Basic Details of the Team and Problem Statement

SMART INDIA HACKATHON 2024

Ministry/Organization Name/Student Innovation : National Technical Research Organization (NTRO)

Problem Statement ID: SIH1685

Problem Statement Title: Building Offline Parallel AV Pipeline to cater multiple AVs for CII entities.

Theme Name: Smart Automation

Institute Name: Bharati Vidyapeeth’s College of Engineering Lavale, Pune

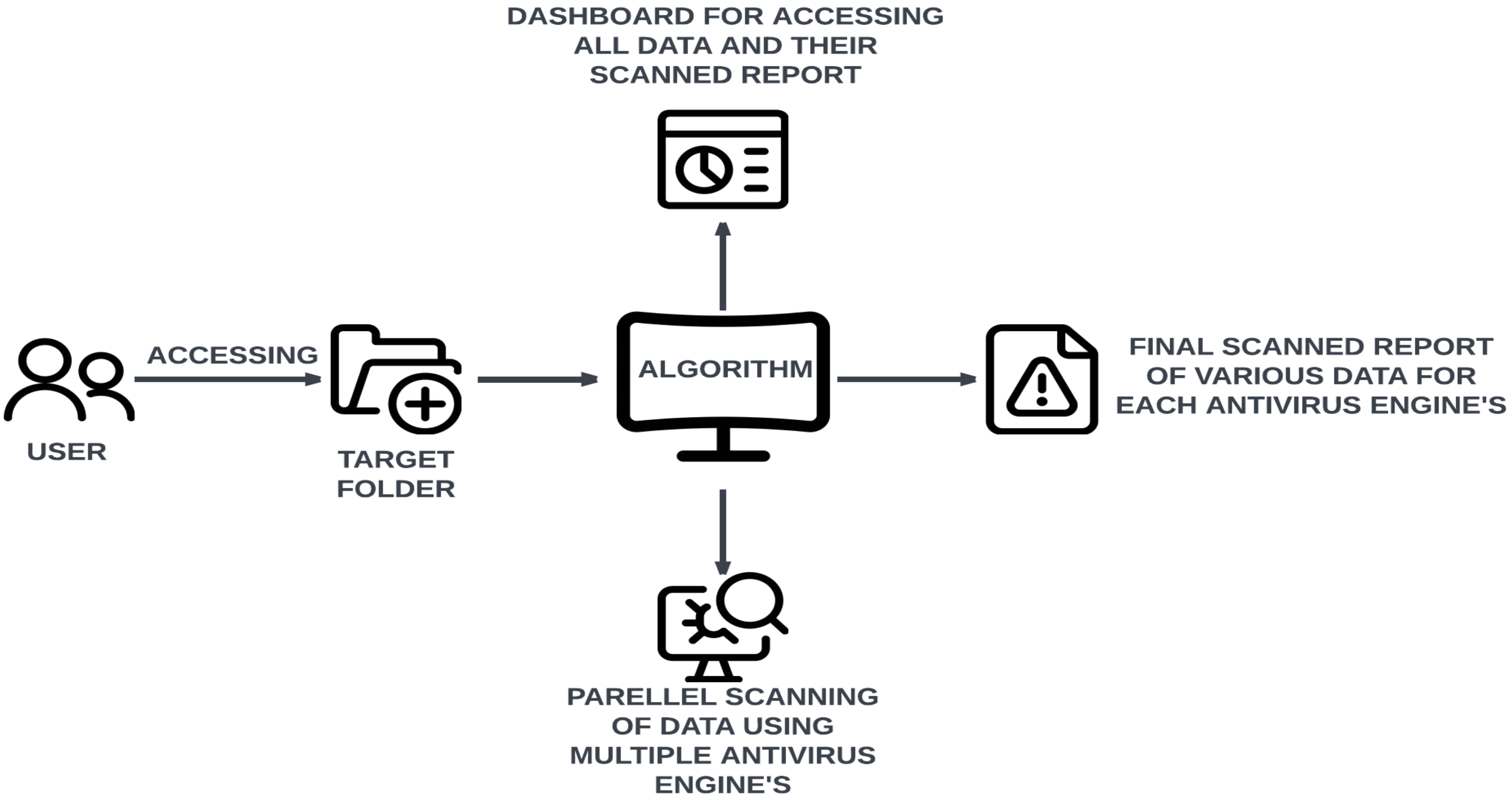
AISHE/AICTE Code : C-41597

Team Name: Antivirus Aegis

Team Id : 46780

Team Leader Name: Mrunal Mehar

SYSTEM OVERVIEW


DASHBOARD FOR ACCESSING ALL DATA AND THEIR SCANNED REPORT
USER
ACCESSING
TARGET FOLDER
ALGORITHM
FINAL SCANNED REPORT OF VARIOUS DATA FOR EACH ANTIVIRUS ENGINE'S
PARELLEL SCANNING OF DATA USING MULTIPLE ANTIVIRUS ENGINE'S

