Baderia Global Institute of Engineering and Management, Jabalpur, Madhya Pradesh 482002

BADERIA GLOBAL THE BEST Institute of Engineering & Management

BrahmaX 1.0

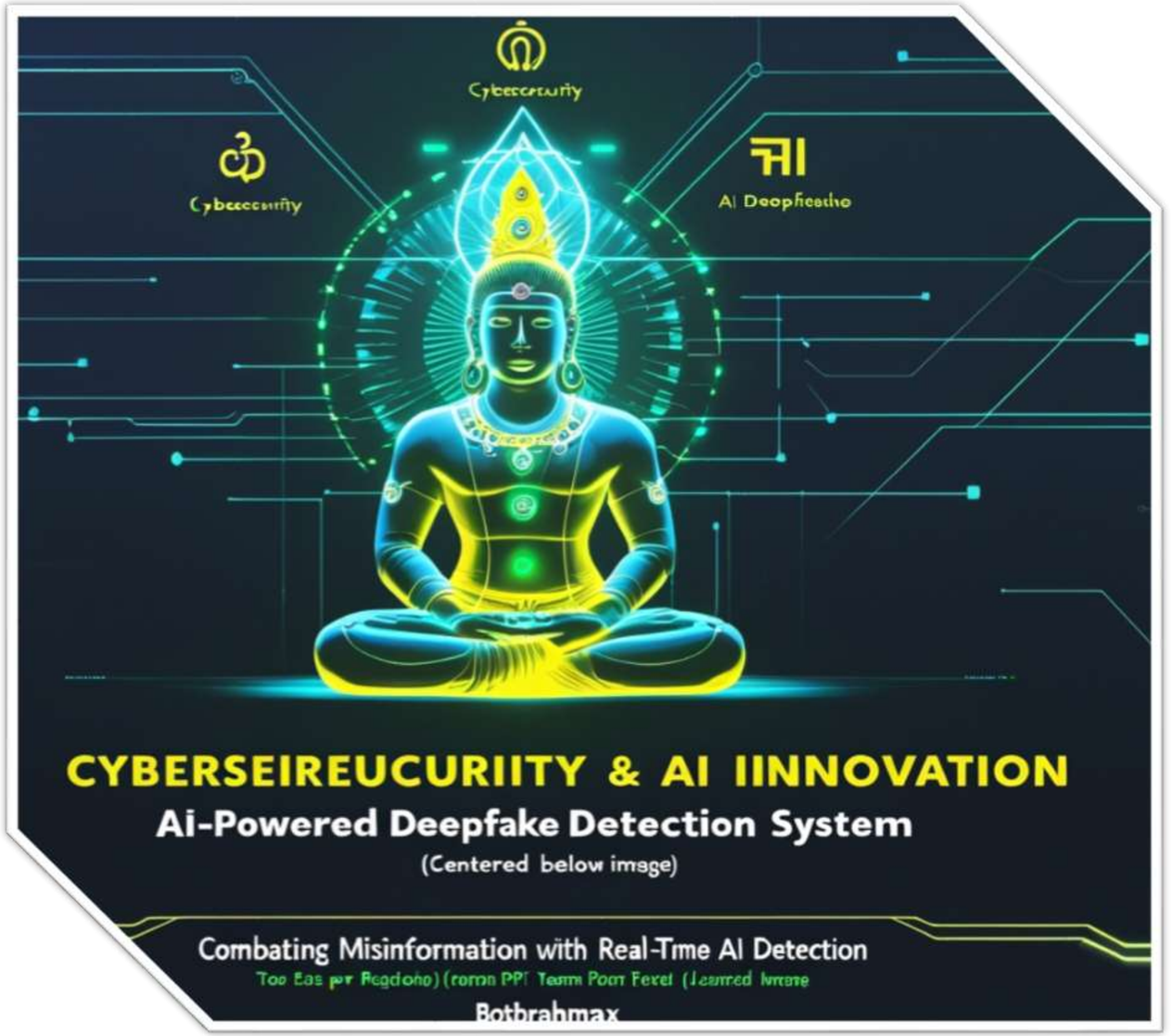
The Creation of Tomorrow

BrahmaX 1.0

www.codecrax.com

Profile Overview

- **Theme** - (Cybersecurity & AI Innovation)
- **Problem Statement Title**- (AI power Deepfake Detection system)
- **Team ID** - ( )
- **Team Name** - (BotBrahmaX)

