.6 References and Acknowledgments 2](#_heading=)

[**2 Overall Description** 3](#_heading=)

[2.1 Product Overview 3](#_heading=h.26in1rg)

[2.2 Product Functionality 3](#_heading=)

[2.3 Design and Implementation Constraints 3](#_heading=)

[2.4 Assumptions and Dependencies 3](#_heading=)

[**3 Specific Requirements** 4](#_heading=)

[3.1 External Interface Requirements 4](#_heading=h.2jxsxqh)

[3.1.1 User Interfaces 4](#_heading=)

[3.1.2 Hardware Interfaces 4](#_heading=)

[3.1.3 Software Interfaces 4](#_heading=)

[3.2 Functional Requirements 4](#_heading=)

[3.3 Use Case Model 4](#_heading=)

[3.3.1 Use Case 1: Log Analysis 4](#_heading=)

[3.3.2 Use Case 2: Image Analysis 5](#_heading=)

[3.3.3 Use Case 3: Document Analysis 5](#_heading=)

[3.3 Class Diagram](#_heading=) 5

[**4 Other Non-functional Requirements** 5](#_heading=)

[4.1 Performance Requirements 5](#_heading=h.1ci93xb)

[4.2 Safety and Security Requirements 6](#_heading=)

[4.3 Software Quality Attributes 6](#_heading=)

[**5 Other Requirements 6**](#_heading=h.3as4poj)

**Revisions**

| **Version** | **Primary Author(s)** | **Description of Version** | **Date Completed** |
| --- | --- | --- | --- |
| Draft Type and Number | Full Name | Information about the revision. This table does not need to be filled in whenever a document is touched, only when the version is being upgraded. | 00/00/00 |

# Introduction

*The project aims to create a Web application which utilizes AI for Digital Forensics to analyze logs, images and documents.*

## Document Purpose

This document provides a comprehensive software requirements specification (SRS) for the **AI in Digital Forensics** system. 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 malicious activity in their device and network. This document defines the key functional and non-functional requirements of the application for ensuring that the user receives the accurate output.

## Product Scope

The main aim of the application is to assist users in automated analysis of any suspicious activities in logs, any tampering or hidden data in images and analyze the text or contents in documents. After the analysis the user shall receive a report which contains information like: probability of any suspicious activity and if the CIA might get compromised or not. It can help users understand the severity of the problem and resolve it at the earliest.

## Intended Audience and Document Overview

a.Users (Non-Technical): The application shall be available to users from non -

technical background for usage in daily life in case they receive any such

images or documents.

b.Users (Technical): The users belonging to technological background who might

use it for analyzing logs or suspicious activities in the network or systems.

c.The automation shall make it user friendly for everyone to use and create

reports.

## Abbreviations

* **AI** – Artificial Intelligence
* **CIA -** Confidentiality, Integrity and Availability
* **MERN** – MongoDB, Express.js, React, Node.js

## Document Conventions

**Font:** Arial

**Line Spacing:** Single

**Margins:** 1’’

## References and Acknowledgments

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)

# Overall Description

## Product Overview

A web application would be created to automate and streamline the forensics analysis process. The application shall be user friendly for users from different backgrounds to use it. The users should have the input data to be given to the application for analysis. For example, the users can upload the logs information into the application and obtain the result from the same.

The application also includes tutorials about different inputs like logs, images and documents. This would help them to explore the platform and the input types and the output for the respective input. These tutorials would also contain the video links of videos which can help users with similar ideas. Each tutorial would be with the button to analyze the respective inputs.

The history of the analyzed logs, images and documents would also be a part of the application where the respective user can see their previous activities or analysis. This can help them with rechecking their analysis and work on it in case required.

## Product Functionality

* Secure file upload and analysis
* Providing accurate tutorials for each category of input i.e. logs, images and documents.
* AI powered anomaly detection in logs.
* Image tampering detection using computer vision techniques
* Text document processing for forensic analysis using techniques from Natural Language Processing.
* Dashboard for viewing results and generating reports.
* The details and output related to the previous analysis shall be saved for the future reference for the user.