IDEA & PROPOSED SOLUTION

DATA COLLECTION & SCANNING PROCESS

- **Target Folder** created to store data.
- Data were scanned for malware using **multiple AV engines** (Windows Defender, Trend Micro, ESET).
- Simultaneous **parallel scanning** ensures fast processing using a **round-robin algorithm** for no file clashes.

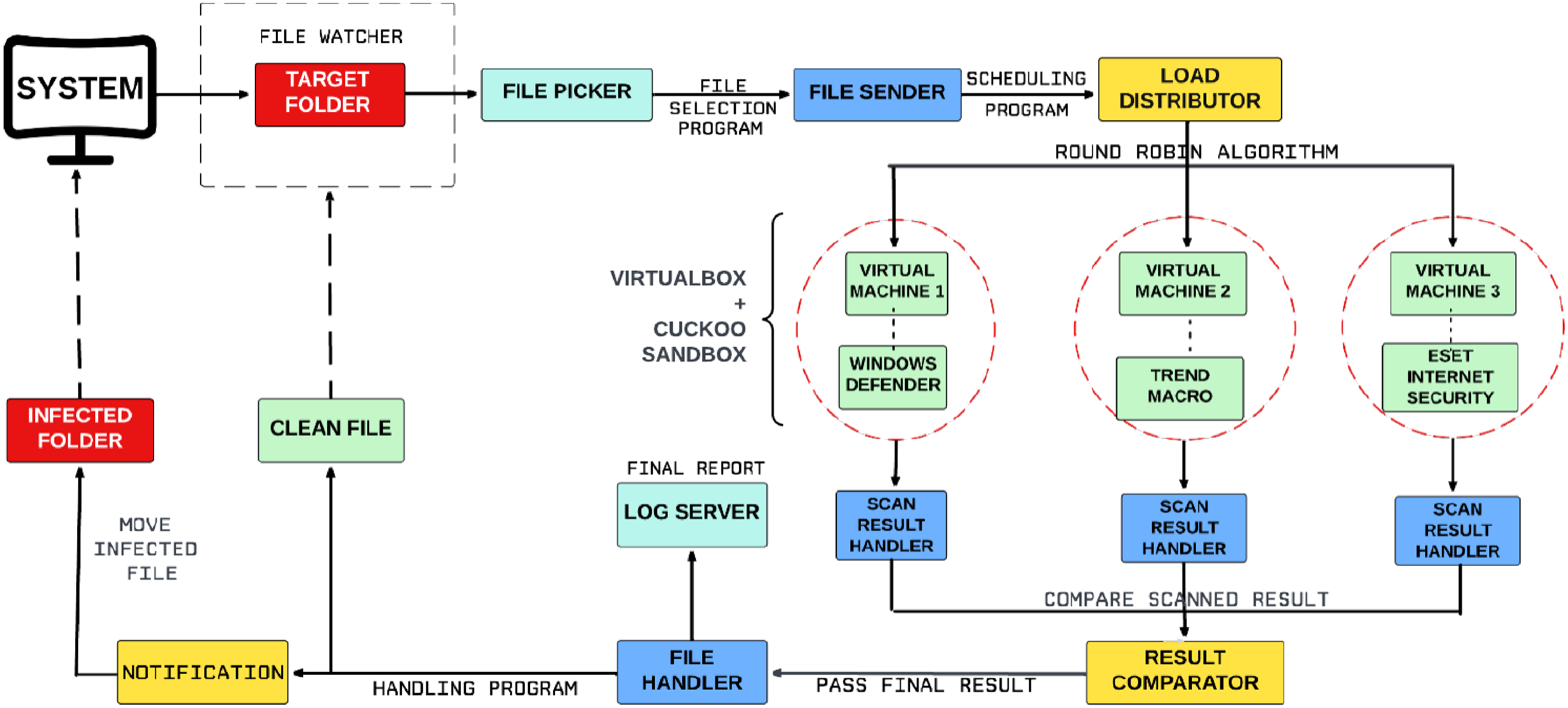
Dashboard & Report Generation

- **Dashboard** shows all files, including their type and **scan results** from each AV engine.
- A **detailed report** highlights **discrepancies** and infected files, which are moved to an Infected Folder.
- Allows easy **navigation**: All Files, Infected Files, Schedule Scan, and Manage AVs.

