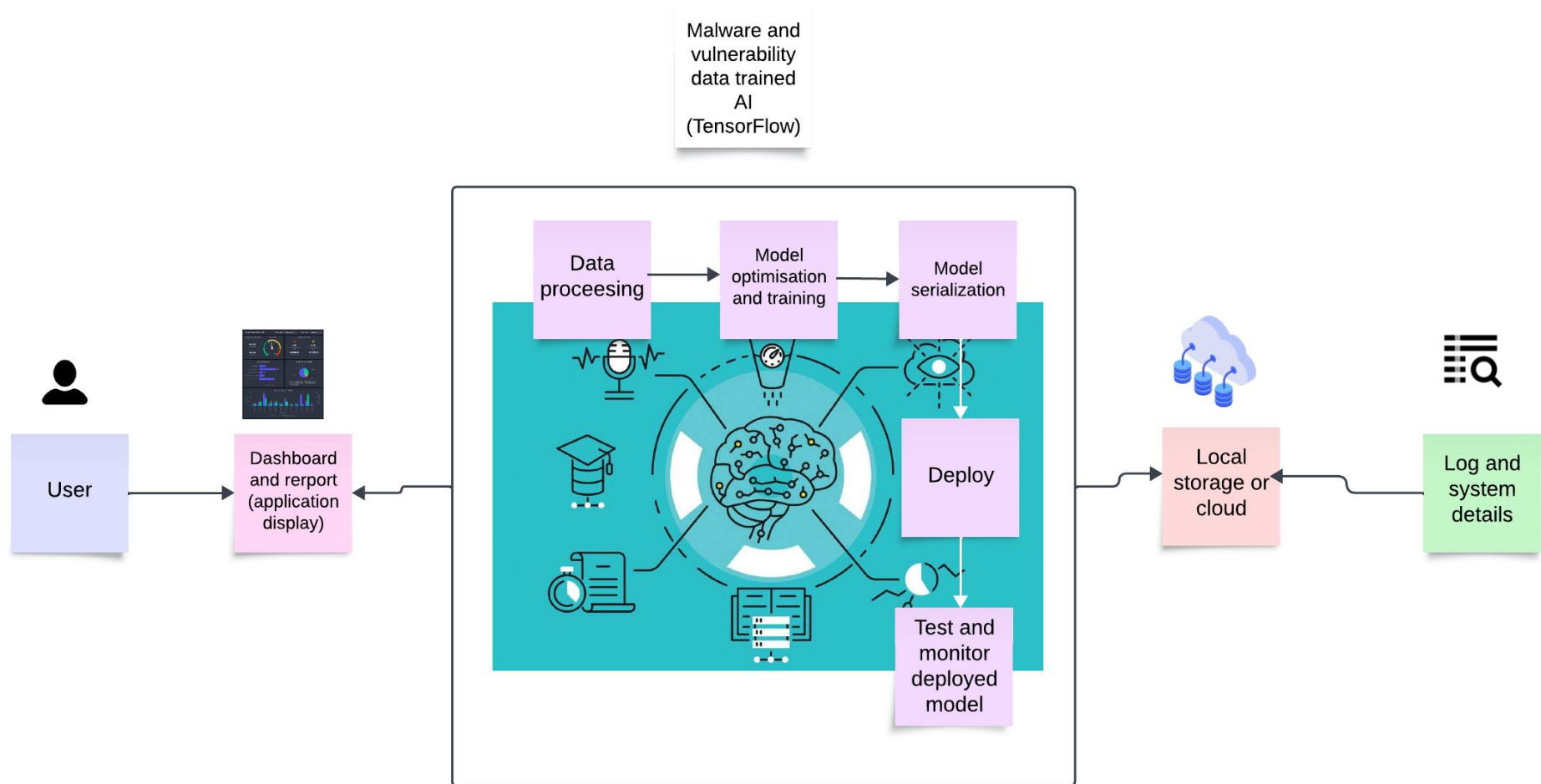


**Project Design Phase-II**  
**Technology Stack (Architecture & Stack)**

Date	26 October 2023
Team ID	PNT2022TMID593452
Project Name	Project - 10 AI-enhanced security analytics dashboard that provides real-time insights into security events, trends, and risks
Maximum Marks	4 Marks

**Technical Architecture:**

**Resource:** [https://lucid.app/lucidspark/2169046d-b0c1-4137-b5a8-91d13ec2d172/edit?beaconFlowId=6F2A8A7C989080D1&page=0\\_0#](https://lucid.app/lucidspark/2169046d-b0c1-4137-b5a8-91d13ec2d172/edit?beaconFlowId=6F2A8A7C989080D1&page=0_0#)



**Table-1 : Components & Technologies:**

S.No	Component	Description	Technology
1.	User Interface	Graphical interface for user interaction	HTML, CSS, JavaScript / Angular Js / React Js
2.	AI-Based Monitoring System	Real-time monitoring for suspicious actions	AI Algorithms, Real-time Data Analysis
3.	Vulnerability Detection	Identify and prevent major vulnerabilities	Machine Learning, Global Vulnerability Databases
4.	Risk Identification & Notification	Identify and notify users about risks	AI Algorithms, Risk Assessment Modules
5.	Dynamic Malware Analysis	Analyze malware behavior for detection	Dynamic Analysis Techniques, Machine Learning
6.	Phishing Detection	Analyze content and structure of emails	Machine Learning, Email Analysis Algorithms
7.	File-Level Malware Scanning	Scan files for malware and prevent execution	Malware Scanning Engines, Threat Intelligence
8.	Unauthorized Access Prevention	Block unauthorized access attempts	Access Control Systems, Intrusion Detection
9.	Patch Management	Automatically scan for vulnerabilities	Automated Patch Management Tools, Vulnerability Scanners
10.	Database	Data Type, Configurations etc.	MongoDB, MySQL
11.	External API-1	For data about existing vulnerabilities	Vulnerability API
12.	External API-2	For data about existing malwares	Malware API
13.	Machine Learning Model	Detect and analyze vulnerabilities and risks	Vulnerability and anomalies detection model
14.	Infrastructure (Server / Cloud)	Application Deployment on Local System / Cloud	Local, Cloud

**Table-2: Application Characteristics:**

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	Utilizing open-source frameworks for development	Technology of Opensource framework

2.	Security Implementations	Implementation of robust security measures	e.g. SHA-256, Encryptions, IAM Controls, OWASP etc.
3.	Scalable Architecture	Employing a scalable architecture for flexibility	3-tier, Micro-services
4.	Availability	Ensuring high availability through advanced techniques	Load balancers, Distributed servers
5.	Performance	Design considerations for optimal performance	Requests per second, Cache usage, CDN integration

#### References:

<https://c4model.com/>

<https://developer.ibm.com/patterns/online-order-processing-system-during-pandemic/>

<https://www.ibm.com/cloud/architecture>

<https://aws.amazon.com/architecture>

<https://medium.com/the-internal-startup/how-to-draw-useful-technical-architecture-diagrams-2d20c9fda90d>

