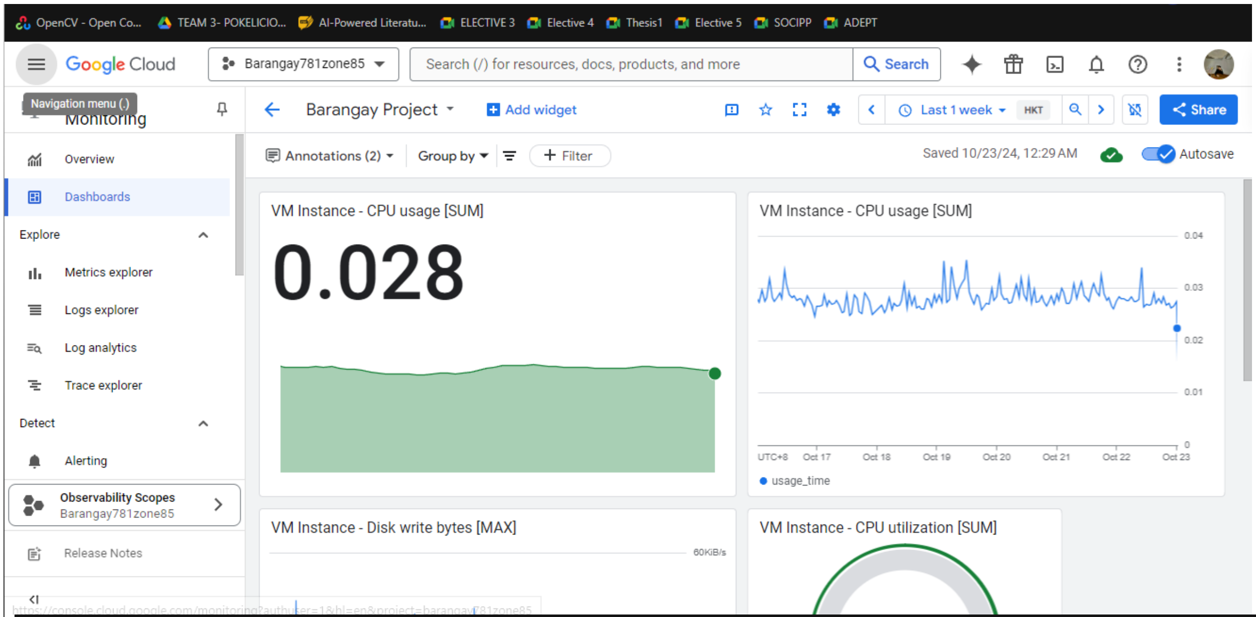
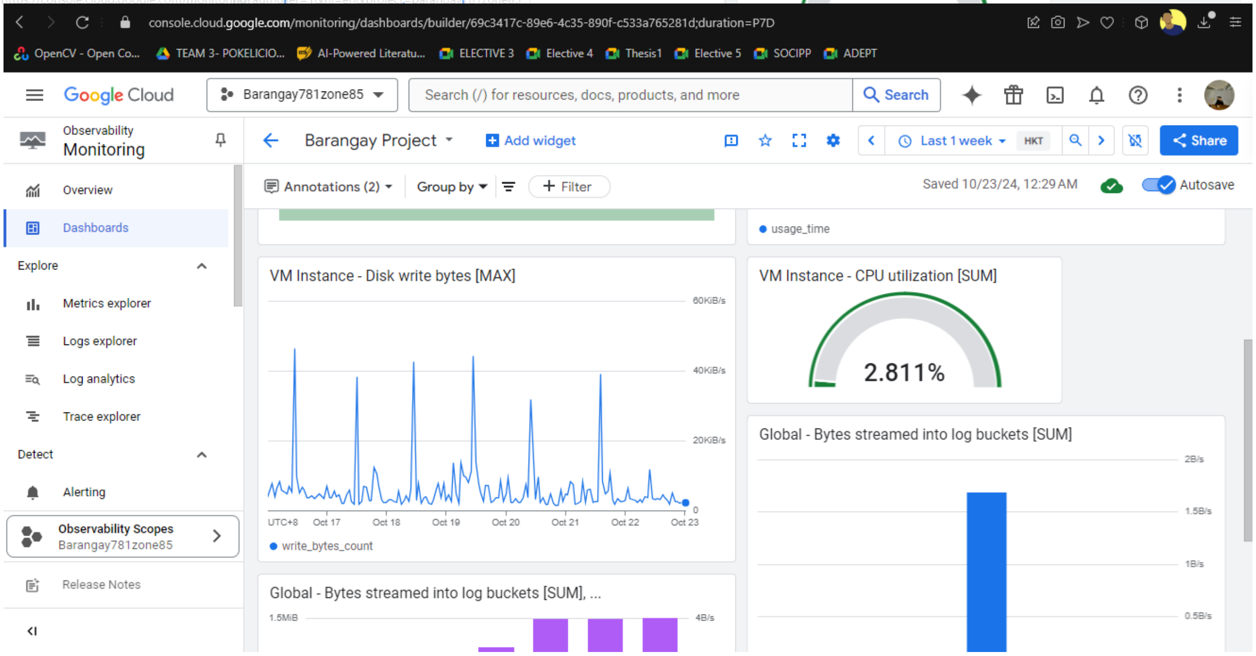
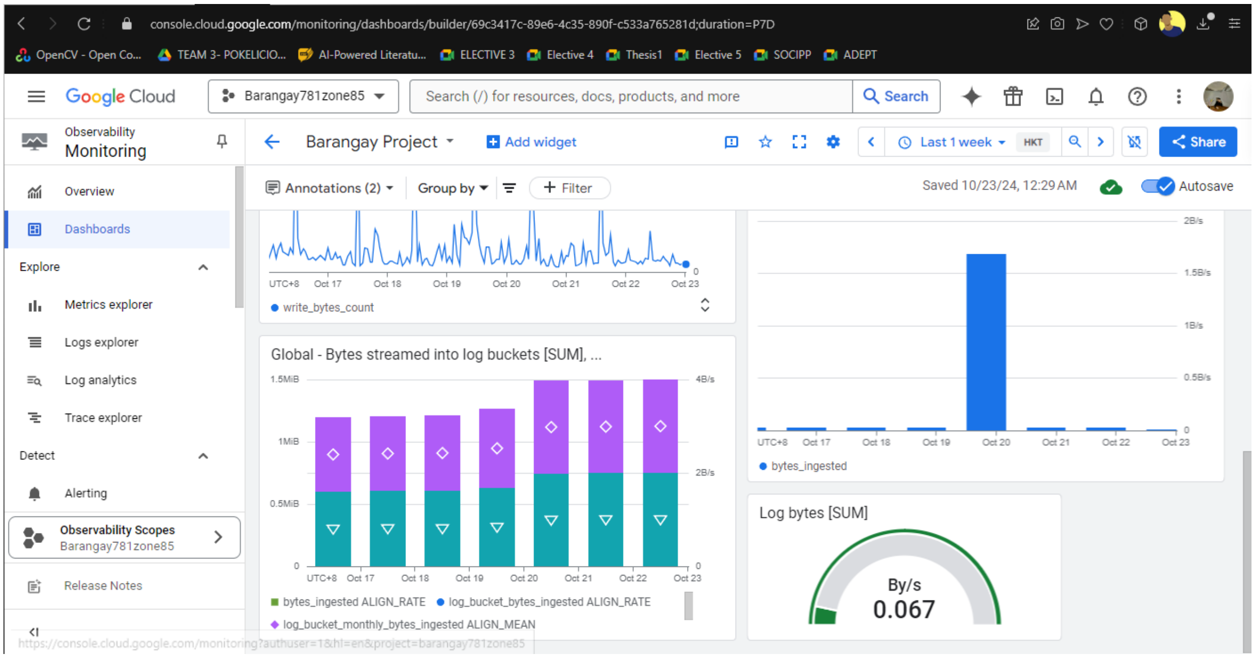
Provide a dashboard layout, add a story telling oh how a data was considered in the cloud, and cloud security using packet tracer.