Key Features

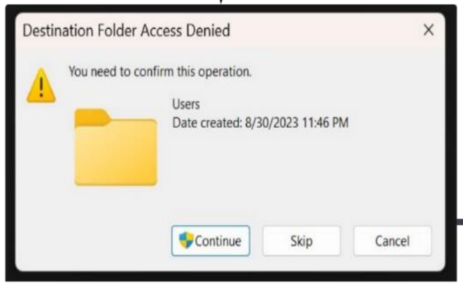
- Using **VirtualBox** each AV engine runs in **isolated Virtual Machines** (VM), ensure better **security** and **flexibility**, making them the **optimal choice** for tasks involving **malware analysis** or **running multiple antivirus** systems on different operating systems.
- **Cuckoo Sandbox's** VM provides strong isolation and advanced **malware analysis capabilities,** also **automate malware analysis** with multiple AV tools in isolated VMs. It stands out as the most **cost-effective, flexible**, and **feature-rich option**, offering dynamic malware analysis in **customizable**, isolated environments.

DETAILED ARCHITECTURE



TECHNICAL APPROACH ON SCANNING DATA

USERS/CLIENT/ ORGANISATION



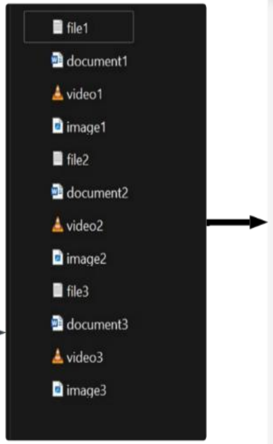
Destination Folder Access Denied ×

You need to confirm this operation.

