Capstone Project Proposal Presentation

Department of Computer Science and Engineering
Thapar Institute of Engineering and Technology

HAVDEF

Hindi Audio Visual Deepfake Defense

CPG NO:207

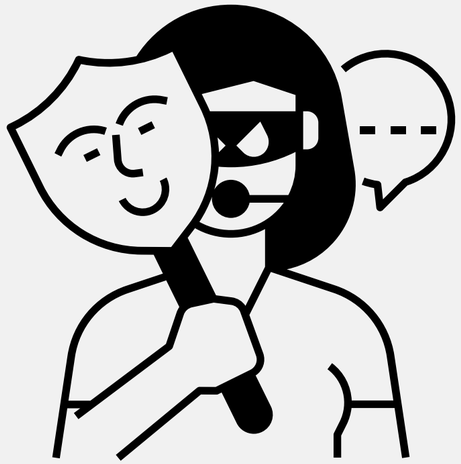
Team Members:

Shivane Kapoor	102203191
Kaustubh Singh	102203194
Japneet Singh	102203205
Arpit Jain	102203499
Diwakar Sood	102253002

Our Mentors:

Dr Seema Bawa (Professor)

Dr Sachin Kansal (Assistant Professor)



Project Overview

AI defense system

HAVDEF is a real-time deepfake detection system protecting against AI voice scams. It analyzes audio, identifying deepfake inconsistencies for immediate alerts

Targeted Hinglish Detection

HAVDEF includes a specialized module for Hinglish (Hindi-English) scams, identifying unique linguistic patterns for enhanced accuracy.

Real Time Alerts

HAVDEF is a real-time deepfake detection system protecting against AI voice scams. It analyzes audio, identifying deepfake

Need Analysis

1

Rise in AI Fraud Calls

Increasing cases of scammers using deepfake voice technology to impersonate trusted individuals.

2

Real-Time Gap

Existing deepfake detection tools focus on videos, not live phone conversations

3

Hinglish Challenges

Most fraud detection systems struggle with mixed Hindi-English speech
patterns.

Literature Survey

1. Key Technologies in Deepfake Detection:-

- **Speech Pattern Analysis:** Detects unnatural rhythm, pitch, and pause timing in AI-generated voices.
- **Feature Extraction & Spectrogram Analysis:** Uses spectrograms to analyze frequency, amplitude, and phase variations.
- **Machine Learning Models:** CNNs, Transformers, and Wav2Vec2 improve deepfake detection accuracy.
- **Language-Specific Detection:** Adapts models for Hinglish phonetics, intonation, and grammar patterns.
- **Real-Time Processing & Noise Reduction:** Enhances detection clarity in noisy phone call environments.

2. Existing Deepfake Audio Detection Systems:-

- **WavLM Model Ensemble:** Uses deep learning for voice pitch and tone analysis.
- **BTS-E Model:** Focuses on breathing, talking rhythms, and silence inconsistencies.
- **Speech Pause Pattern Analysis:** Identifies deepfake voices based on unnatural pauses.
- **Spectrogram-Based Detection:** Uses visual frequency patterns to differentiate AI and real voices.

Feature	Existing Technology	HAVDEF
Detection Approach	✅ML/DL models (CNNs, RNNs, spectrogram analysis)	✅Real-time AI-based fraud detection
Language Support	❌English/Hindi only	✅Hinglish (Hindi-English mix)
Dataset	✅ Pre-recorded speech datasets	✅Custom-built Hinglish fraud call dataset
Real-Time Detection	❌Offline analysis, no real-time support	✅Real-time fraud detection & alerts
Deployment Feasibility	❌Research-based, no real-world applications	✅Practical mobile app for real use
Fraud Call Focus	❌ Generic deepfake detection	✅ Explicitly targets AI-based fraud calls

