**Secure AI-Powered Customer Service Chatbot for E-commerce**

**Team Structure**

**3 Full-Stack Developers:** Students 1, 2, and 3  
**Role Rotation:** All students work across the entire stack, with rotating lead responsibilities

**Project Overview**

Develop a secure, AI-powered customer service chatbot for an e-commerce platform, focusing on protecting customer data, preventing security breaches, and providing safe, automated customer support.

**Key Components**

1. **Natural Language Processing (NLP)** for understanding customer queries
2. **Secure handling of customer data and transactions**
3. **Integration with a mock e-commerce backend**
4. **User authentication and access control**
5. **Audit logging and anomaly detection**

**Technology Stack**

* **Frontend:** React.js for web interface
* **Backend:** Python with FastAPI
* **Database:** SQLite for development (can be scaled to PostgreSQL)
* **NLP:** Hugging Face Transformers (e.g., BERT) for intent classification
* **Authentication:** JWT with refresh tokens
* **Encryption:** Python cryptography library

**Project Tasks and Timeline**

**Week 1: Project Setup and Planning**

* **All Members:**
  + Project kickoff, tool selection, and environment setup
  + High-level system design and task allocation
  + Begin learning/refreshing on required technologies
* **Lead (Student 1):** Oversee project setup and initial architecture design

**Week 2: Basic Chatbot and Frontend Setup**

* **All Members:**
  + Implement basic chatbot interface
  + Set up backend structure and database
  + Create initial NLP model for intent classification
* **Lead (Student 2):** Guide NLP model development and integration

**Week 3: Security Infrastructure and User Authentication**

* **All Members:**
  + Implement user authentication system
  + Set up encryption for sensitive data
  + Create secure API endpoints for chatbot communication
* **Lead (Student 3):** Manage security implementation and best practices

**Week 4: E-commerce Integration and Transaction Security**

* **All Members:**
  + Develop mock e-commerce backend integration
  + Implement secure handling of transaction data
  + Enhance chatbot with e-commerce-specific intents
* **Lead (Student 1):** Coordinate e-commerce feature integration

**Week 5: Advanced NLP and Anomaly Detection**

* **All Members:**
  + Improve NLP model with more complex intents and entities
  + Implement basic anomaly detection for unusual user behavior
  + Develop audit logging system
* **Lead (Student 2):** Oversee NLP enhancements and anomaly detection

**Week 6: System Integration and Security Hardening**

* **All Members:**
  + Integrate all system components
  + Conduct security audit and address findings
  + Implement additional security features (e.g., rate limiting, input sanitization)
* **Lead (Student 3):** Manage system integration and security hardening

**Week 7: Testing and Refinement**

* **All Members:**
  + Conduct thorough system testing, including security testing
  + Refine chatbot responses and UI based on testing
  + Optimize system performance and security
* **Lead (Student 1):** Coordinate testing efforts and prioritize refinements

**Week 8: Documentation and Presentation**

* **All Members:**
  + Write technical documentation and user guide
  + Prepare final presentation and live demonstration
  + Conduct final security review
* **All Leads:** Collaborate on project finalization and presentation planning

**Key Features to Implement**

1. Secure user authentication and session management
2. Encrypted storage of sensitive customer data
3. NLP-based intent classification for customer queries
4. Secure handling of basic e-commerce transactions
5. Anomaly detection for potential security threats
6. Comprehensive audit logging
7. Admin dashboard for monitoring chatbot interactions and security events

**Security Considerations**

* Implement end-to-end encryption for all communications
* Use secure coding practices to prevent common vulnerabilities (e.g., XSS, CSRF)
* Implement strict input validation and sanitization
* Ensure proper access controls and principle of least privilege
* Regular security assessments throughout development

**Deliverables**

1. Functional prototype of the secure AI-powered customer service chatbot
2. API documentation for potential integration with e-commerce platforms
3. Technical report on the NLP model and security features implemented
4. User guide for customers and administrators
5. Project presentation with a live demonstration of the chatbot and its security features