Users
Date created: 8/30/2023 11:46 PM

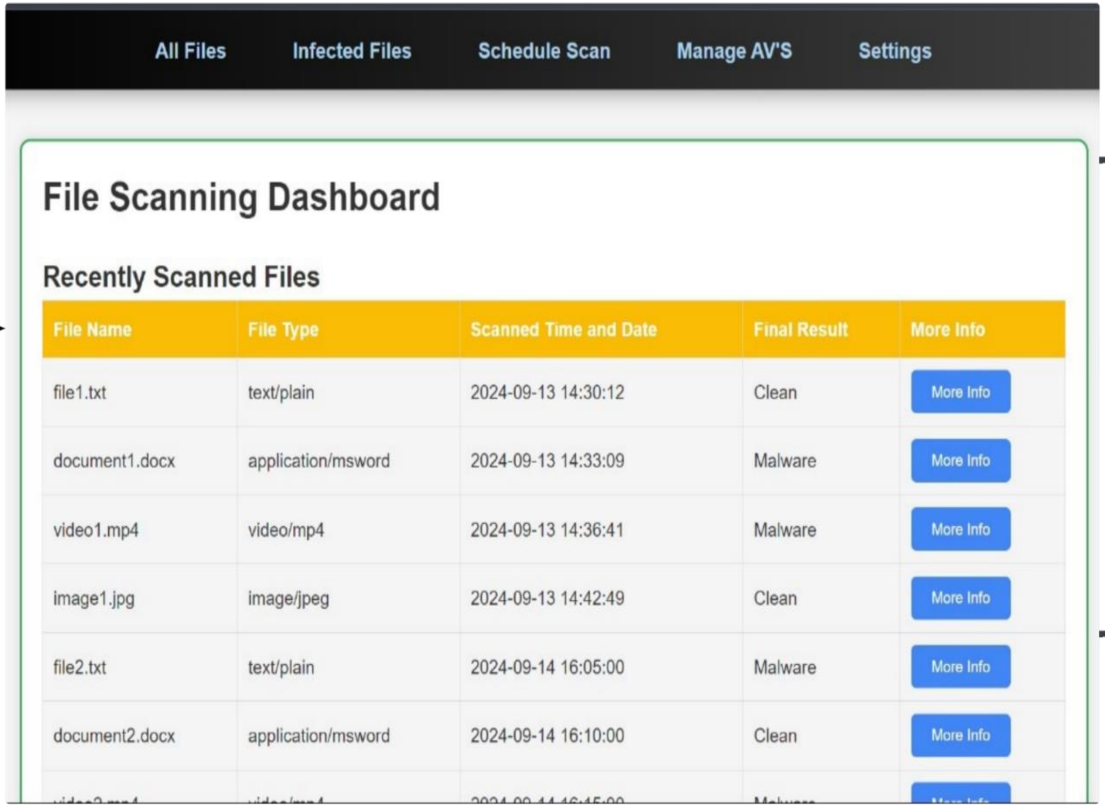
TARGET FOLDER

DATA INSERTED



- file1
- document1
- video1
- image1
- file2
- document2
- video2
- image2
- file3
- document3
- video3
- image3

ADMINISTRATION/ORGANISATION INTERFACE

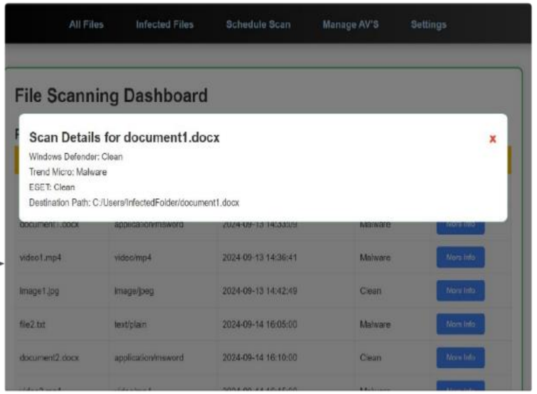


File Scanning Dashboard

Recently Scanned Files

File Name	File Type	Scanned Time and Date	Final Result	More Info
file1.txt	text/plain	2024-09-13 14:30:12	Clean	More Info
document1.docx	application/msword	2024-09-13 14:33:09	Malware	More Info
video1.mp4	video/mp4	2024-09-13 14:36:41	Malware	More Info
image1.jpg	image/jpeg	2024-09-13 14:42:49	Clean	More Info
file2.txt	text/plain	2024-09-14 16:05:00	Malware	More Info
document2.docx	application/msword	2024-09-14 16:10:00	Clean	More Info
video2.mp4	video/mp4	2024-09-14 16:15:00	Malware	More Info

MORE INFO



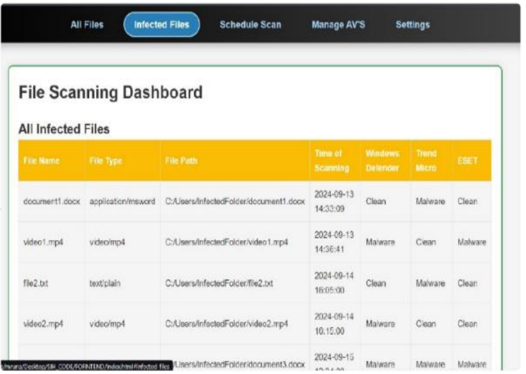
File Scanning Dashboard

Scan Details for document1.docx ×

Windows Defender: Clean
Trend Micro: Malware
ESET: Clean
Destination Path: C:/Users/InfectedFolder/document1.docx

document1.docx	application/msword	2024-09-13 14:33:09	Malware	More Info
video1.mp4	video/mp4	2024-09-13 14:36:41	Malware	More Info
image1.jpg	image/jpeg	2024-09-13 14:42:49	Clean	More Info
file2.txt	text/plain	2024-09-14 16:05:00	Malware	More Info
document2.docx	application/msword	2024-09-14 16:10:00	Clean	More Info

