MIT | Arts, Commerce & Science College

ALANDI (D), PUNE

Affiliated to

SAVITRIBAI PHULE PUNE UNIVERSITY

An IT PROJECT REPORT

ON

"GOOGLE CONFIGURATION REVIEW"

BY

RAMKRISHNA JAYPRAKASH SAWANT

Under The Guidance Of

PROF.MANDAR P. PARALE

In Partial fulfilment of

SYMSC (COMPUTER SCIENCE)

Academic Year 2022-23

MIT | Arts, Commerce & Science College

CERTIFICATE

This is to certify that, the project report entitled “GCP configuration Review" which is submitted by Mr. Ramkrishna Sawant in partial fulfilment of Master of Science - Computer Science has satisfactorily completed the project work under our guidance and supervision.

We wish our best wishes for his future endeavor.

Prof. Mandar Parale

Project guide

Dr. Sangita Birajdar

HOD (Science and Computer Science)

Internal Examiner

External Examiner

SECURITYBOAT
Frontline Of Your Business

Feb 6th, 2023

Ramakrishna Sawant

Re: Internship offer

Dear Ramakrishna Sawant

On behalf of Securityboat, I am excited to extend an offer to you for an internship position as a Security Analyst Intern.

This position is scheduled to begin on Feb 6th, 2023, and will be 6 months paid internship opportunity ending on Aug 6th 2023. The schedule for this position is flexible. This position will pay ₹6000 per month. Your work location would be Pune, Maharashtra, India. As a temporary employee in the role of an intern, you will not be eligible for any company-sponsored benefits. In this role, you will report directly to Ninad Mathpati. We are confident that you would play a significant role in the overall success of the venture and wish you the most enjoyable, learning packed and truly meaningful internship experience with Securityboat.

*Your appointment will be governed by the terms and conditions presented in the **Annexure A**.*

We look forward to having you begin your Security Analyst Intern career at Securityboat and wish you a successful internship. Welcome to our team!

Sincerely,

Ninad Mathpati
Founder & CEO

Securityboat Pvt Ltd

+91 8888332999
support@securityboat.in
www.securityboat.in
Pune, Maharashtra, India

SECURITYBOAT
Frontline Of Your Business

Date: 23 May 2023

TO WHOM IT MAY CONCERN

This is to certify that Mr. Ramkrishna Jayprakash Sawant a Student of Department of Computer Science, **"MIT Arts Commerce & Science College Alandi Pune"**, has undergone a project work in **Q1** from **06th February 2023 – 15th May 2023** titled **"GCP Configuration Review".**

We found him hardworking & Sincere in his work. We extend our best wishes for his future professional growth.

Thank You,

Ninad Mathpati
CEO & Founder
SecurityBoat Cybersecurity Solutions Private Limited.

Disclaimer: This document is valid, subject to the associate being employed with us and undergone the above titled project.

+91 9175154999 www.securityboat.in Pune Maharashtra, India

ACKNOWLEDGEMENT

I take this opportunity to express my sincere gratitude to everyone who has directly or indirectly helped me in completing the project successfully.

I own profound intellectual debt to Mr. Mandar Parale who notwithstanding his busy schedule and personal commitments has been guiding the force and a source of encouragement and helped me throughout the course of my project and for being an inspirational force and devoting genuine interest throughout the progress of the project, interacting with him I learnt a few important aspects of project and I am sure the knowledge imparted to me will help me to enrich my career in the long run.

I am also thankful to Prof. Dr. B. B. Waphare, Principal MIT Arts Commerce and Science College Alandi, Pune and also to Dr. Sangita Birajdar, HOD(Science and Computer Science) for providing me with this opportunity.

I express my gratitude for Dr. Sangita Birajdar for providing me an opportunity to have his valuable guidance and continuous monitoring.

I take this opportunity to thank my family members, friends without their cooperation I would not have been able to complete this project.

Ramkrishna Sawant

SYMSC(CS)

DECLARATION

I, hereby declare that the project report on "GCP Configuration Rewiew'' is written and submitted by me to MAEER's MIT Arts Commerce and Science College, Alandi (D), Pune, towards the partial fulfilment for the study of Masters of Science (Computer Science) in year 2022-2023 is original work done by me, which is based on the primary and secondary data and it is based on the knowledge and material gained from the company , website and other documents.

The contents provided are true to the best of my knowledge and beliefs.

I further declare that this project report has not been submitted to any other college or university for any other degree or course earlier.

Place: Alandi Devachi,Pune

Date:

Ramkrishna Sawant

SYMSC(CS)

INDEX

1.Abstract

The Google Configuration Review Project is an automated bash script that simplifies and enhances the process of assessing configuration settings for Google services. By leveraging bash automation, the project scans and analyzes Google configurations against best practices and security guidelines, identifying vulnerabilities and suggesting improvements. The project promotes consistency, scalability, and proactive security measures, enabling organizations to optimize their use of Google services while maintaining compliance and strong security posture.

