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

Date	30 October 2023
Team ID	Team-593479 (2.9)
Project Name	Malware Detection and Classification
Maximum Marks	4 Marks

Team Members:

Ramar Priya Maha Lakshmi

Chevala Syam Sai

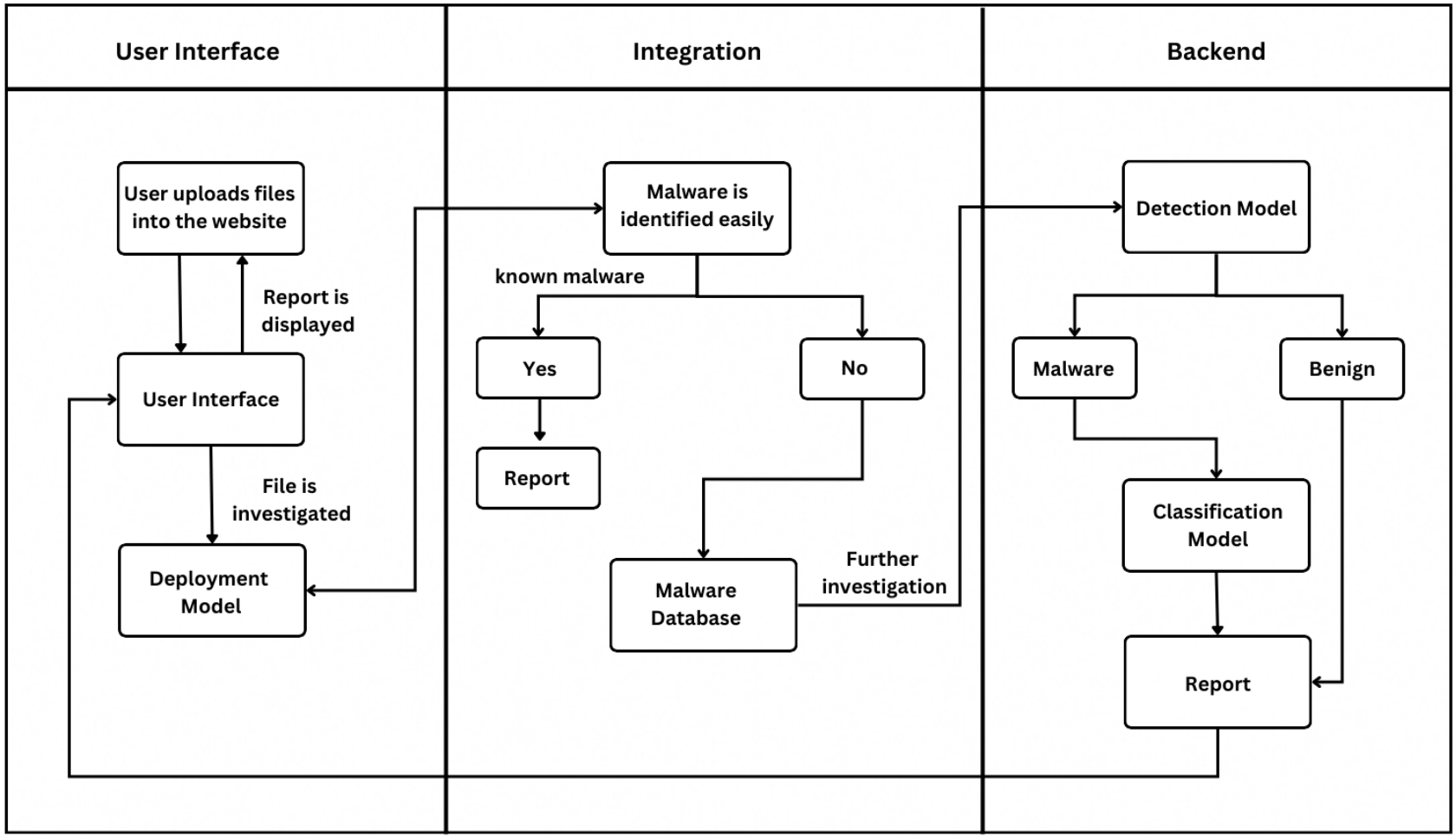
Panchada Varun

Mulumudi Prabhas

Technical Architecture:

The technological architecture for malware detection and classification encompasses a multi-layered system, starting with a user-friendly web interface and secure authentication protocols. This frontend interfaces with an AI-powered backend responsible for threat classification, leveraging machine learning algorithms for dynamic threat analysis. Concurrently, user education modules operate alongside the classification system, enhancing user awareness. The heart of this architecture lies in the cloud-based infrastructure, providing the foundation for scalable and secure data storage, compliance adherence, and seamless integration of evolving threat intelligence. This architecture encapsulates a sophisticated and adaptable framework, where the front-end user experience, AI-driven threat analysis, user education, and secure data handling converge to create a robust ecosystem for malware detection and classification.

Technical Architecture Diagram:



Guidelines:

1. Include all the processes (As an application logic / Technology Block)
2. Provide infrastructural demarcation (Local / Cloud)
3. Indicate external interfaces (third party API's etc.)
4. Indicate Data Storage components / services.
5. Use AI learning Models.

Table 1: Components and Technologies

S.No	Component	Description	Technology
1.	User Interface	How user interacts with application e.g. Web UI, Mobile App, Chatbot etc.	HTML, CSS, JavaScript / Angular Js / React Js etc.
2.	Application Logic-1	Logic for a process in the application	Java / Python
3.	Backend	For Server-Side Logic	Python, Node.js
4.	Security Measures	For data Integrity	SSL for encryption, secure file uploads.
5.	Database	Data Type, Configurations etc.	MySQL, NoSQL, etc.
6.	Cloud Database	Database Service on Cloud	AWS, Azure etc.
7.	File Storage	File storage requirements	IBM Block Storage or Other Storage Service or Local Filesystem
8.	External API-1	Purpose of External API used in the application	Storage and Data API
9.	External API-2	Purpose of External API used in the application	OAuth API, etc.
10.	AI/ML Model	Deploying for threat classification	TensorFlow, Scikit-learn etc

11.	Infrastructure (Server / Cloud)	Application Deployment on Local System / Cloud op	Local, Cloud Foundry, Kubernetes, etc.

Table-2: Application Characteristics:

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	List the open-source frameworks used	TensorFlow, PyTorch, Flask etc
2.	Security Implementations	List all the security / access controls implemented, use of firewalls etc.	SSL Encryptions, OWASP, GnuPG, WAF etc.
3.	Scalable Architecture	Both 3-tier architecture and microservices present viable options offering scalability through targeted, independent, and efficient scaling strategies to manage increased user interactions and evolving demands.	3-tier Architecture
4.	Availability	Justifying the availability aligns with user trust, operational continuity, market competitiveness, adherence to SLAs, resilience against cyber threats, and the implementation of scalable, reliable architecture.	use of load balancers, distributed servers, secure file upload and storage.
5.	Performance	This amalgamation of cutting-edge technologies ensures high-performance levels in threat detection accuracy, user education, and secure data management. The website's overall performance is characterized by its responsiveness, accuracy in threat analysis, user-friendly design, and a robust security framework, assuring users of a reliable and comprehensive platform for tackling malware threats.	AI/ML Libraries, Compliance Rules etc