FINAL PROJECT PROPOSAL

# Project Title: Deepfake Detection

---

Track name: AI & Data Science - Microsoft Machine Learning Engineer

Instructor: Eman El-galad Round

Code: GIZ3_AIS2_S2

Submitted by:

- Mohab Hamdy Saleh Mustafa (Team Leader)
- Ahmed Sief Al-Aslam
- Mohamed Ragab Abo-Baker
- Youssef Ezzat Abd-Shafy
- Omar Mustafa Omar
- Osama Abd-Rahman Saad

Date: 10/2025

## 1. Project Description

The Deepfake Detection project aims to develop an intelligent system capable of detecting manipulated videos and images generated using deep learning techniques such as Generative Adversarial Networks (GANs). With the rapid rise of synthetic media and AI-generated content, deepfakes pose serious threats to privacy, security, and public trust.

This project leverages machine learning and computer vision algorithms to analyze facial features, motion inconsistencies, and visual artifacts to classify content as real or fake. By training a convolutional neural network (CNN) or transformer-based model on large-scale datasets like FaceForensics++ and DeepFake Detection Challenge (DFDC), the system will learn to accurately identify subtle manipulations that are difficult for humans to detect.

The ultimate goal is to build a web-based tool that allows users to upload media and instantly receive a deepfake authenticity analysis, helping organizations and individuals verify digital content credibility and mitigate the spread of misinformation.

## 2. Group Members & Roles

| Names | IDs | Roles & Contributions |
|---|---|---|
| Mohab Hamdy Saleh Mustafa (Team Leader) | 21065472 | • Team coordination and task planning<br>• Data preprocessing and feature extraction<br>• Model design, training, and performance evaluation<br>• Model deployment and integration supervision<br>• Documentation and presentation management |
| Ahmed Sief Al-Aslam | 21011557 | • Data cleaning and augmentation<br>• Model training and optimization using TensorFlow<br>• Evaluation and comparison between different models<br>• Contribution to project documentation |
| Mohamed Ragab AboBaker | 21000751 | • Dataset preparation and balancing<br>• Support in model development and testing<br>• Performance monitoring and result analysis<br>• Report writing and data visualization |
| Youssef Ezzat AbdShafy | 21009275 | • Data preprocessing and integration with model pipeline<br>• Support in result interpretation and visualization<br>• Preparing project presentation materials<br>• Documentation and teamwork coordination |

| | | |
|---|---|---|
| | | |
| Omar Mustafa Omar | 21098126 | • Research on deepfake detection techniques and |
| | | related work<br>• Assistance in data labeling and organization<br>• Model deployment and integration supervision<br>• Contributing to report and presentation design |
| Osama Abd-Rahman Saad | 21011952 | • Data preprocessing and augmentation<br>• Model testing and evaluation support<br>• Contribution to performance tracking and reporting<br>• Documentation and result summarization |

Collaboration Methodology: All team members work collaboratively in pairs, with each pair building upon the work of previous pairs. Every member contributes across all project phases, ensuring comprehensive involvement and knowledge sharing throughout the development lifecycle.

## 4. Objectives

a. Collect and prepare data:
   Gather and preprocess datasets of real and fake videos/images from trusted public sources such as the DeepFake Detection Challenge (DFDC) and FaceForensics++.
b. Develop and train detection models:
   Design, implement, and train deep learning models — such as CNNs or Vision Transformers (ViT) to accurately distinguish between real and manipulated media.
c. Evaluate and optimize performance:
   Assess model performance using metrics like accuracy, precision, recall, and F1-score, and fine-tune hyperparameters to enhance reliability and reduce false detections.
d. Build a user-friendly interface:
   Develop a web-based application that allows users to upload videos or images for real-time deepfake analysis and detection results.
e. Deploy and test the complete system:

Integrate the trained model into a cloud-based or local deployment environment, ensuring scalability, efficiency, and real-world usability.

f. Promote awareness and ethical AI use:
Highlight the importance of detecting deepfakes to support digital safety, authenticity, and trust in online media.

## 5. Tools & Technologies

a. Programming Languages: Python, JavaScript.
b. Frameworks & Libraries: TensorFlow, Keras, OpenCV, Flask, React.
c. Dataset: DeepFake Detection Challenge (DFDC) / FaceForensics++.
d. Environment: Google Colab / Jupyter Notebook / Kaggle.
e. Deployment: Streamlit, Flask API, Docker, AWS / Render.