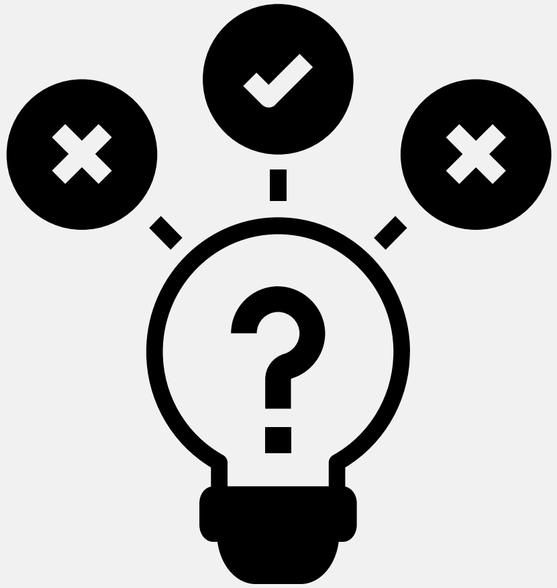
Problem Statement:

- AI-generated deepfake voices are increasingly used for **fraudulent phone calls.**
- Existing solutions **fail to detect** deepfake voices in **real time.**
- **Hinglish** conversations pose additional challenges for speech analysis.
- The goal is to develop an AI model that instantly identifies **deepfake calls** and **alerts users**.

Objective:

1. Develop an AI-powered deepfake detection model for **real-time fraud detection.**
2. Ensure **Hinglish language support** by training models on Hinglish speech datasets.
3. Implement a real-time fraud alert system that warns users about **AI-generated calls.**
4. Optimize the system for **mobile devices** to enable seamless integration.

Assumptions & Constraints



Assumptions:-

- AI fraud calls use cloned voices to impersonate real people.
- Hinglish is the dominant language in Indian phone scams.
- Users need real-time alerts to prevent fraud.
- Deepfake detection requires advanced AI models trained on diverse datasets.

Constraints:-

- Real-time processing is crucial – Detection must happen instantly.
- Limited Hinglish deepfake datasets – Hinglish-specific training data is scarce.
- Integration challenges – The system must work with existing mobile apps.
- Trade-off between accuracy and speed – AI models must balance detection speed and reliability.

Project Execution Plan

Data Collection & Preprocessing

- Collect real & AI-generated Hinglish voice samples from datasets like ASVspoof.
- Preprocess data to remove noise and enhance clarity.

Model Development

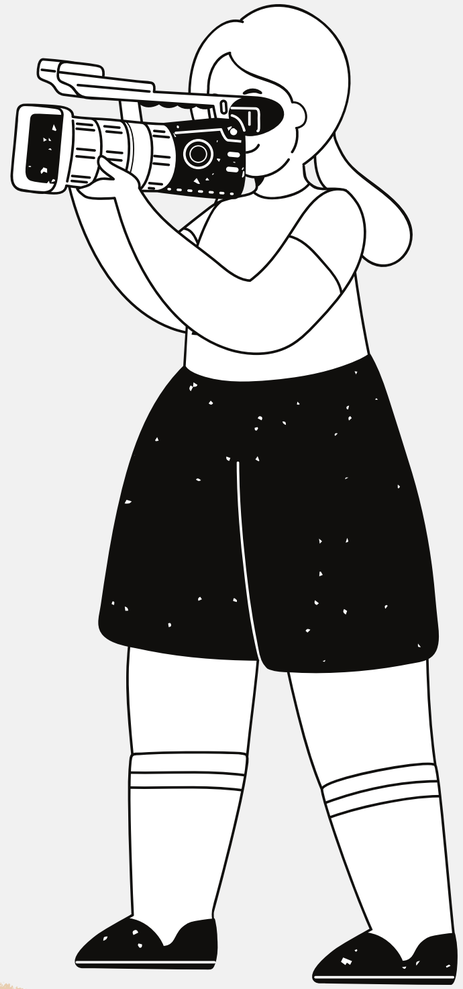
- Train deepfake detection models using Wav2Vec2, Whisper, and CNNs.
- Fine-tune models for Hinglish accents and speech patterns.

