
Final Project – Proposal Submission

Project Title:

Multimodal AI Anomaly Detection System for Cybersecurity

Project Description:

This project aims to build a **multimodal anomaly detection system** that enhances cybersecurity by identifying different types of digital threats using artificial intelligence. The system integrates **three specialized AI models**:

1. **Network Anomaly Detection Model:**
   A fully connected **Autoencoder** trained on the **UNSW-NB15 dataset** to detect abnormal network packet behaviors that may indicate DDoS or intrusion attacks.
2. **Image Authenticity Detection Model:**
   A **ConvNeXt-based classifier** (similar to this Kaggle notebook) trained to distinguish **AI-generated vs. real images** to prevent phishing and image-based deception attacks.
3. **Text Authenticity Detection Model:**
   A **Natural Language Processing (NLP)** model that detects whether text content is **AI-generated or human-written**, helping protect users from phishing or scam messages.

Together, these models form a unified security system capable of identifying malicious network activity, fake images, and AI-generated phishing texts — offering end-to-end protection against modern cyber threats.

Group Members & Roles:

Name	Role
محمد احمد محمد عطيه	Model Training
محمد السيد عبدالسلام السيد	Frontend Developer & Deployment
علي محمد صلاح الدين ابو هندي	Preprocessing
عبد الرحمن أحمد عبده الهبيان	Model Evaluator
رزق سعيد محمد سيداحمد	Data gathering
محمد عبد الخالق عبد المنعم امنه	Pipeline Setup

Team Leader:

Mohammed Atia

Objectives:

1. Develop an **AI-based anomaly detection system** for network packets to identify potential DDoS or intrusion attempts.
2. Build an **image authenticity detection model** to classify AI-generated vs. real images.
3. Create a **text authenticity detector** to identify AI-generated phishing messages.
4. Integrate all three models into a **single deployable system (API)** that provides real-time predictions.
5. Enhance cybersecurity by providing **automated, AI-driven threat detection** with minimal false positives.

Tools & Technologies:

- **Programming Languages:** Python
- **Libraries:** TensorFlow, Keras, NumPy, Pandas, Scikit-learn.
- **Deep Learning Architectures:** Autoencoder, ConvNeXt, BERT/DistilBERT
- **Dataset:** UNSW-NB15 Network Attack Dataset, ai-vs-human-generated-dataset, and Hello-SimpleAI/HC3
- **Development Environment:** Kaggle, Google Colab, VS Code
- **Deployment:** FastAPI / Flask API, Docker.

Milestones & Deadlines:

Milestone	Description	Deadline
Data Collection & Preprocessing	Cleaning and preparing network, image, and text datasets	Week 2
Model 1: Network Anomaly Detection	Train and evaluate Autoencoder on UNSW-NB15	Week 4
Model 2: Image Authenticity Detection	Train ConvNeXt classifier for AI vs real images	Week 6
Model 3: Text Authenticity Detection	Train NLP model for AI text detection	Week 8
Integration & API Development	Combine models into unified API	Week 9
Final Testing & Report Submission	Evaluate performance and finalize documentation	Week 10

KPIs (Key Performance Indicators):

1. Data Quality

- Percentage of missing values handled: **100%**
- Data accuracy after preprocessing: **98%**
- Dataset diversity (representation of different categories): **90%**

2. Model Performance

Metric	Expected Value
Model accuracy (Accuracy/F1-Score)	**95% (Network), 86% (Image), 90% (Text)**
Model prediction speed (Latency)	**~50 ms/request**
Error rate (False Positive/False Negative Rate)	**<5%**