2.Introduction

2.1 Motivation

Google Cloud Configuration Review is becoming increasingly important in today's technology landscape. While there are some concerns about data privacy, ensuring that customer data is 100% accurate is a top priority for any organization.

As I embarked on the Google Cloud Configuration Review project, Mr. Ninad Mathpati provided me with invaluable guidance and support, helping me to deepen my understanding of the concepts and serving as a source of motivation throughout my journey from a novice to a subject matter expert. Their expertise and mentorship have been instrumental in my professional development and have inspired me to continue pursuing excellence in my work.

2.2 Problem Definition:

Moving into the era of cloud computing, it is crucial to ensure that the security of cloud services and applications is thoroughly reviewed and configured. At Google Cloud, we understand the importance of protecting our customers' data and infrastructure from security threats. Therefore, we offer a security configuration review service that provides our customers with a comprehensive assessment of their security posture and identifies potential vulnerabilities.

Our goal at Google Cloud is to provide our customers with a comprehensive security review that identifies potential security risks and provides actionable recommendations to improve their security posture. We believe that our security configuration review service can help our customers achieve a more secure and resilient cloud infrastructure, ensuring the safety and confidentiality of their data.

2.3 Purpose of the Project:

1. To identify and mitigate security risks in the Google Cloud environment by reviewing the security configuration settings via automated checks.

2. To ensure that all data and information stored in the Google Cloud platform is properly secured and protected against unauthorized access, modification, or deletion.

3. To assess the organization's compliance with relevant security standards and best practices, such as the CIS Google Cloud Computing Foundations Benchmark.

4. To help the organization in developing and implementing an effective security strategy for the Google Cloud platform, which includes ongoing monitoring, auditing, and reporting of security-related events.

2.4 Literature Survey

1. When it comes to cloud security, Google Cloud faces tough competition from other cloud providers like Amazon Web Services (AWS), Microsoft Azure, and IBM Cloud.

2. The unique selling proposition (USP) of Google Cloud's security configuration review is its ability to provide comprehensive and efficient security solutions to businesses with a focus on securing critical data and infrastructure.

3. Google Cloud has always been a leader in the cloud industry by continuously introducing new security features and technologies, such as Google Cloud Armor, Cloud Identity-Aware Proxy, and VPC Service Controls.

4. Google Cloud's security configuration review is not only designed for traditional IT infrastructure but also for modern cloud-native architectures and services, such as Kubernetes, BigQuery, and Cloud Storage.

5. Precision and accuracy are paramount when it comes to securing cloud infrastructure and protecting sensitive data. Therefore, Google Cloud maintains a strict quality threshold of 99% accuracy in its security configuration review to ensure maximum protection against cyber threats.

2.5 Project Scope & Limitations:

1. To provide a secure environment for the Google Cloud services and applications by reviewing the security configuration settings.
2. Identify any potential vulnerabilities or misconfigurations that could lead to security breaches or data leaks.
3. Develop recommendations to improve security posture and ensure compliance with industry best practices and regulatory requirements.
4. Limitations include the fact that some security vulnerabilities or misconfigurations may not be detected during the review process due to limitations in the review tools or access to certain system components.
5. Additionally, the review is focused solely on the security configuration settings and does not cover any security issues that may arise from application code or user behavior. Users are encouraged to follow best security practices and guidelines when using Google Cloud services.

3. System Analysis

Systems analysis the process of observing systems for troubleshooting or de velopment purposes. It is applied to information technology, where computer-based systems require defined analysis according to their makeup and design.

3.1 Comparative Study of Existing System

1. Existing systems focus on infrastructure provisioning and configuration, while ScoutSuite specializes in security auditing and assessment for cloud environments.
2. The existing systems automate the provisioning and configuration of GCP resources, whereas ScoutSuite identifies security misconfigurations and vulnerabilities.
3. Infrastructure as Code is commonly used in existing systems, allowing the management of infrastructure using scripts or declarative templates. ScoutSuite provides predefined security checks and rules specific to GCP.
4. The existing systems offer customization and flexibility, while ScoutSuite provides comprehensive security coverage across multiple cloud providers, including GCP, with reporting and visualization capabilities.

3.2 Scope & Limitations of Existing Systems

Scope-

1. Conduct a comprehensive review of the Google Cloud security configuration and settings.
2. Analyze access control policies, network security configurations, and other security controls to ensure they are aligned with industry best practices and compliance standards.
3. Evaluate security posture for Google Cloud services such as Compute Engine, Kubernetes Engine, and Cloud Storage.
4. Provide recommendations for remediation of security risks and vulnerabilities.

Limitations-

1. The configuration review is limited to Google Cloud services and does not cover third-party applications or services that may be integrated with the Google Cloud environment.
2. The review does not guarantee the detection of all security risks or vulnerabilities in the Google Cloud environment.
3. The review does not cover physical security controls at Google data centers or other physical infrastructure.
4. The review does not provide legal or regulatory compliance assessments but may provide recommendations for alignment with industry best practices and standards.