MEMBERS:
Enrique, Jhon Mark
Canlas, Clyde
Formanes, Patrick
Recto, John Elvin







Story: CERTIFACE:AN ONLINE BARANGAY SYSTEM WITH IDENTITY AUTHENTICATION THROUGH INTEGRATION OF FACE RECOGNITION FOR BARANGAY 781 ZONE 85 STA.ANA MANILA GROWTH AND PERFORMANCE MONITORING.

Overview: CERTIFACE is an innovative **online barangay system** that integrates **identity authentication** using **face recognition** technology. It was designed to streamline services for Barangay 781 Zone 85 in Sta. Ana, Manila. The system handles a variety of sensitive data, authenticating users via facial scans for applications such as barangay clearance requests, resident information management, and community services. This story focuses on how CERTIFACE's **performance and growth** are monitored and managed through cloud infrastructure metrics.

Metrics Overview:

1. **VM-Instance: CPU Usage**
2. **VM-Instance: Disk Write Bytes**
3. **VM-Instance: CPU Utilization**
4. **Global: Bytes Streamed into Log Buckets**
5. **Audited Resources: Log Bytes**

VM-Instance: CPU Usage:

As the system expands, more users interact with CERTIFACE for face recognition-based identity authentication. This increases the load on the CPU of the virtual machine instances hosting the system. Monitoring CPU usage is crucial to ensure the system responds swiftly to authentication requests, avoiding delays that could frustrate users.

Recently, the CPU usage spiked during a period of high demand when the barangay implemented online submission for government aid, suggesting the need for system scaling during peak hours. This triggered the automatic scaling of additional VM instances to balance the load. Monitoring this metric allowed the system administrator to adjust resources dynamically, maintaining service reliability and performance.

VM-Instance: Disk Write Bytes

The Disk Write Bytes metric tracks the amount of data being written to disk by the virtual machines. With each new resident registration or face authentication, the system generates data logs, transaction histories, and face recognition comparison files. The system experienced a surge in disk write operations when face recognition logs for over 500 residents were stored in one day. This correlated with a registration drive that encouraged new residents to sign up for the barangay’s e-services.

Regular monitoring of disk writes helped administrators optimize data storage solutions, ensuring that sufficient space was available for data-intensive operations like saving face recognition templates and user activity logs.

VM-Instance: CPU Utilization

The CPU utilization metric provides a holistic view of how the system's resources are being used. CERTIFACE's face recognition system is computationally heavy, requiring a considerable amount of processing power to analyze and compare facial images during authentication.

CPU utilization gradually increased as more residents began using the system daily for identity verification. It peaked at 85% utilization during peak hours when both residents and barangay officials accessed the system simultaneously.

This led to the implementation of an auto-scaling feature that spun up additional VM instances during high-traffic periods, ensuring that the system remained responsive without overloading a single CPU.

Global: Bytes Streamed into Log Buckets

CERTIFACE generates logs for various activities, from user authentications to administrative actions within the system. The Bytes Streamed into Log Buckets metric reflects how much data is being stored in the cloud for auditing and monitoring purposes. This is critical for transparency and ensuring compliance with local governance standards.

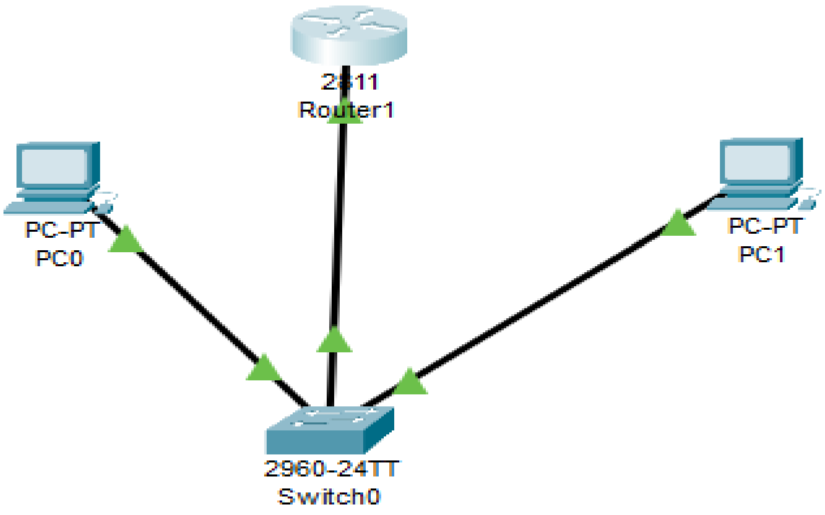
There was a significant increase in log bytes streamed into the buckets after face recognition failed attempts were logged by the system during routine audits. This alerted the team to a possible misconfiguration in the recognition algorithm, causing an unusual number of authentication failures. By tracking log bucket usage, the system administrators could investigate the issue promptly. They identified a technical bug that caused false negatives in the facial recognition match, allowing them to adjust the algorithm and improve accuracy.

Audited Resources: Log Bytes

As CERTIFACE deals with sensitive resident data, auditing logs is essential for tracking and analyzing all actions performed within the system. This includes data access, face recognition attempts, and administrative interventions.

After a security audit, a rise in log bytes was observed due to more detailed logs being created as part of an effort to enhance cloud security and user transparency. These logs were invaluable in pinpointing security vulnerabilities and ensuring that resident data was securely handled in compliance with the Data Privacy Act**.**

The team used the audited logs to enhance security protocols, set up more granular logging of sensitive actions, and implemented an alert system for suspicious activities such as multiple failed logins or unauthorized access to resident data.


2811
Router1
PC-PT
PC0
PC-PT
PC1
2960-24TT
Switch0