3. Deployment & Scalability

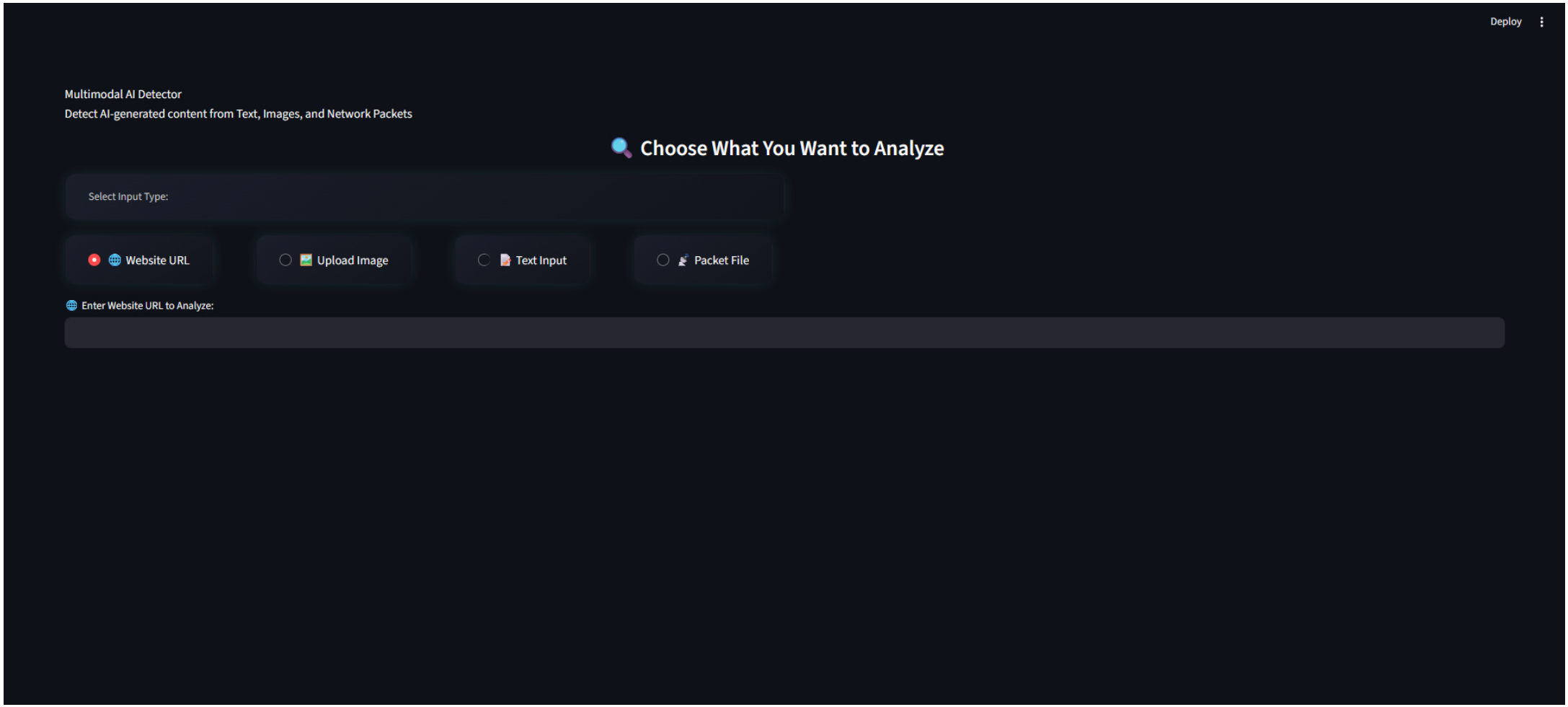
Metric	Expected Value
API uptime	**99%**
Response time per request	**<100 ms**
Real-time processing speed (if video models added later)	**30 FPS**