Real-Time Call Security

- Monitor phone calls and analyze speech features in real time.
- Compare voice signals to AI detection models

Fraud Alert System

- Notify users immediately if an AI-generated call is detected.
- Provide recommendations (e.g., hang up, verify identity).



Software & Platforms:

Programming Language:
Python

Machine Learning Frameworks:
TensorFlow

App Development:
Flutter , MongoDB

Datasets
FakeCatcher, Custom Hinglish dataset

Expected Project Outcomes

1

Product:

A mobile app that detects and alerts users about deepfake fraud calls..

2

Service:

API integration for businesses Enables telecoms and banks to integrate fraud detection.

3

Impact:

Enhanced security – Prevents AI-based phone scams.
Increased awareness – Educates users about AI-driven fraud.

Work Plan &Timeline

Phase 1

(Jan 2025 – Feb 2025)

Requirement Analysis & System Design

- Identify fraud patterns in AI-generated voice scams.
- Define system architecture and Hinglish-specific detection techniques.

Phase 2

(Mar 2025 – Jun 2025)

AI Model Development & Data Collection

- Collect real & AI-generated Hinglish voice samples.
- Train deepfake detection models (Wav2Vec2, Whisper).

Phase 3

(Jul 2025 – Oct 2025)

Application Development & Integration

- Develop Android app for real-time fraud detection.
- Integrate AI models for live call analysis & fraud alerts.

Phase 4

(Oct 2025 – Dec 2025)

Testing, Optimization & Deployment

- Optimize AI models for real-time efficiency.
- Conduct user trials & deploy final version.

Team Responsibilities

Name	Roles	
Shivane Kapoor	Data Preparation & Preprocessing	Model Development
Kaustubh Singh	Speech Processing	Documentation
Japneet Singh	Data Collection	Frontend & Backend
Arpit Jain	Model Development	Testing & Optimization
Diwakar Narayan Sood	Frontend & Backend	Documentation

References

- J. Yi, C. Wang, J. Tao, X. Zhang, C. Y. Zhang, and Y. Zhao, "**Audio deepfake detection: A survey**," *arXiv preprint arXiv:2304.08531, 2023*. Available: https://arxiv.org/abs/2308.14970

- N. V. Kulangareth, J. Kaufman, J. Oreskovic, and Y. Fossat, "**Investigation of deepfake voice detection using speech pause patterns: Algorithm development and validation**," *PubMed*, 2023. [Online]. Available: https://biomedeng.jmir.org/2024/1/e56245/

- S. Kaura, M. Buhari, N. Khandelwal, P. Tyagi, and K. Sharma, "**Hindi audio-video-deepfake (HAV-DF)**: A Hindi language-based audio-video deepfake dataset," *arXiv preprint*, 2023. [Online]. Available: https://arxiv.org/abs/2411.15457

- K. Bhatia, A. Agrawal, P. Singh, and A. K. Singh, "**Detection of AI synthesized Hindi speech**," *arXiv preprint*, 2023. [Online]. Available: https://arxiv.org/abs/2203.03706

- A. Shetty, H. Karani, S. K. H., R. Khan, and A. G. Amruth, "**Deepfake audio detection using deep learning**," *IEEE Xplore*, 2023. [Online]. Available: https://ijarcce.com/papers/deepfake-audio-detection-using-deep-learning/

- H. H. Kilinc and F. Kaledibi, **"Audio deepfake detection by using machine and deep learning,**" *IEEE Xplore*, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10323004

- T.-P. Doan, L. Nguyen-Vu, S. Jung, and K. Hong, "**BTS-E: Audio Deepfake Detection Using Breathing-Talking-Silence Encoder,**" School of Computer Science, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10095927

Thank you very much!