3.3 Stake Holders

1. Customers.
2. Organizations.

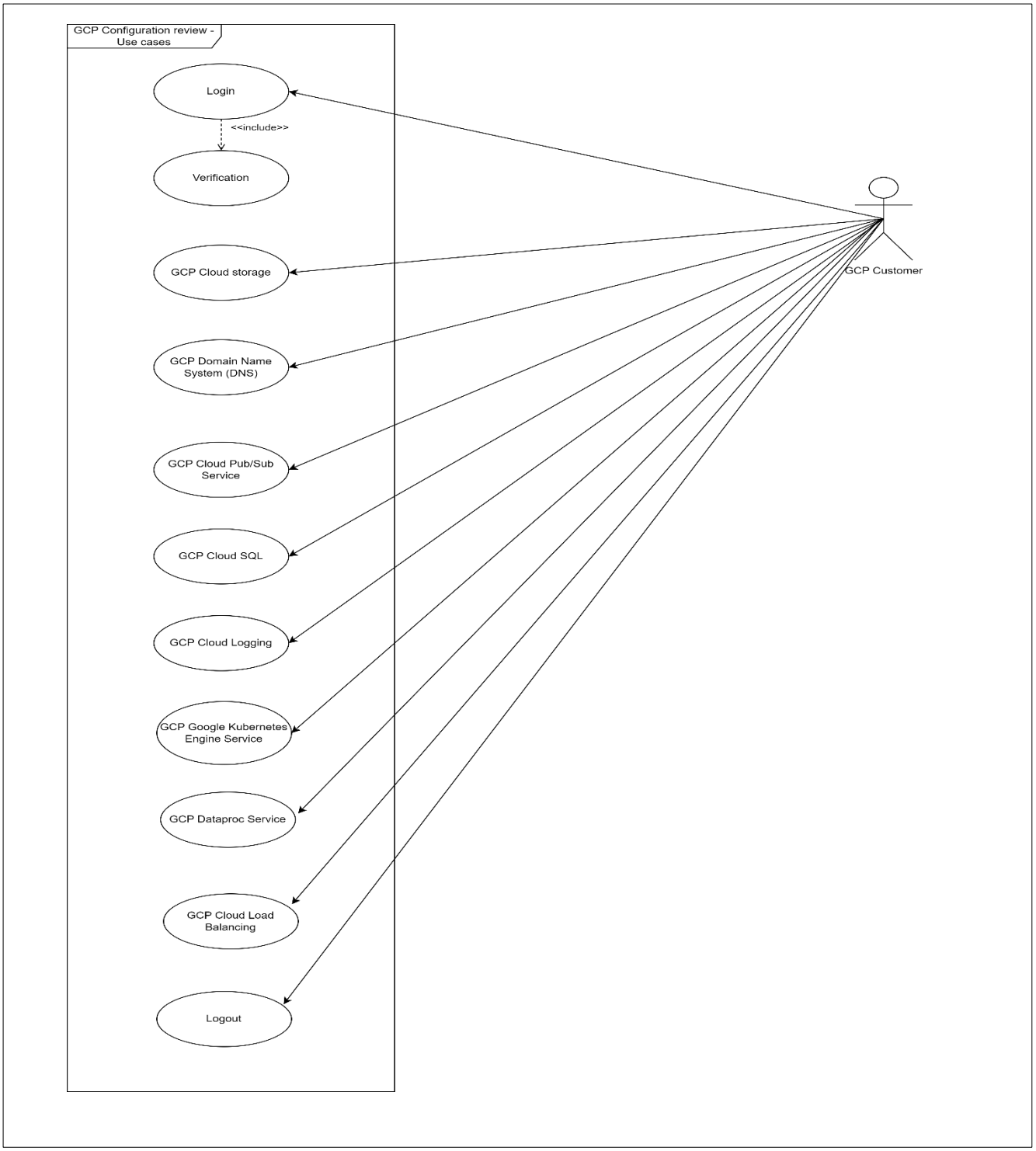
4. System Design

4.1 Design Constraints

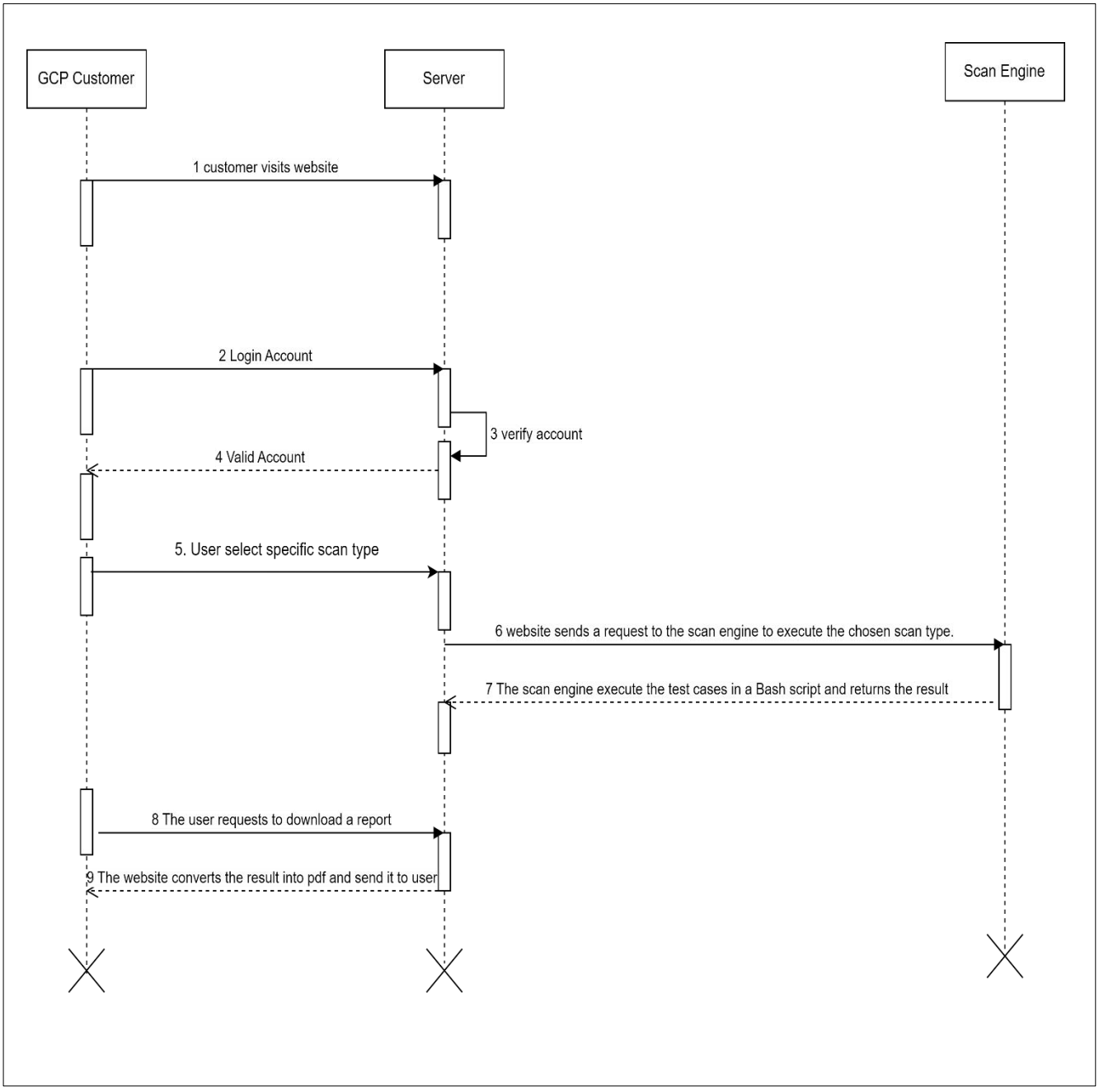
In this Projects the Design Constraints were *Use Diagram, Sequence Diagram, Activity , Deployment Diagram.* Reason for these Constraints are that High Confidentiality of the Project - Limited Information is shared with the respective teams.