INFECTED FILES



File Scanning Dashboard

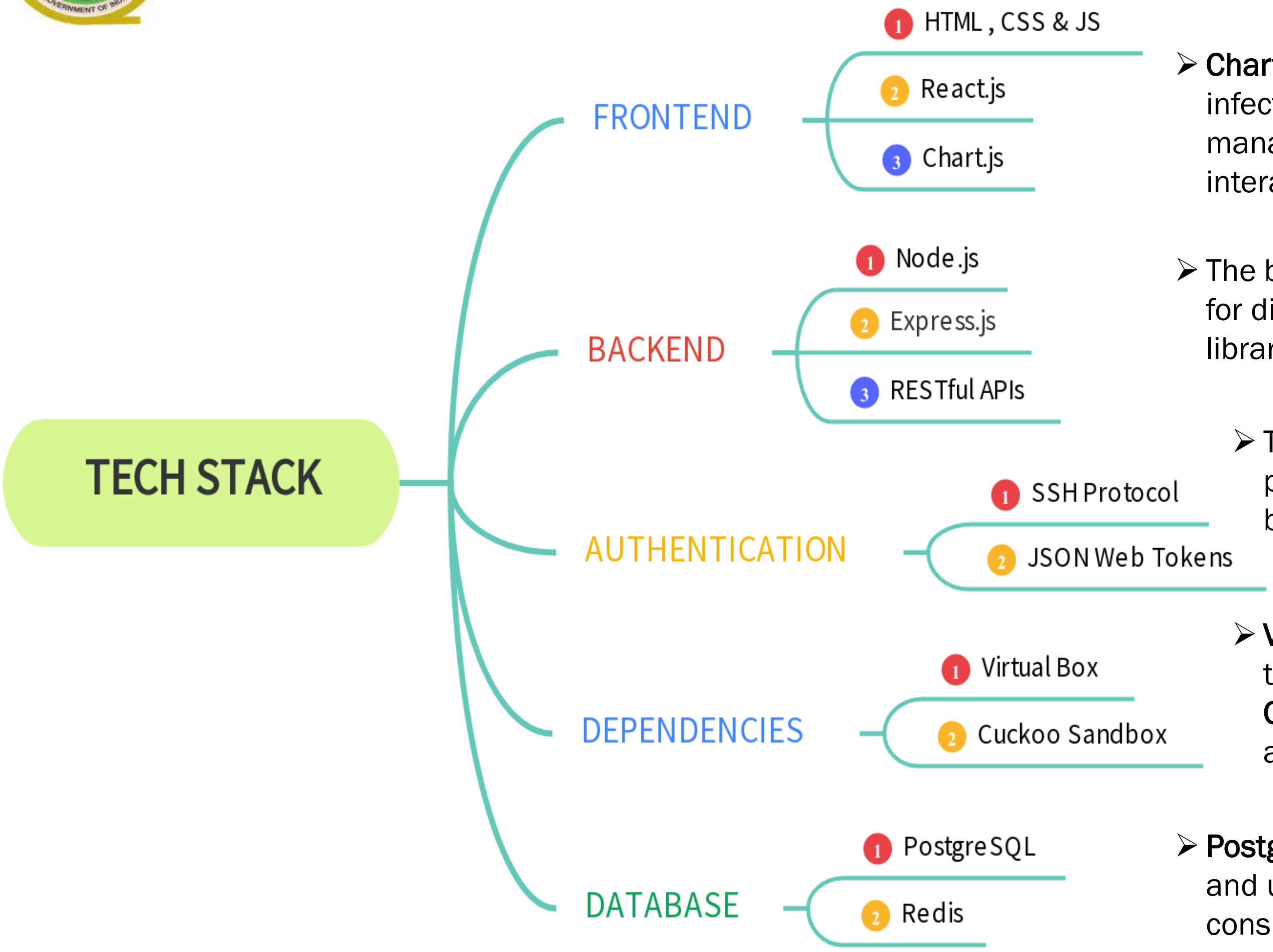
All Infected Files

File Name	File Type	File Path	Time of Scanning	Windows Defender	Trend Micro	ESET
document1.docx	application/msword	C:/Users/InfectedFolder/document1.docx	2024-09-13 14:33:09	Clean	Malware	Clean
video1.mp4	video/mp4	C:/Users/InfectedFolder/video1.mp4	2024-09-13 14:36:41	Malware	Clean	Malware
file2.txt	text/plain	C:/Users/InfectedFolder/file2.txt	2024-09-14 16:05:00	Clean	Malware	Clean
video2.mp4	video/mp4	C:/Users/InfectedFolder/video2.mp4	2024-09-14 16:15:00	Malware	Clean	Clean
		/Users/InfectedFolder/document3.docx	2024-09-15	Malware	Malware	Malware

