Mobile Application Development

Project Title:

ChatVerse – Secure Mobile Chat Application with Private AI Assistant

Submitted By:

Malik Saad Naeem (232202001)

Zoya Yasir (232202011)

Muhammad Maaz (232202018)

Submitted To:

Sir Uzair Hassan

BSCS 6

Project Proposal

Introduction

With the increasing use of AI chat platforms, data privacy has become a major concern. Most public AI systems store or process user conversations on external servers, which poses security risks—especially for organizations handling confidential information. There is a strong need for a secure communication platform that provides both real-time user chat and private AI assistance without data leakage.

Problem Statement

Existing AI chat platforms do not ensure complete data privacy. User conversations and uploaded documents may be exposed to third-party services. This makes them unsuitable for companies that need to share internal documents, policies, or sensitive information securely.

Proposed Solution

This project proposes a **secure mobile application built with React Native** that allows:

- Real-time **user-to-user chat**
- Interaction with a **private AI assistant**

The AI assistant is powered by **Ollama**, which runs locally or on a private server, ensuring that no data is shared with public AI platforms. **Appwrite** is used for secure authentication and real-time messaging, while **FastAPI** and **MongoDB** handle AI-related processing and data storage.

Key Features

- Secure authentication and real-time messaging using Appwrite
- Private AI assistant using Ollama
- Upload and query **PDF and text documents**
- AI responses based only on user or company-provided documents

Applications

- Internal company support systems
- Employee training and onboarding
- Secure knowledge-sharing platforms
- Privacy-focused personal AI assistants

Conclusion

This project delivers a **privacy-first mobile chat solution** that combines secure communication with private AI capabilities. It is suitable for both individuals and organizations that require secure, reliable, and confidential AI-assisted communication.