4.2 System Model – UML Diagrams

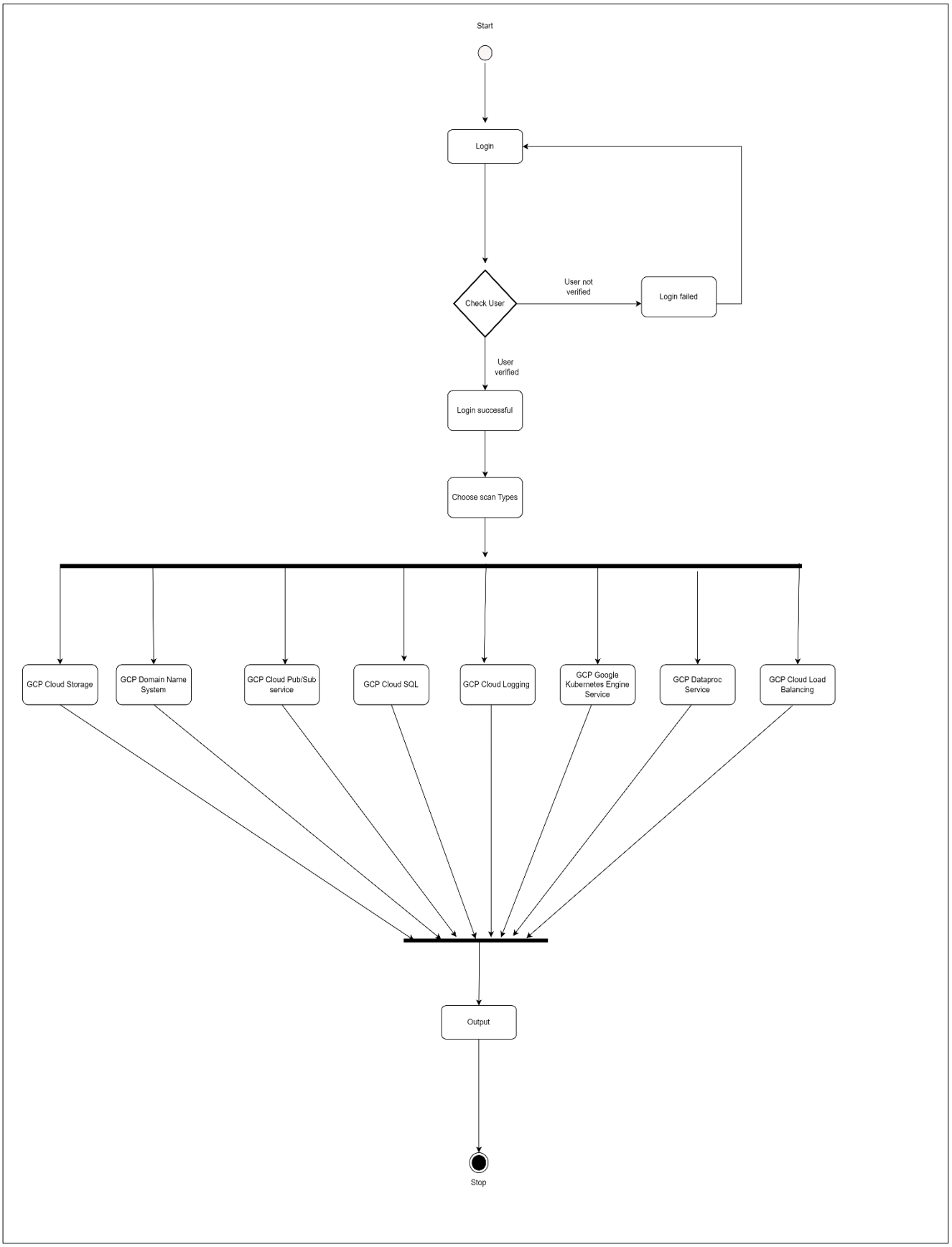
Use Case Diagram



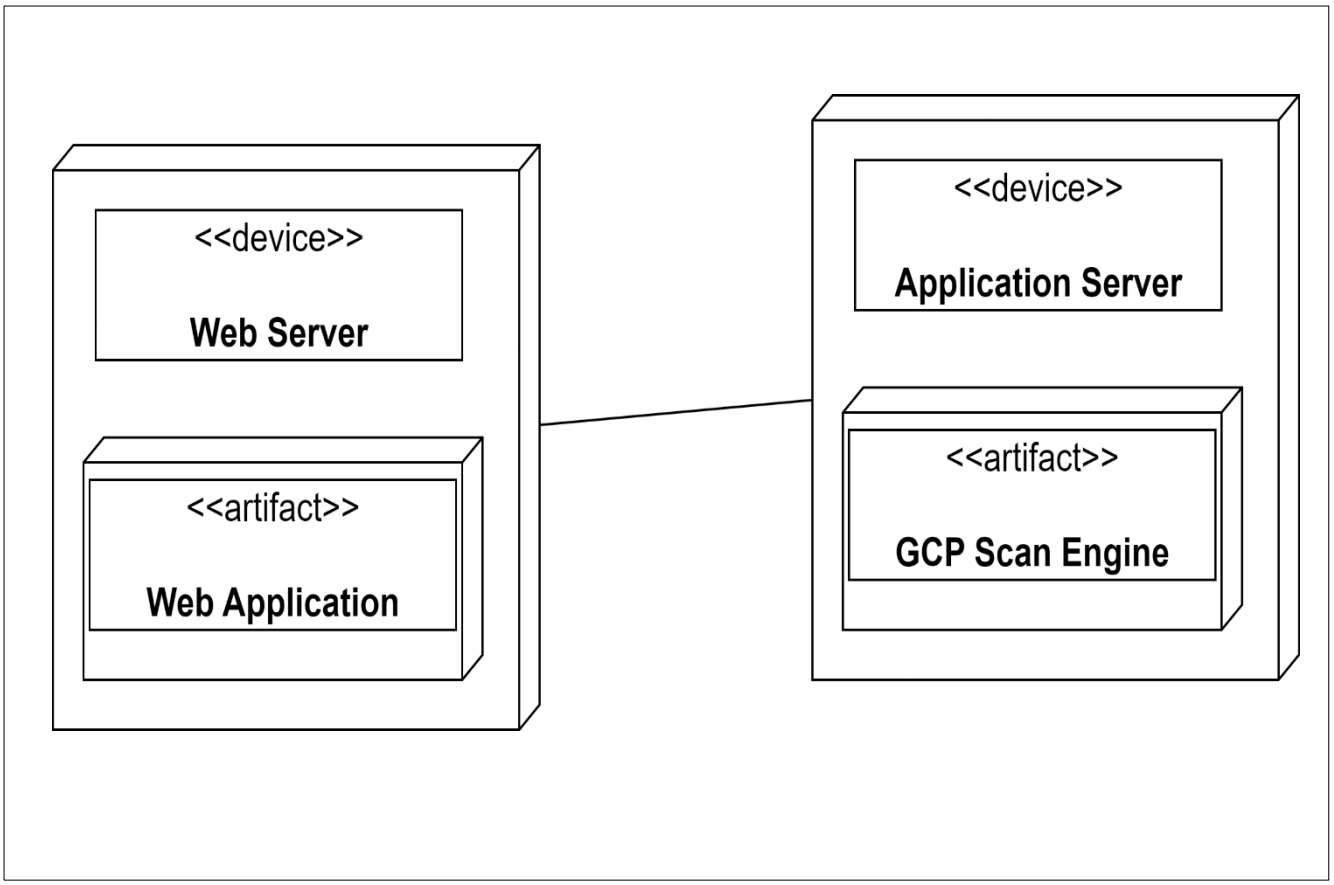
