Project Design Phase-II
Technology Stack (Architecture & Stack)

Date	30 October 2023
Team ID	9.3
Project Name	Network Anomaly Detection
Maximum Marks	4 Marks

Technical Architecture:

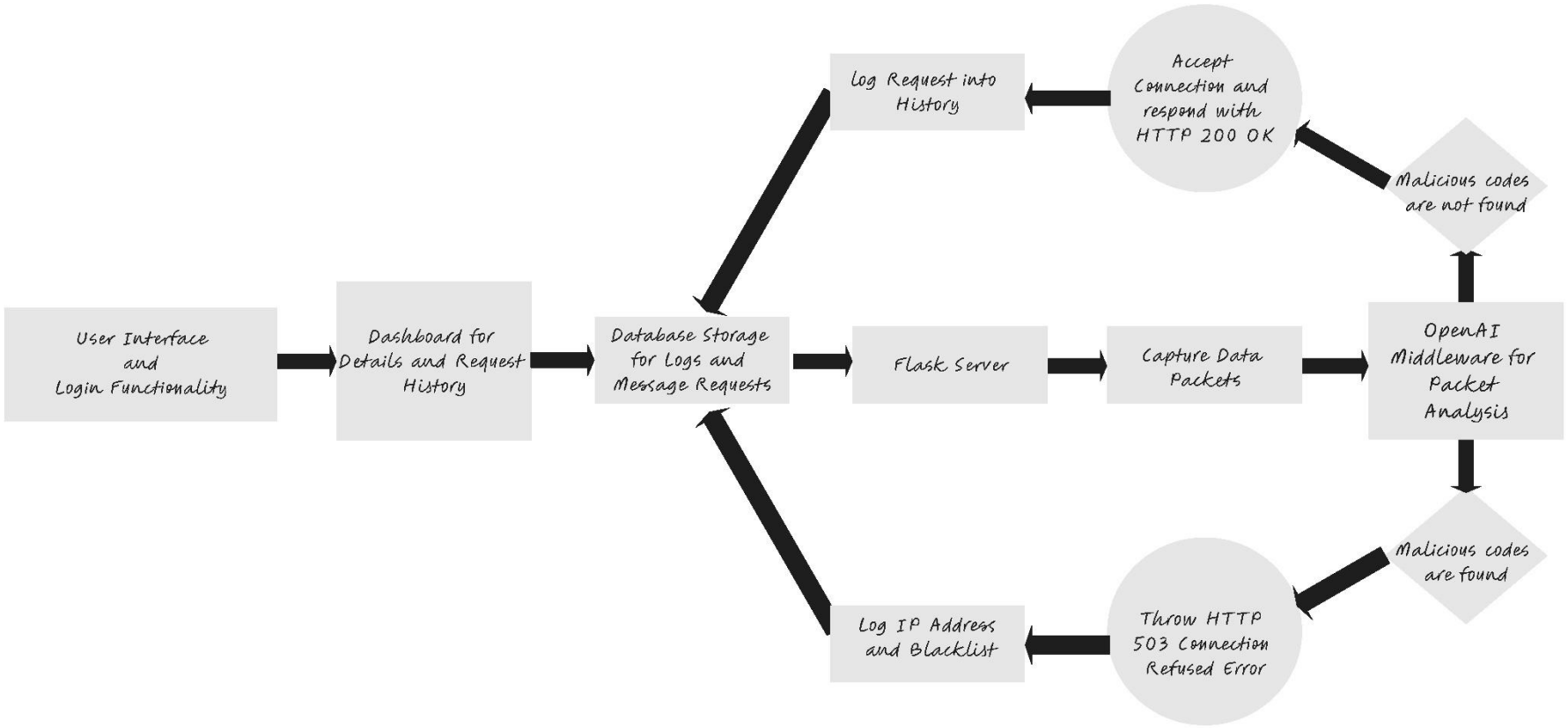

Table-1 : Components & Technologies:

Sr. No	Component	Description	Technology
1.	User Interface	Accepts user input for packet submission. Displays feedback and results from the backend.	HTML, CSS, JavaScript, JAVA
2.	Communication with Backend	Receives HHTP responses and displays the results to the user.	HHTP POST request.
3.	Backend	The Data Packet is extracted into a string (through JSON format)	Flask Server
4.	Backend	The server sends the extracted string to OpenAI to analyze for maliciousness.	API Call
5.	Cloud Database	Saves the user log in information.	MongoDB
6.	File Storage	All files and logs are stored on the cloud.	Replit Cloud Storage and MongoDB Database
7.	Open AI	Purpose of OpenAI for processing the packets of malicious code.	GPT-4
8.	Infrastructure (Server / Cloud)	Cloud Server used for hosting the entire application.	REPLIT

Table-2: Application Characteristics:

Sr. No	Characteristics	Description	Technology
1.	Open-Source Frameworks	Chat GPT-4, Replit, MongoDB	
2.	Security Implementations	All server-side processing. If malicious data in packet is found, then HTTP request is denied.	HTTP and Server Side Processing
3.	Scalable Architecture	Multi–tier	HTML/CSS/JavaScript/JAVA/Python/OpenAI-GPT-4/MongoDB/Replit
4.	Availability	Utilizing cloud services, implementing disaster recovery practices, and distributing components	Java, HTML/CSS/JavaScript, MongoDB, Replit, GPT-4/ Python

		across multiple servers or regions contribute to a highly available architecture for the security dashboard application. These considerations collectively enhance the system's resilience to fluctuations in traffic and potential failures, providing a reliable and available service to users.	
5.	Performance	Can handle up to 100 requests per sec, and continuous spam HTTP requests is auto blocked by Replit	Replit