## Design and Implementation Constraints

* **MERN stack** with Python-based AI models.
* AI models require **Flask/FastAPI** integration.
* Requires a **MongoDB database** for data storage.
* Processing times must be optimized to ensure real-time analysis.

## Assumptions and Dependencies

* Users must upload **structured logs**.
* Image tampering detection works best with **JPEG/PNG** formats.
* Text analysis depends on **pre-trained NLP models**.

# Specific Requirements

## Functional Requirements

***F1: Log Analysis Module***

Description: Analysis of logs for finding any suspicious activities.

Details:

1. Uploading log files for analysis.

2. Detecting suspicious activity in the logs.

3. Provides output to the user regarding any suspicious activity.

***F2: Image Analysis Module***

Description: Analysis of images for any tampering.

Details:

1. Uploading image file (according to the specified format).

2. Detecting image tampering.

3. *Gives output to the user regarding any maliciousness in the image provided.*

***F3: Document Analysis Module***

Description: Analysis of document for malicious or suspicious content.

Details:

1. Uploading the document file (according to the specified format).

2. Detecting malicious content in the document.

3. *Tells users about the malicious or hidden content in the document.*

***F4: History of the previous analysis***

Description: Provides data regarding previous analysis completed by the user.

Details:

1. Showing reports of previous analysis.

2. Ability to edit and perform re-analysis.

## Use Case Model

### 

### Use Case 1: Log Analysis

* **Actors**: User, AI Model
* **Preconditions**: Log file uploaded.
* **Postconditions**: Log analyzed, report generated.
* **Flow of Events**: Logs are uploaded → Detects anomalies → Displays results.

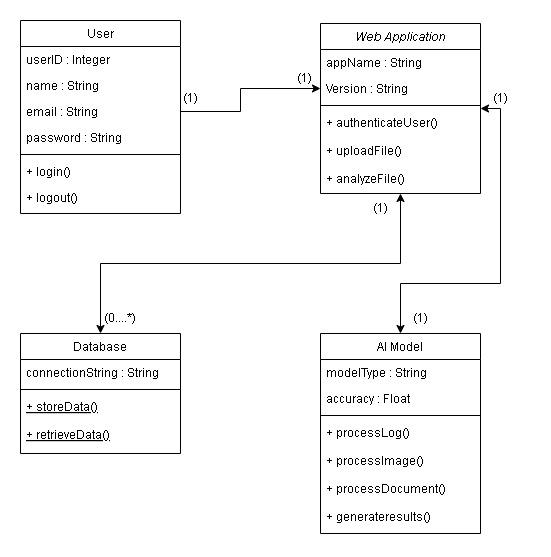
### Use Case 2: Image Analysis

* **Actors**: User, AI Model
* **Preconditions**: Image file uploaded.
* **Postconditions**: Image analyzed, forensic report generated.
* **Flow of Events**: Image is uploaded→ Detects tampering → Displays results.

### Use Case 3: Document Analysis

* **Actors**: User, AI Model
* **Preconditions**: Document file uploaded.
* **Postconditions**: Document analyzed, forensic insights extracted.
* **Flow of Events**: Document is uploaded→ Extracts insights → Displays results.

## 3.3 Class Diagram



# Other Non-functional Requirements

## Performance Requirements

* Algorithms should be efficient and faster in performing the analysis .
* The model used should be accurately providing results.
* The user interface should be responsive.

## Safety and Security Requirements

* **Secure Authentication:** securing authentication of the users to their account.
* **Secure Uploading and storage of data**
* **Secure API calls** (HTTPS).
* System logs all forensic activities for audit purposes.

## Software Quality Attributes

* **Reliability**: System should handle **high-volume forensic data**.
* **Scalability**: Supports multiple concurrent users.
* **Usability**: Intuitive dashboard with clear forensic insights.
* **Maintainability**: Modular code structure for easy updates.

**Appendix A - Group Log**