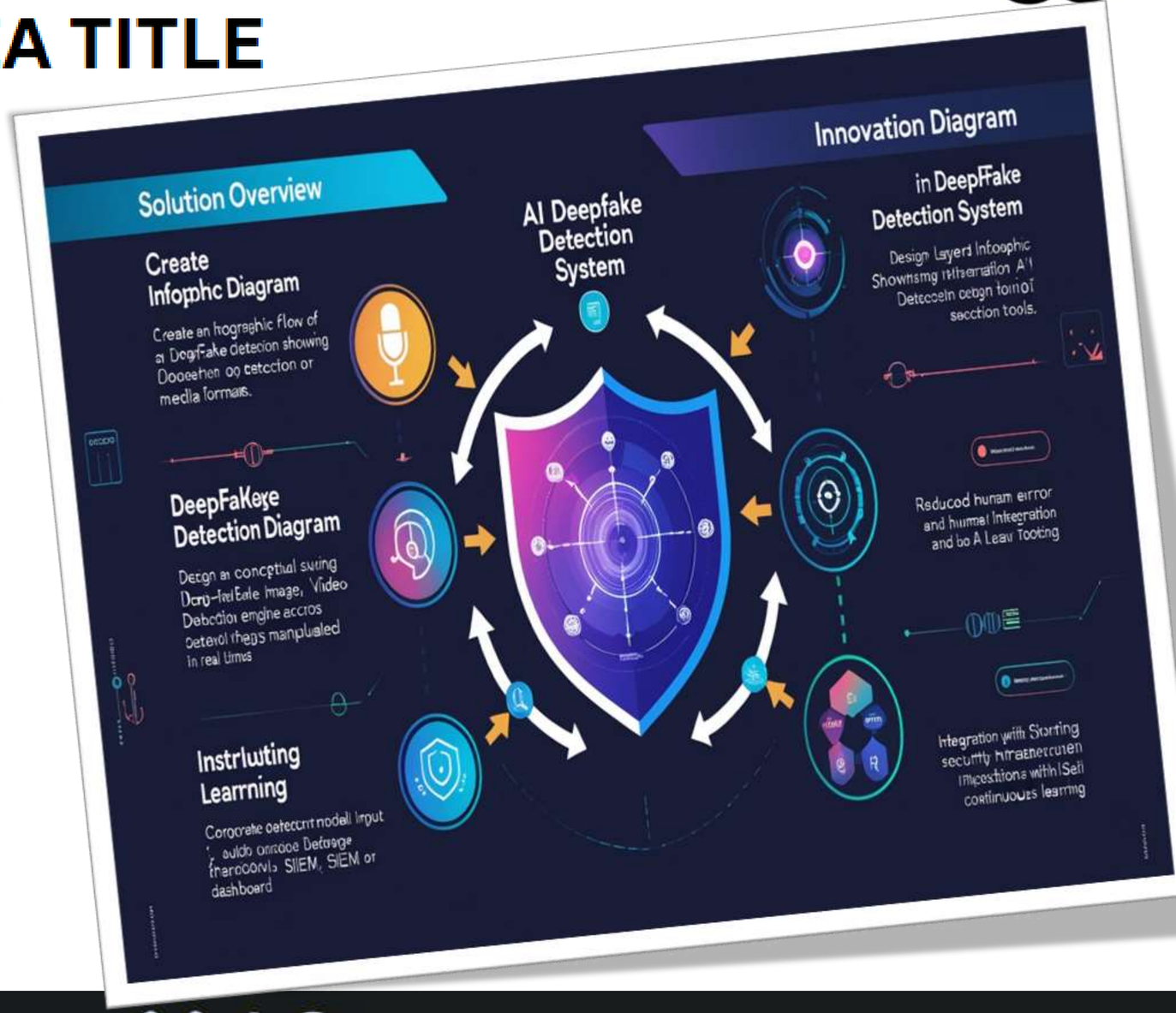


IDEA TITLE

❑ Solution Overview: - Detects deepfakes in voice, image, and video formats. Flags manipulated media in real-time. Integrates with existing corporate security infrastructure.

❑Problem-Solving: - Addresses cyber fraud, social engineering, and misinformation. Reduces human error and response delays.

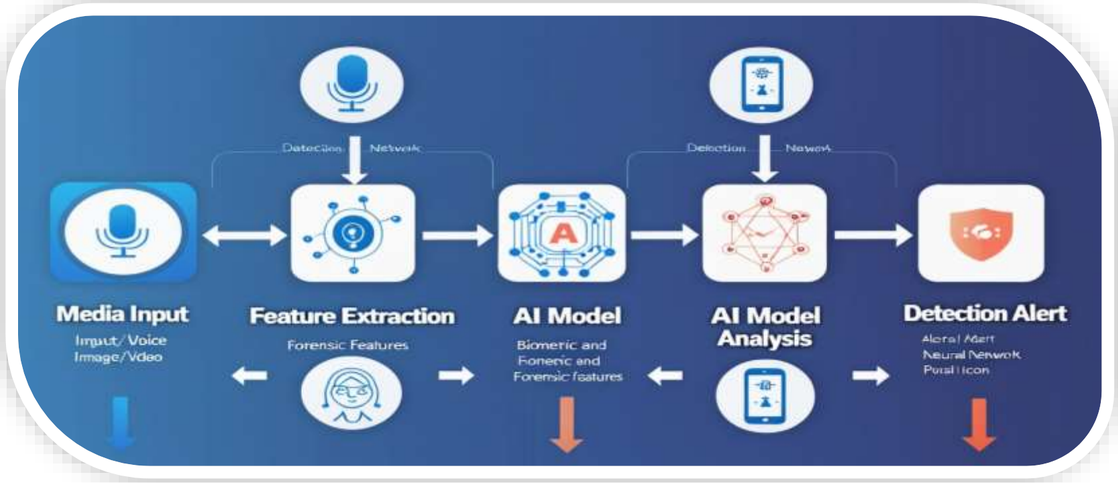
❑Innovation: - Real-time detection using multi-modal AI models. Seamless integration with SIEM and endpoint detection tools. Continuous model l



Technical Approach

❖Technologies Used: - Python, TensorFlow, PyTorch, OpenCV. - Pre-trained CNNs, RNNs for audio Analysis. - Real-time APIs, Docker, Kubernetes.