Sequence Diagram



Activity Diagram

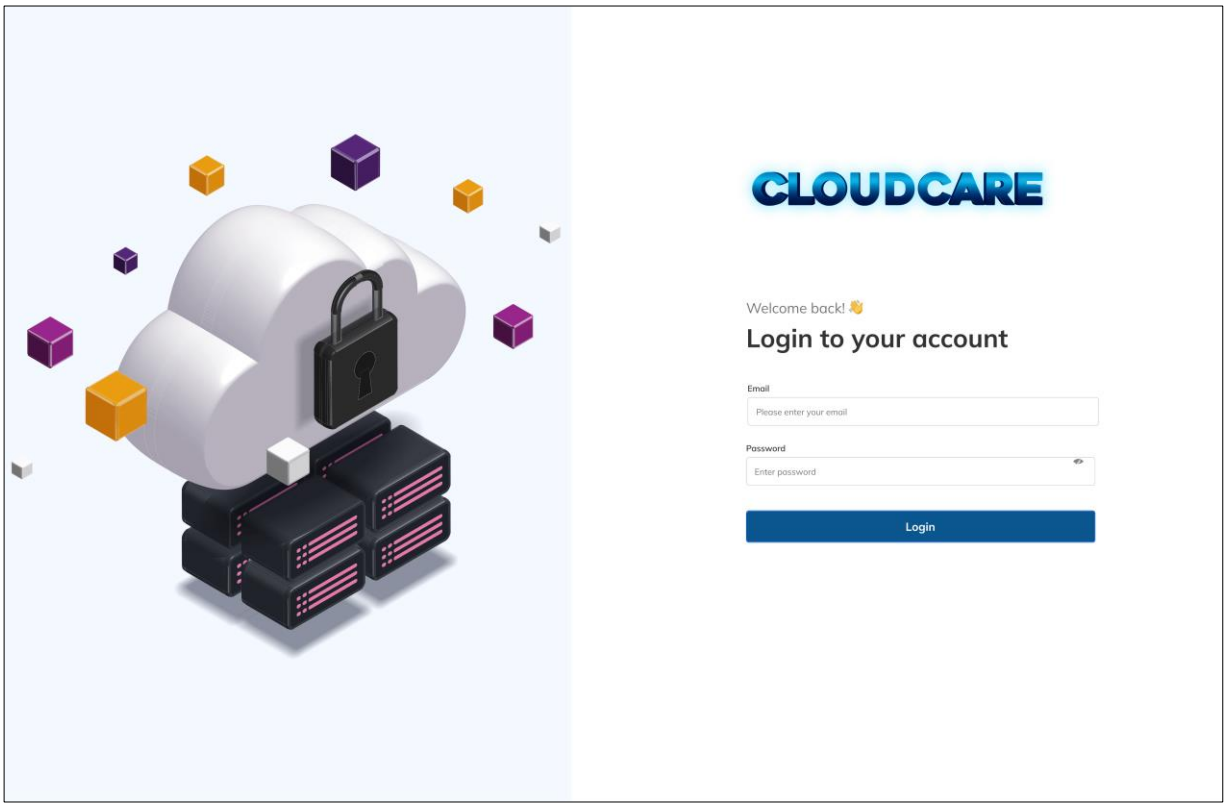


Deployment Diagram