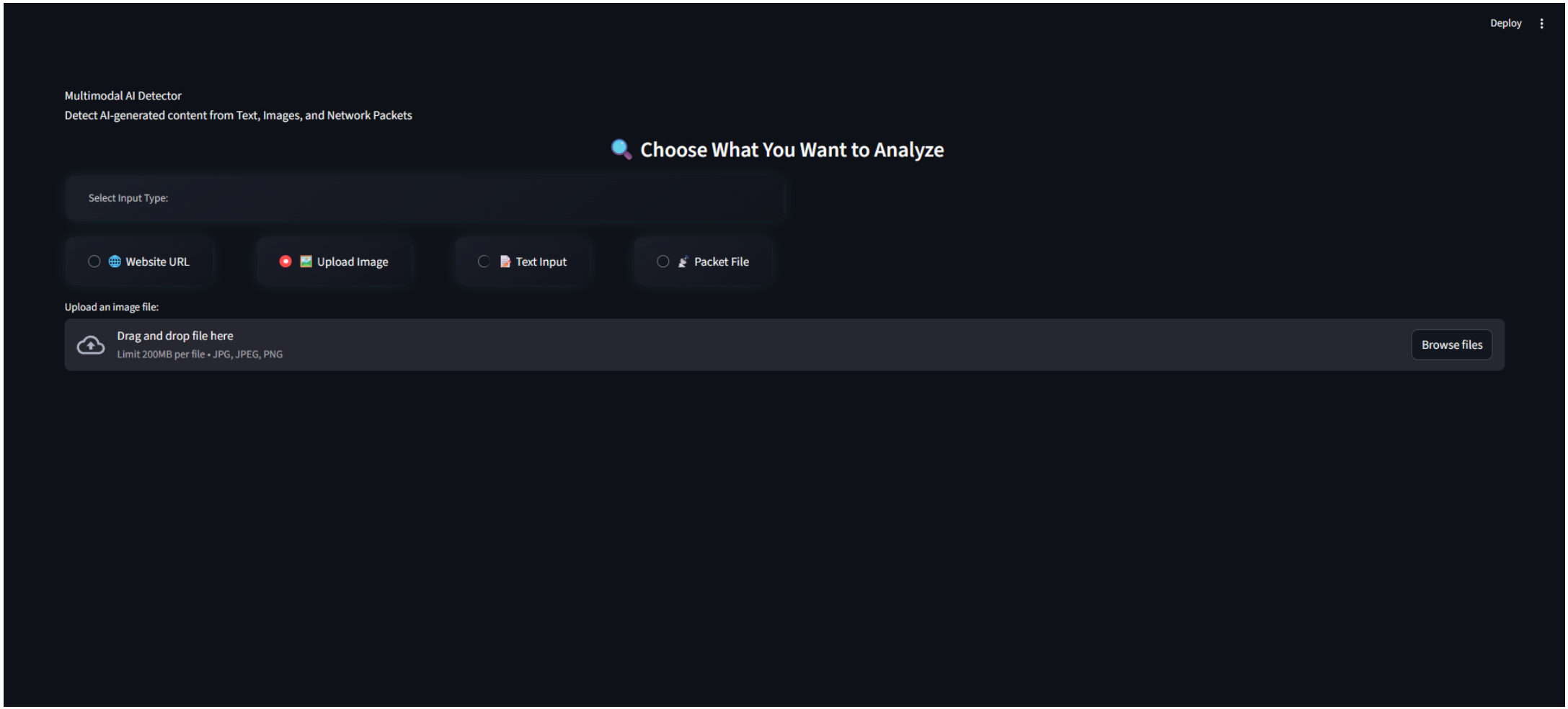
4. Business Impact & Practical Use

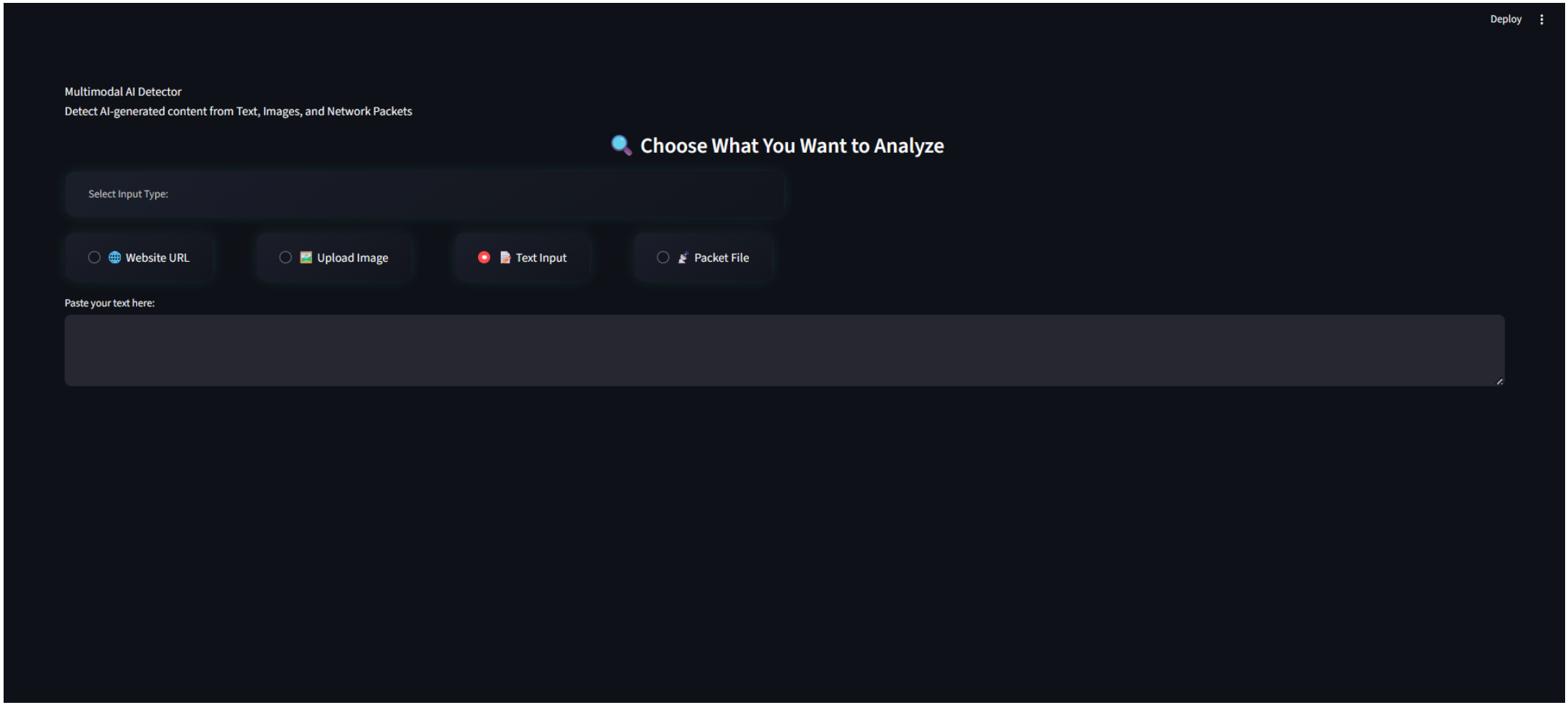
Metric	Expected Value
Reduction in manual effort	**85%**
Expected cost savings	**70%**
User satisfaction	**95%**

