# Synopsis

## Project Title:

PrivAI – A Modular AI Assistant Balancing Privacy and Cloud Capability

## 1. Name/Title of the Project

PrivAI – A Modular AI Assistant Balancing Privacy and Cloud Capability

## 2. Statement About the Problem

As artificial intelligence becomes deeply integrated into daily life, concerns about user privacy, data leaks, and dependency on cloud-based models have grown significantly. Many AI assistants rely exclusively on cloud servers for processing, meaning sensitive data often leaves the user's device. This raises privacy concerns and limits user control over their data.  
  
This project aims to address these concerns by designing an AI assistant with a modular architecture. Although the long-term vision is to run entirely offline using open-source LLMs like Phi-3 or LLaMA on local hardware, the current implementation leverages Google Gemini API for language understanding and multimodal processing (text, image, video, and PDF). This temporary use of Gemini is a practical bridge due to time and hardware constraints, enabling feature-rich functionality while preserving the system’s core privacy-focused architecture for future updates.

## 3. Significance of the Project

This project offers a practical solution for real-world users who seek both privacy and high capability from their AI assistants. By using a hybrid approach—cloud API during prototyping and local model integration in later versions—PrivAI becomes a scalable and privacy-conscious alternative to fully cloud-dependent assistants.  
  
Its modular architecture supports future migration to offline inference, making it adaptable for privacy-focused individuals and developers seeking self-hosted AI systems. This project not only solves an immediate implementation challenge but also serves as a blueprint for responsible AI development.