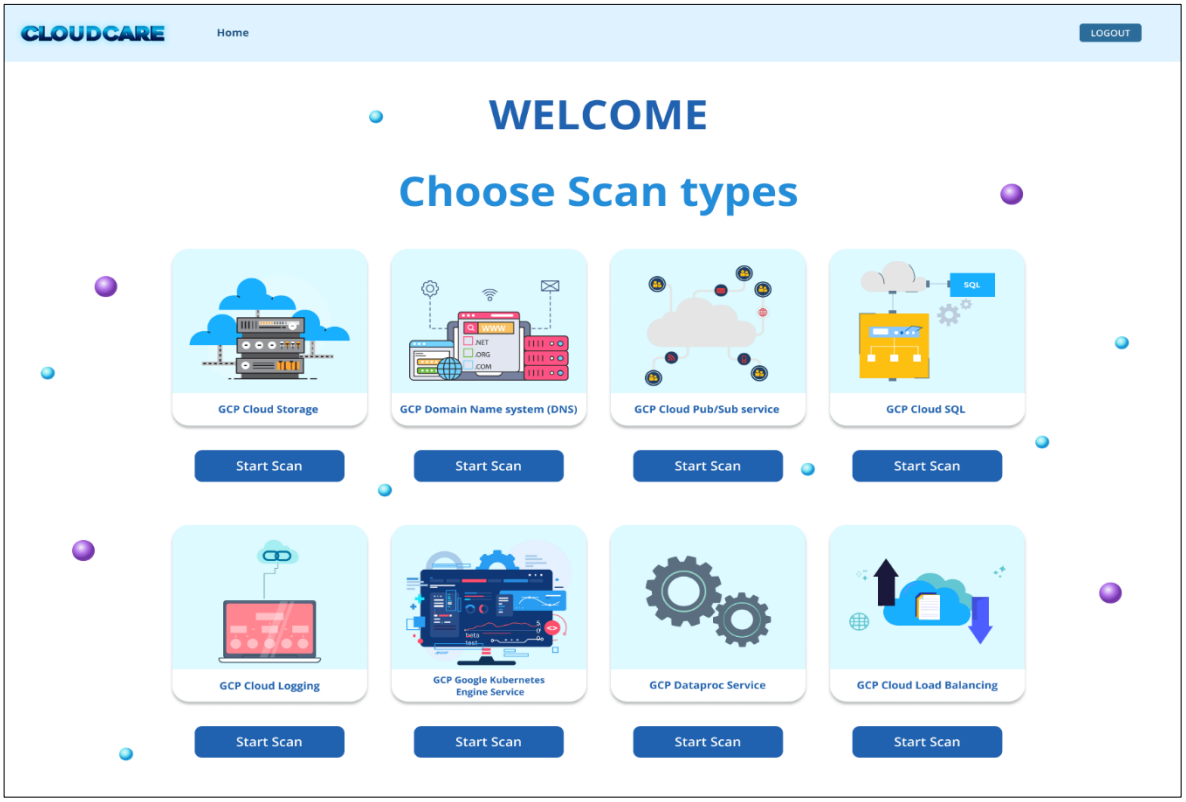


4.3 User Interface

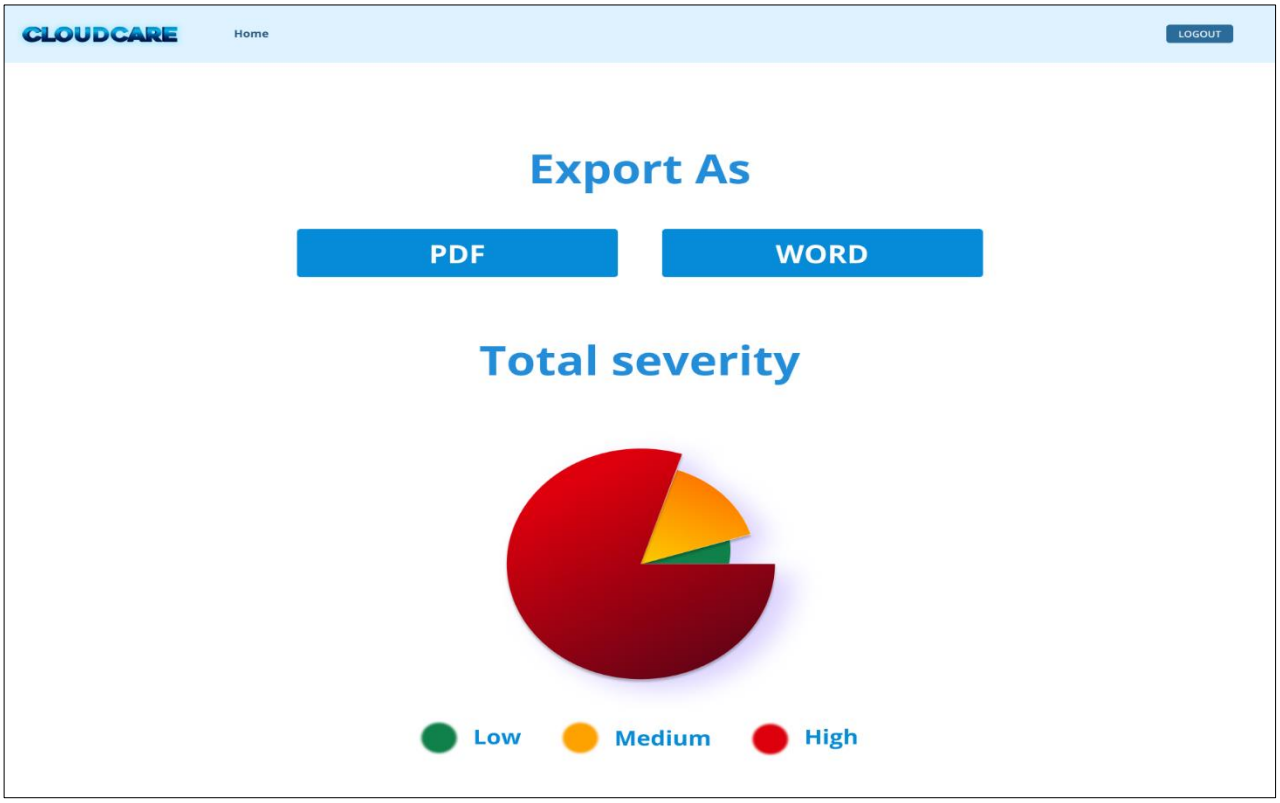
1. Customer Login page.