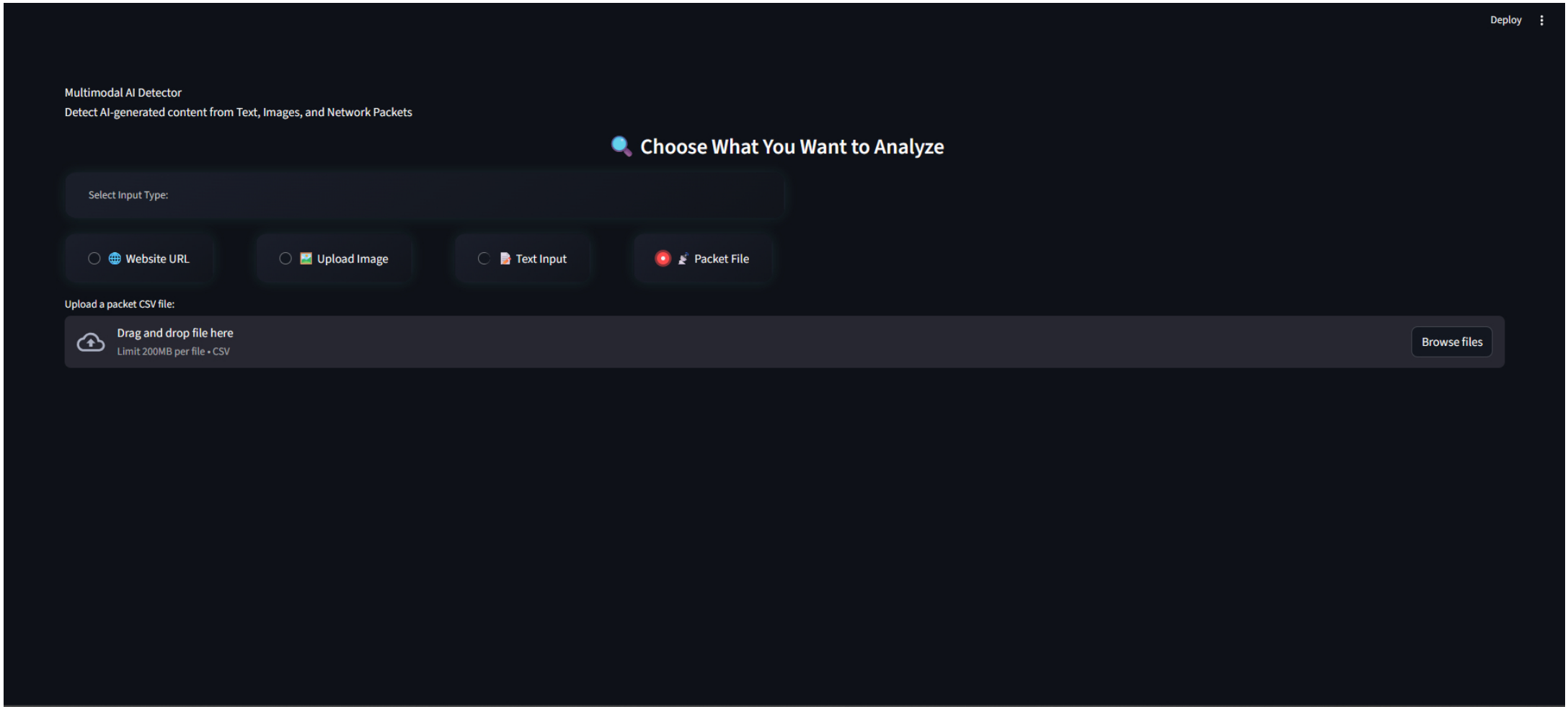
✅ **Summary:**

This multimodal anomaly detection project combines **network analysis, computer vision, and natural language processing** to detect cyber threats from multiple attack surfaces. By using advanced AI models like Autoencoders, ConvNeXt, and NLP transformers, it provides a **comprehensive defense mechanism** that can be integrated into real-world security systems.


Deploy
Multimodal AI Detector
Detect AI-generated content from Text, Images, and Network Packets
Choose What You Want to Analyze
Select Input Type:
Website URL
Upload Image
Text Input
Packet File
Enter Website URL to Analyze:


Deploy
Multimodal AI Detector
Detect AI-generated content from Text, Images, and Network Packets
Choose What You Want to Analyze
Select Input Type:
Website URL
Upload Image
Text Input
Packet File
Upload an image file:
Drag and drop file here
Limit 200MB per file • JPG, JPEG, PNG
Browse files


Deploy
Multimodal AI Detector
Detect AI-generated content from Text, Images, and Network Packets
🔍 Choose What You Want to Analyze
Select Input Type:
Website URL
Upload Image
Text Input
Packet File
Paste your text here:


Deploy
Multimodal AI Detector
Detect AI-generated content from Text, Images, and Network Packets
Choose What You Want to Analyze
Select Input Type:
Website URL
Upload Image
Text Input
Packet File
Upload a packet CSV file:
Drag and drop file here
Limit 200MB per file • CSV
Browse files