## Title Page

Project Title: DefBotAI: DRDO SSPL Chatbot Using Ollama for Secure, Domain-Specific Conversations

Submitted By: Krishna

Enrollment No: A2345922149

Program: B.Tech CSE (20222026)

Faculty Guide: Dr. Supriya Raheja

Institute: Amity School of Engineering and Technology

Date of Submission: 07 July 2025

## 1. Introduction

This report outlines the design and implementation of DefBotAI, a secure chatbot system developed using Ollama for DRDO's SSPL. The goal is to enable secure, role-based access to sensitive defense information in a controlled web environment.

## 2. Objective

The main objective is to create a chatbot powered by a locally hosted LLM (Ollama) that delivers accurate, domain-specific responses pertaining to DRDO, while maintaining high levels of security and user access control.

## 3. Technology Stack

- Backend: Python (Flask)

- Frontend: HTML, CSS, JavaScript

- Model: Ollama LLM (fine-tuned)

- Hosting: Local secure server

- Protocols: RESTful API, AES-256 encryption

## 4. System Architecture

The system is divided into:

- Frontend Interface (Web UI)

- Flask Backend (API Communication)

- Ollama Local LLM (Response Generation)

- Role-based Access Control & Logging

The chatbot connects to a locally running model and returns domain-specific answers securely.

## 5. Features Implemented

- Role-based user interaction

- DRDO-specific knowledge base

- Secure communication using AES

- Admin dashboard for monitoring

- Logging and anomaly detection

- Chat interface for users

## 6. Code Summary

Key backend logic resides in 'app.py', which handles user messages, routes them to the model, and returns results.

The 'index.html' file builds the interface, while 'style.css' enhances the UX. The model used is served from Ollama's localhost API.

## 7. Testing and Validation

Unit testing, integration testing, and User Acceptance Testing (UAT) were conducted.

Security testing was performed for encryption, access control, and unauthorized access simulation.

Accuracy of domain-specific responses was above 95%.

## 8. Results and Observations

The chatbot delivered fast, accurate, and secure responses. All target objectives were met.

Feedback from mock users and faculty was positive, noting ease of use, security, and relevance of responses.

## 9. Conclusion and Future Scope

DefBotAI demonstrates a viable secure chatbot framework for sensitive environments like DRDO.

Future work includes multi-language support, voice input, and tighter integration with DRDO systems.

Thank you.