SMART INDIA HACKATHON 2024

TITLE PAGE

- **Problem Statement ID -** 1683
- **Problem Statement Title -**

  Development of AI/ML based solution for detection of face-swap based deep fake videos.
- **Theme-** Miscellaneous
- **PS Category-** Software
- **Team ID -** MUJSIH064
- **Team Name -** Shenanigans

Shenanigans

VeriFace

SMART INDIA HACKATHON 2024

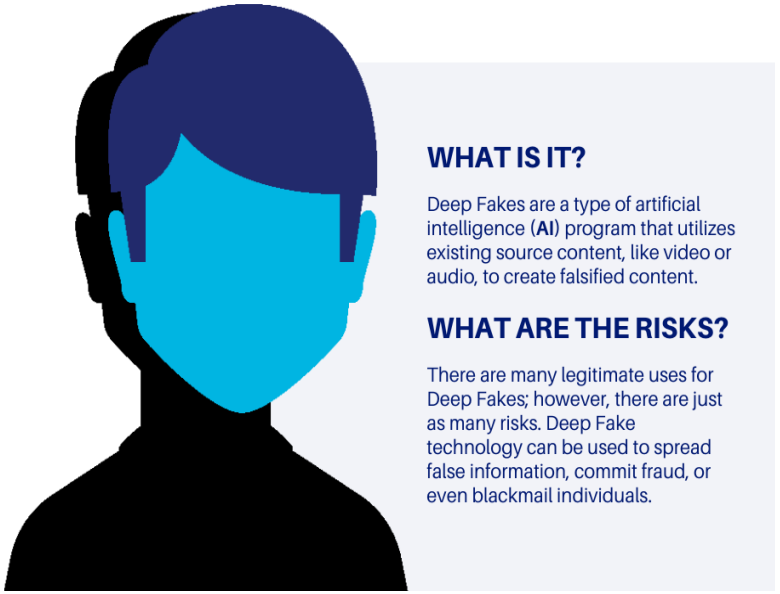
Proposed Solution

An ensemble-based model combining multiple models for both video and audio deep fake detection.

Made up of a combination of the technologies like CNNs, RNNs, Capsule Networks, etc.

With an added integration of GAN to expand training data, making the detection models more robust.

The model not only takes into consideration video abnormalities but also any audio ones and the general async in the audio/video.