2. Dashboard consists of various scan types.



3.Report exporting Dashboard.



5. Implementation Details

5.1 Software Hardware Specification

Coder -

Hardware Requirement: -

1. Processor: Intel I9
2.RAM: 8 Gb
3.Operating System: Linux
4. Hardisk: 1 TB

Software Requirement: -

1. Browser: Any Browser
2. Backend: PHP, Bash,
3. FrontEnd: HTML, CSS, JAVASCRIPT.

User –

Browser.

6. Test cases

Sr. No	Test Case ID	Test Case Objectives	Expected Result	Actual Result	Status
1	Case 01	Check for Publicly Accessible Cloud Storage Buckets	Check for the bucket is publicly accessible.	The bucket found publicly accessible the add it to output file.	Pass
2	Case 02	Check for Sufficient Data Retention Period	Check for Sufficient Data Retention Period conformity rule settings.	During test case it was observed that the data retention is of 7 days.	Pass
3	Case 03	Enable Object Versioning for Cloud Storage Buckets.	Check for Object Versioning for Cloud Storage Buckets is enabled or not.	During the test case it was observed that Object Versioning is enabled .	Pass
4	Case 04	Enable Uniform Bucket-Level Access for Cloud Storage Buckets	Check for Uniform bucket-level access setting is enabled .	During the test case it was observed that Uniform bucket-level access setting is enabled .	Pass

5	Case _05	Enable Lifecycle Management for Cloud Storage Objects	Check for Lifecycle Management is configured or not.	During the test case it was observed that Lifecycle Management is configured .	Pass
6	Case _06	Check for DNSSEC Key-Signing Algorithm in Use	Check for the DNS SEC uses rsasha1 algorithm.	During the test case it was observed that DNSSEC uses rsasha1 algorithm.	Pass
7	Case 07	Enable DNSSEC for Google Cloud DNS Zones	Check for state of DNSSEC for Google Cloud DNS Zones is off.	During the test case it was observed that the state is off.	Pass
8	Case 08	Check for Cloud SQL Database Instances with Public IPs	Check for Cloud SQL database instances are configured to use private IP addresses instead of public IPs.	During the test case it was observed that the SQL database instance uses private IP.	Pass
9	Case 09	Check for MySQL Major Version	Check for the GCP uses latest MYSQL version	During the test case it was observed that GCP uses MySQL 8.0.	Pass

10	Case 10	Check for POSTgreSQL Major Version	Check for the GCP uses latest POSTgreSQL version	During the test case it was observed that GCP uses POSTgreSQL 14.	Pass
11	Case 11	Check for Insecure SSL Cipher Suites	Check the Secure Socket Layer (SSL) policies associated with your HTTPS and SSL Proxy load balancers	During test case it is observed that load balancer uses Weak cipher suite	Pass
12	Case 12	Enable HTTPS for Google Cloud Load Balancers	check that your Google Cloud Platform (GCP) load balancers are configured to use valid SSL/TLS certificates	The load balancer is not mapped with SSL and TLS certificates.	Pass

13	Case 13	Enable Auto-Repair for GKE Cluster Nodes.	Check For the Auto-Repair feature is enabled for all your GKE cluster nodes.	During the test it was observed that the management configuration is **null** which means Auto-Repaiir is not enabled.	Pass
14	Case 14	Enable Secure Boot for Cluster Nodes.	Check for the secure Boot security feature is enabled for your GKE cluster nodes.	During the test it was observed that shieldedInstanceConfig was **null** which means Secure Boot for Cluster Nodesis disabled.	Pass
15	Case 15	Configure Root Password for MySQL Database Access	Check for Google Cloud MySQL database instances do not allow anyone to connect with administrative privileges only.	Detailed information of patient is displayed	Pass

7. Conclusion

Automating the GCP configuration review process offers numerous benefits, including improved efficiency, accuracy, and consistency. It enables the identification of misconfigurations, security vulnerabilities, and adherence to best practices. Automation reduces manual efforts, streamlines the review process, and ensures a secure GCP infrastructure.

8. References

- https://www.trendmicro.com/cloudoneconformity/knowledge-base/gcp/
- https://cloud.google.com/docs
- https://github.com/jorwalk/cloud-architect-gcp/blob/master/Best-Practices.md