Specification Document

Assignment 2

Eden Adiv
Alon Ravinovitch

1. **Challenge Identification**

Attack Surface:

The attack surface consists of the following exposed components:

1. Web Interface: The upload page where lab technicians submit blood samples files. Exposed to potential unauthorized access and malicious file uploads.
2. Ubuntu Server (VirtualBox): The processing server running AWS CLI. Handles file validation and transfer operations.
3. S3 Object ACLs: Access Control Lists at the object level that could be misconfigured to allow public access to individual files.

Attack Vectors:

The following attack vectors threaten the data transfer process.

1. Malicious File Upload: Attackers may upload files containing malware or scripts disguised as blood sample reports.
2. Data Tampering: Modification of file content or metadata during transfer to corrupt medical records.
3. Unauthorized Access: Bypassing authentication to upload files.
4. File Type Spoofing: Uploading non-PDF files with modified extensions to bypass validation.
5. Content Injection: Files that appear valid but lack proper blood sample identifiers, indicating potential sabotage.

2. Solution Concept

Secure File Upload Process

- Web Interface Upload: Lab technicians upload files through a web page hosted on Vercel (free hosting service).
- Immediate Transfer to Temporary Bucket: Files are immediately moved to a Temporary S3 Bucket to prevent attacks during server-side processing.
- Server-Side Validation: The Ubuntu server pulls files from the Temporary Bucket and validates them.
- Routing Decision: Valid files are moved to the Production Bucket; invalid files are moved to the Quarantine Bucket.

File Validation Criteria

A file is considered valid if it meets both of the following conditions:

- File extension is ".pdf"
- File content contains the text "Blood Sample"

Files that fail either condition are flagged as invalid and sent to quarantine.

Isolation and Notification

Quarantine Process: Invalid files are moved to a dedicated Quarantine Bucket. Files are not deleted to preserve evidence and allow manual review of potentially important data that failed validation.

Alert Mechanism: When an invalid file is detected, the system sends an email notification to the Information Security Officer using SMTP protocol.

3. **Technical Architecture**

System Components:

Component	Description
Web Interface	Hosted on Vercel; provides upload functionality for lab technicians
Ubuntu Server	VirtualBox VM running Ubuntu with AWS CLI 2; handles validation logic
Temporary Bucket	S3 bucket for staging incoming files before validation
Production Bucket	S3 bucket for validated files ready for processing by medical systems
Quarantine Bucket	S3 bucket for isolated invalid files pending security review

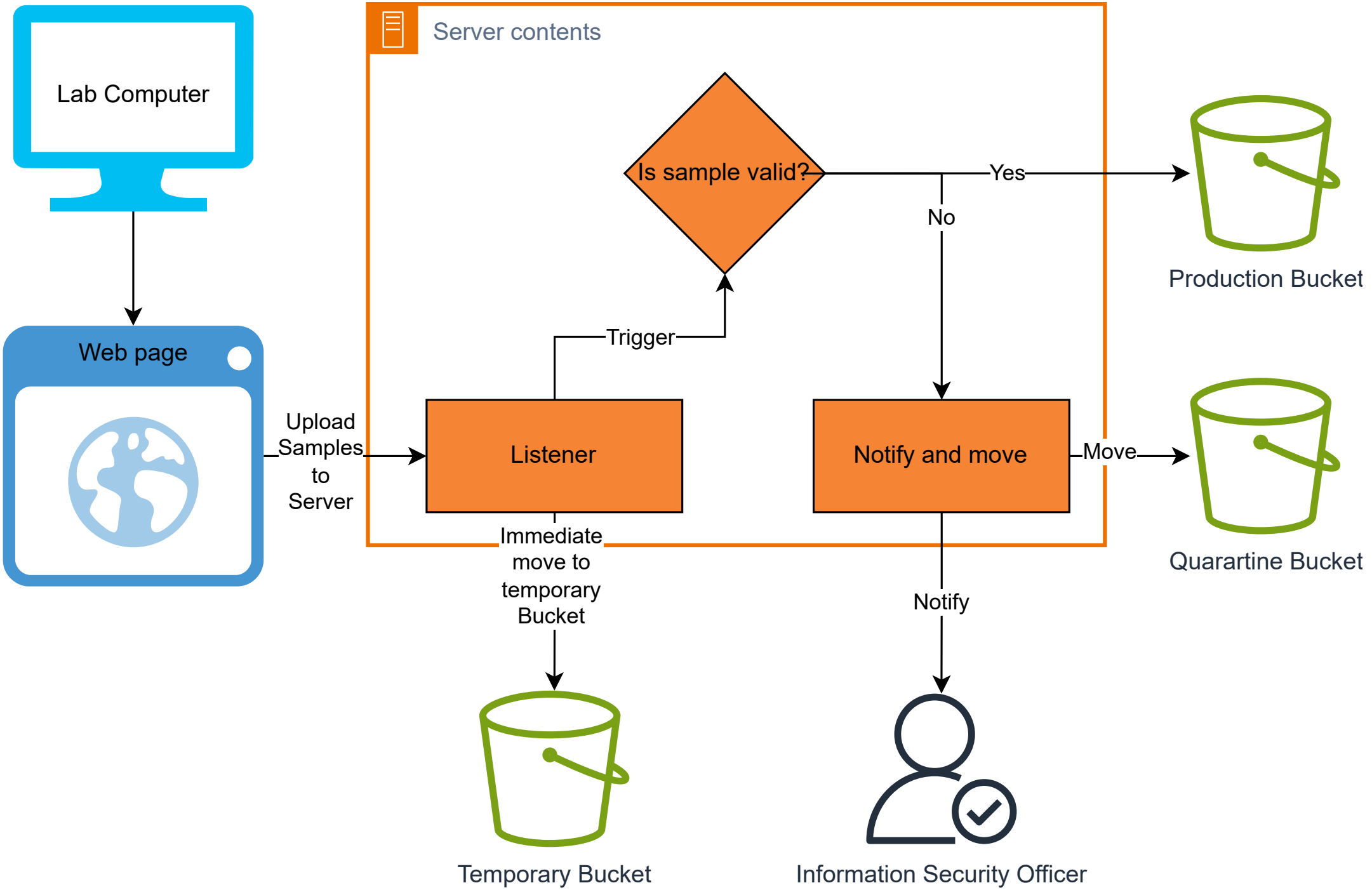
Data Flow

1. Lab technician uploads file via Web Interface Hosting on hosting service like Vercel (free hosting service).
2. File is transferred to the Ubuntu Server
3. Server immediately moves file to Temporary Bucket (prevents attacks during processing)
4. Server pulls file from Temporary Bucket for validation
5. Validation checks: PDF extension + "Blood Sample" content

6a. If valid → Move to Production Bucket

6b. If invalid → Move to Quarantine Bucket + Send email alert to Security Officer

Note: There is a separate Architecture file showing the diagram.


Lab Computer
Web page
Upload Samples to Server
Server contents
Is sample valid?
Yes
No
Trigger
Listener
Notify and move
Move
Production Bucket
Quarantine Bucket
Immediate move to temporary Bucket
Notify
Temporary Bucket
Information Security Officer