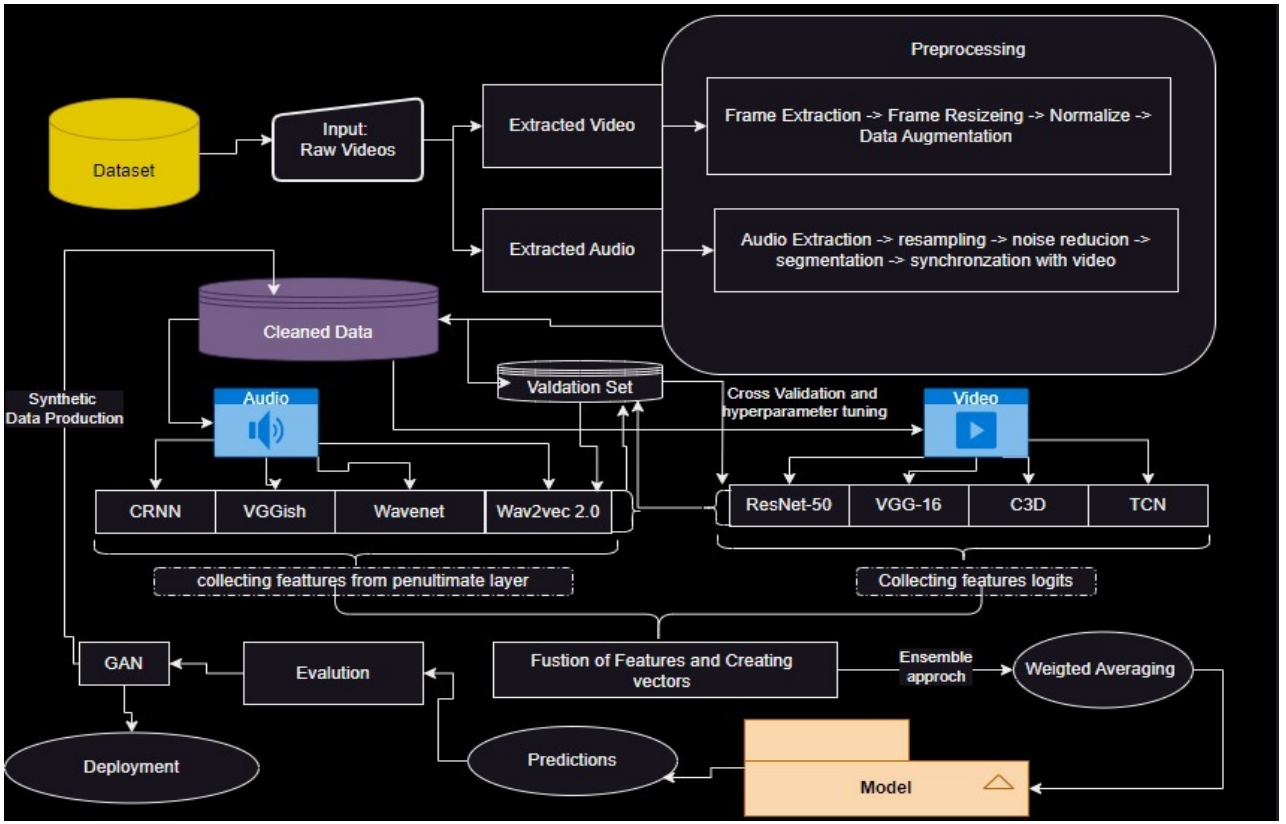


Shenanigans

TECHNICAL APPROACH

SMART INDIA HACKATHON 2024

- **Languages**: Python
- **Dataset Management**: Kaggle Datasets, Google Datasets.
- **Data Processing Libraries**: OpenCV, Librosa, NumPy, Pandas.
- **Training & Evaluation Libraries**: Scikit-learn Matplotlib, Seaborn.
- **Deep Learning Frameworks**: TensorFlow, Keras, PyTorch, Hugging Face Transformers.
- **Experiment Tracking**: Weights & Biases, MLflow.
- **Deployment Tools**: Flask/FastAPI, TensorFlow Serving, Docker, Kotlin, Android Studio.
- **Hardware**: NVIDIA GPUs (CUDA-enabled), cloud-based platforms like Google Colab or AWS.



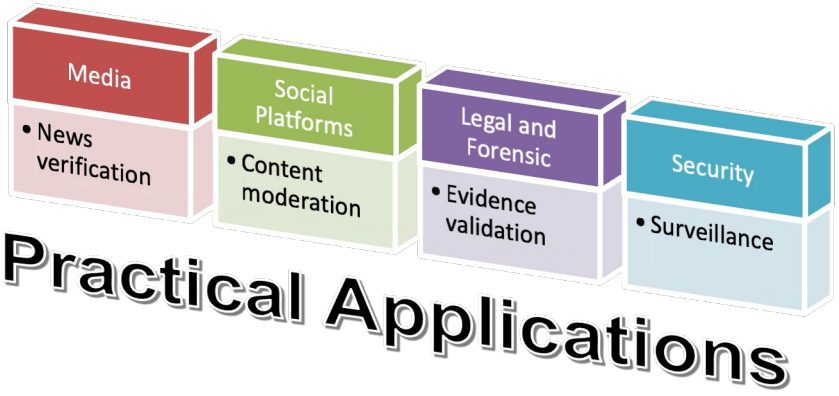
Shenanigans

FEASIBILITY AND VIABILITY

SMART INDIA HACKATHON 2024

Analysis of the feasibility of the idea:

This idea is technologically and operationally feasible, provided sufficient computational resources and time are available for training and implementation. It's highly relevant due to increasing concerns over deep fakes, making it a practical solution for various sectors.



Potential challenges & Strategies to overcome them

Incorrect classification affects trust:

Strategy: Regularly update and retrain models, combine detection methods, and use ensemble method

Evasion Techniques:

Strategy: Implement adaptive learning, collaborate with research institutions, and be updated on new evasion techniques.

Inadequate data impacts model performance.

Strategy: Use data augmentation, generate synthetic data, and utilize crowdsourcing for dataset collection

Computational Resources:

Strategy: Optimize models through quantization and pruning, leverage cloud computing, and explore efficient architecture

Shenanigans

IMPACT AND BENEFITS

SMART INDIA HACKATHON 2024

- **Privacy & Reputation Protection**: Safeguards against defamatory and harmful fake content.
- **National Security**: Prevents politically motivated deep fakes and disinformation.
- **Fraud Prevention**: Detects fake content used in financial scams.
- **Trust in Digital Media**: Ensures authenticity of online videos and media.
- **Compliance**: Helps meet regulatory requirements against synthetic media.
- **Forensics & Law Enforcement**: Aids in verifying video evidence in investigations.
- **Content Moderation**: Assists platforms in flagging deep fakes.

Shenanigans

RESEARCH AND REFERENCES

SMART INDIA HACKATHON 2024

References

- https://www.authenticid.com/glossary/deep-fakes/

Research

- https://ieeexplore.ieee.org/document/9721302
- https://www.researchgate.net/publication/336058980_Deep_Learning_for_Deepfakes_Creation_and_Detection_A_Survey