❖Methodology: 1. Input media (voice, video, image) 2. Extract biometric and forensic features. 3. AI models evaluate authenticity. 4. Flag and alert user/system



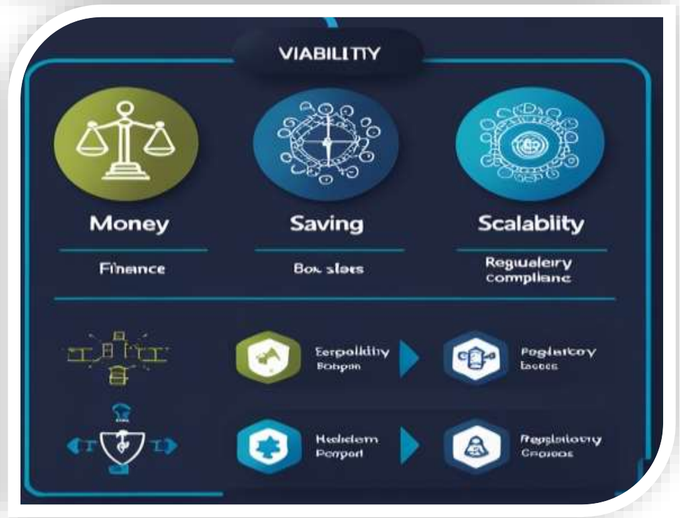
FEASIBILITY AND VIABILITY

FEASIBILITY :

- ☑ **Advanced AI Models**: Pre-trained CNNs, RNNs, transformers widely available
- ☑ **Real-Time Capability**: High-performance hardware enables rapid processing
- ☑ **Easy Integration**: Works with existing systems like **CCTV**, **sensors**, **access logs**

Viability :

- **Multi-Sector Use**: Healthcare, Finance, Government, Security
- **Cost-Saving**: Automation = reduced manual efforts & fraud losses
- **Scalability**: Modular system architecture allows easy expansion
- **Regulatory Push**: Compliance and cyber laws drive adoption



IMPACT AND BENEFITS

▽ **Impact (Challenges/Risks from Deepfakes)**

1.False Detection – Incorrectly labeling real content as fake or vice versa
2.Security Gaps – Existing tools fail to detect sophisticated deepfakes
3.Data Poisoning – Malicious data used to corrupt training datasets
4.Model Theft – AI models can be stolen or reverse engineered by attackers

☑ **Benefits (Outcomes of Your Solution)**

- ☑ **Prevents Fraud & Misinformation** – Reduces chances of identity theft, financial scams
- ☑ **Enhances Cybersecurity Posture** – Adds an active layer of defense to existing systems
- ☑ **Supports Compliance & Law Enforcement** – Helps meet regulatory requirements and aids investigation

REFERENCES

Core Framework:

- [PyTorch](#) – Primary deep learning framework for model training.

Deep Learning Models:

- [XceptionNet](#) – Backbone for deepfake detection.
- [MesoNet (PyTorch)](#) – Alternative architecture for experimentation.

Dataset:

- [FaceForensics++](#) – Main dataset for training and evaluation.

Python Libraries:

- [OpenCV](#) – Image/video processing.
- [Pillow (PIL)](#) – Image manipulation.
- [NumPy](#) – Numerical operations.

- **Torchvision** – Image datasets & transforms.
- **Tqdm** – Progress bar for loops and data loading.

Cybersecurity & Threat Intelligence

1.MITRE ATT&CK Framework

1. Learn how attackers use social engineering and deepfakes:
   https://attack.mitre.org/

2.CISA (Cybersecurity & Infrastructure Security Agency)

1. U.S. government resources on deepfake threats and countermeasures:
   https://www.cisa.gov/

AI, Deep Learning & Model Repositories

4.Papers With Code (Deepfake Detection)

4. Explore top models with code for face/video forgery detection:
   https://paperswithcode.com/task/deepfake-detection

5.ArXiv

4. Research papers on deepfake detection, adversarial learning, etc.:
   https://arxiv.org/

News & Trends (AI + Deepfake Legislation)

10.The Hacker News

10. Tracks emerging threats and global legal policies on AI misuse:
    https://thehackernews.com/

11.AI Index Report (Stanford)

10. Annual report that highlights AI trends, risks, and societal impact:
    https://aiindex.stanford.edu/