INSTITUTE OF SPACE TECHNOLOGY
KICSIT, Kahuta Campus

**Mobile Application Development**

**Project Report**

**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**

## 1. Introduction

ChatVerse is a secure mobile chat application developed using **React Native** that allows users to communicate with each other in real time and interact with a **private AI assistant**. The project was built to address privacy concerns associated with public AI chat platforms and to provide a secure environment for both personal and organizational communication.

The application integrates **user-to-user messaging**, **private AI conversations**, and **document-based AI querying** within a single mobile platform.

## 2. Problem Statement

Most existing AI chat platforms do not guarantee full data privacy. User messages and uploaded documents are often processed or stored on third-party servers, which creates security risks. This is particularly problematic for organizations that need to share **confidential documents, internal policies, or rulebooks** with AI systems.

## 3. Objectives

The main objectives of this project were:

- To build a **secure mobile chat application**
- To enable **real-time user-to-user communication**
- To provide a **private AI assistant** without using public AI services
- To support **document upload (PDF/TXT)** and AI-based querying
- To ensure **data privacy and security** for individuals and organizations

## 4. System Overview

The system consists of three major components:

- **Mobile Application (React Native):**
  Provides the user interface for chat, authentication, and document upload.
- **Backend (FastAPI):**
  Handles AI-related requests, document processing, and communication with the AI model.

- **Database & AI Layer:**
  MongoDB is used to store AI chat data, while Ollama runs the AI model locally or on a private server.

**5. Technologies Used**

**Frontend (Mobile App)**

- React Native (Expo)
- Appwrite (Authentication & User-to-User Chat)

**Backend**

- FastAPI
- Uvicorn
- MongoDB

**AI & Document Processing**

- Ollama (Private AI model)
- LangChain
- PyPDF2 (PDF text extraction)

**6. Working of the System**

First, the user opens the React Native mobile application and logs in using **Appwrite authentication**. After successful login, the user can chat with other registered users in real time.

For AI interaction, the user can send messages to the **personal AI assistant** or upload text/PDF documents. These requests are sent to the **FastAPI backend**, where the document content is extracted and passed to the AI model using **LangChain**.

The AI model, powered by **Ollama**, generates responses based only on the provided input or uploaded documents. AI-related chats are stored in **MongoDB**, and the generated response is sent back to the mobile application and displayed to the user.

**7. Security and Privacy**

Security and privacy were key focuses of this project:

- Ollama runs locally or on a private server, ensuring **no data is sent to public AI platforms**
- Appwrite provides **secure authentication and real-time messaging**
- Documents uploaded by users remain within the system
- AI responses are generated only from user-provided data

**8. Use Cases**

This application can be used for:

- Secure personal AI assistance
- Internal company support systems
- Employee training and onboarding
- Private knowledge-sharing platforms
- Organizations handling sensitive documents

**9. Results and Outcome**

The project was successfully implemented with all planned features working as expected:

- Real-time user chat was achieved using Appwrite
- Private AI assistant worked securely using Ollama
- Document upload and AI-based querying functioned correctly
- The system maintained user data privacy throughout

## 10. Conclusion

ChatVerse successfully demonstrates how **secure communication**, **private AI**, and **document-based intelligence** can be combined into a single mobile application. By avoiding public AI services and using a private AI model, the project ensures strong data privacy and security. This system is suitable for both individual users and organizations requiring confidential AI-assisted communication.