/maruna/Desktop/SIH_CODE/FORNTEND/index.html#infected-files

Demo Link: Prototype

TECH STACK & DEPENDENCIES



TECH STACK

FRONTEND
1 HTML , CSS & JS
2 React.js
3 Chart.js

BACKEND
1 Node.js
2 Express.js
3 RESTful APIs

AUTHENTICATION
1 SSH Protocol
2 JSON Web Tokens

DEPENDENCIES
1 Virtual Box
2 Cuckoo Sandbox

DATABASE
1 PostgreSQL
2 Redis

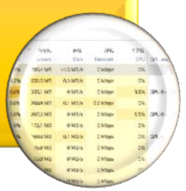
- **Chart.js** creates interactive charts for scan results, infection rates, and system activity, while **Redux** manages global state for real-time data and user interactions.
- The backend is built on **Node.js**, utilizing various libraries for different functionalities like **Chokidar** library, **SSH2** library, **FTP** library etc.
- The **SSH2 library** secures file transfers with SSH keys or passwords, while **JWT** ensures secure communication between frontend and backend.
- **VirtualBox** provides isolated environments for running antivirus tools. A custom round-robin function assigns files to VMs, while **Cuckoo Sandbox** offers an API for deeper behavioral analysis and result retrieval.
- **PostgreSQL** for handling various structured data such as logs, reports, and user data . For distributed **task scheduling** across multiple servers, consider **Redis** to coordinate scheduled jobs.

Prototype Codebase: GitHubRepositoryLink

FEASIBILITY & VIABILITY

- **ISSUE :-** Running multiple antivirus engines in isolated VMs can be resource-intensive.
- **SOLUTION -** Use containerization (e.g., Docker) or cloud-based services (e.g., AWS, Google Cloud) for better resource utilization and scalability.

Resource Intensity



- **ISSUE** - Integrating multiple antivirus engines with Cuckoo Sandbox can be challenging.
- **SOLUTION -** Develop a modular architecture with standardized APIs and protocols (e.g., OpenVAS) for easy integration.

Integration and Compatibility

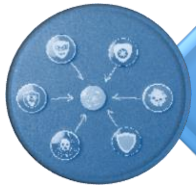
- **ISSUE -** Comparing results from multiple antivirus engines can lead to false positives and discrepancies.
- **Solution:** Implement a voting system or weighted scoring mechanism to determine the final verdict.

False Positives and Discrepancies

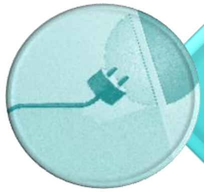
- **ISSUE -** Regular updates and maintenance of antivirus engines and Cuckoo Sandbox are required.
- **SOLUTION -** Implement an automated update mechanism and establish a feedback loop with vendors and community

Maintenance and Updates

INNOVATION & IMPACT

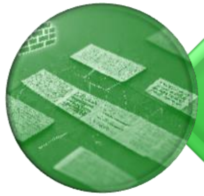


Multi-Engine Threat Detection **Improved detection rates** and **reduced false positives**, enhancing overall cybersecurity posture.



Open API and Integration Framework Enabling seamless integration with **third-party tools** and systems, promoting innovation and collaboration.

Seamless integration with Existing Security Tools and systems, enhancing the **overall security posture** and reducing complexity.



Automated Threat Segregation: Automatically segregating infected files from clean files, reducing the risk of malware spread and improving incident response.

Advanced File Analysis: Providing advanced file analysis, including **behavioral analysis** and sandboxing, to improve threat detection and **reduce false negatives**.

TEAM MEMBER DETAILS

Team Leader Name : Mrunal Mehar

Branch: B.E. **Stream: Electronics & Tele Communication** **Year: III**

Team Member 1 Name: Nisha Lohar
Branch: B.E. **Stream: Computer Engineering** **Year: III**

Team Member 2 Name: Pallavi Jadhav
Branch: B.E. **Stream: Computer Engineering** **Year: III**

Team Member 3 Name: Aditya Kaul
Branch: B.E. **Stream: Computer Engineering** **Year: III**

Team Member 4 Name: Hemant Jodha
Branch: B.E. **Stream: Electronics & Tele Communication** **Year: III**

Team Member 5 Name: Sahil Bhandarwar
Branch: B.E. **Stream: Electronics & Tele Communication** **Year: III**

Team Mentor 1 Name : Mr. Sandesh Lohar

Category: Industry **Expertise: Virtual Machine , APIs** **Domain Experience (in years): 20+**

"ZERO DEFECT, MORE EFFECT- MAKE IN INDIA."

-PM NARENDRA MODI JI