## 6. Stakeholder Analysis

The Deepfake Detection project involves multiple stakeholders who influence the design, implementation, and impact of the system. The following table outlines each stakeholder, their interests, influence level, needs, and engagement approach.

| **Stakeholder** | **Role / Interest** | **Influence / Priority** | **Needs / Expectations** | **Engagement /Communication** |
|---|---|---|---|---|
| End Users (Journalists, Investigators, General Public) | Use the tool to verify the authenticity of videos or images before sharing or publishing. | High | Accurate detection (Real/Fake), confidence score, simple and fast user interface, data privacy. | User-friendly interface, educational content, and post-use feedback surveys. |
| Media Agencies / Social Media Platforms / Cybersecurity Firms | Integrate the detection tool into their systems to prevent misinformation and verify content authenticity. | High | High accuracy, detailed detection reports, accessible API, strong data protection and privacy policies. | Demonstrations, API documentation, progress reports, and collaboration meetings. |

| | | | | |
|---|---|---|---|---|
| Development Team / Researchers | Responsible for building, training, and maintaining the deepfake detection model and web system. | Medium–High | Clean and balanced dataset, effective development environment, performance monitoring, and version control. | Weekly sync meetings, GitHub issue tracking, and internal technical documentation. |
| Instructor / Evaluator | Provides academic supervision, evaluation, and feedback on project progress and deliverables. | High | Clear objectives, consistent progress updates, and final deliverables including trained model, web demo, and report. | Progress reports, milestone reviews, and presentation meetings. |

## 7. Milestones & Deadlines

| Milestones | Description | Deadlines |
|---|---|---|
| M1: Project Planning & Research | Conduct a literature review on deepfake technologies, existing detection methods, and relevant datasets. Finalize the project scope and requirements. | 29 Sep.2025 |
| M2: Dataset Collection & Preprocessing | Gather real and fake media samples from DFDC and FaceForensics++ datasets. Perform cleaning, labeling, and augmentation for balanced data. | 6 Oct.2025 |
| M3: Model Design & Training | Develop and train deep learning models (CNN, XceptionNet, or ViT) for deepfake classification. Experiment with hyperparameters for best performance. | 25 Oct.2025 |

| | | |
|---|---|---|
| M4: Evaluation & Optimization | Test the model using validation data, measure accuracy, F1-score, and latency, and optimize for improved detection performance. | 1 Nov.2025 |
| M5: Web Application Development | Build and integrate a user-friendly web interface (React + Flask) for uploading and analyzing videos or images. | 7 Nov.2025 |
| M6: Deployment & Final Testing | Deploy the model to a cloud platform (e.g., Render or AWS), perform user testing, and prepare final documentation and presentation. | 10 Nov.2025 |

## 8. KPIs (Key Performance Indicators)

A. Data Quality

| Metric | Description | Expected Result |
|---|---|---|
| Missing Values Handled | Percentage of missing or incomplete data successfully identified and handled during preprocessing. | 98% |
| Data Accuracy After Preprocessing | Degree of correctness and consistency of data after cleaning, normalization, and augmentation. | 95% |
| Dataset Diversity | Measures the variation in samples, ensuring the dataset includes different genders, ethnicities, lighting, and backgrounds. | 90% |

B. Model Performance

| Metric | Description | Expected Result |
|---|---|---|
| Model Accuracy | Proportion of correct classifications among total predictions (real vs. fake). | ≥ 90% |
| F1-Score | Harmonic mean of precision and recall, representing model balance and reliability. | ≥ 0.90 |
| Latency per Image | Average time required to process and classify one image or video frame. | % |

| | | |
|---|---|---|
| | | |

C. Deployment & Scalability

| Metric | Description | Target / Result |
|---|---|---|
| API Uptime | Measures the system's availability and reliability during continuous operation. | ≥ 99% (Goal) |
| Response Time | Time taken for the API to return detection results after receiving input. | ≤ 2000ms (Goal) |

D. Practical Impact

| Metric | Description | Target / Result |
|---|---|---|
| Reduction in Manual Verification | Percentage decrease in time or effort needed for manual fake-content verification compared to baseline. | % |
| User Satisfaction | Percentage of positive feedback received from users during testing and evaluation phases. | % |

## 9. UI/UX Design (Using Streamlit)

**1. Objective:**

The purpose of the UI/UX design is to create a clean, intuitive, and interactive interface that allows users to easily interact with the system. Streamlit was selected as the framework because it provides a fast and simple way to build web applications with a strong focus on usability and data visualization.

**2. Interface Structure:**

The interface is organized into several main sections to ensure clear navigation and engaging user experience:

1. **Header:**
   Displays the project title and a short description of the system or its purpose.
2. **Sidebar (Navigation):**
   Allows the user to navigate between sections such as *Home*, *About*, *Visualization*, and *Main Features*.
3. **Main Content Area:**
   Displays the selected page content dynamically, depending on the user's navigation choice.
4. **About Section:**
   Introduces the project, its purpose, and background.
   Includes details about the development team (names, roles, and contact information).
5. **Visualization Section:**
   Allows users to view and interact with visual representations of the project's data or results.
   This includes charts, graphs, and metrics explaining how the system processes or analyzes the data.
6. **Footer:**
   Displays version information, acknowledgments, or useful links.

**3. User Experience (UX) Considerations**

To ensure smooth and efficient user experience, the following design principles are applied:

- Simple and minimal layout for easy navigation.
- Consistent use of colors and spacing for readability.
- Interactive widgets (buttons, sliders, dropdowns) for data input.
- Real-time updates and feedback without page reload.
- Clear labels and error messages for better usability.