DEGREE PROJECT

Insider Threat For Service Account in Google Cloud Platform

Ravikiran M Talekar

Information Security, master's level (120 credits)
2023

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

LULEÅ UNIVERSITY OF TECHNOLOGY

[This page intentionally left blank]

Abstract

As most software industry is migrating from traditional servers and depending more on Cloud-based services, we are encountering new problems hitherto unknown to us. Due to the various advantages offered by Cloud services and the numerous problems whose solutions are provided by Cloud technologies, cloud-based services have become very popular. Organizations of all sizes widely use them to meet their day-to-day technology needs. Cloud infrastructure mainly consists of Cloud resources and services, which are accessed through user and service accounts.

This thesis considers the challenge of securing service accounts of cloud providers by service account keys. In the realm of cloud security, a central challenge revolves around the effective protection of service account keys to thwart unauthorized access and the potential for data breaches, all while ensuring that legitimate operations maintain the necessary access. Each service account is intricately linked to a set of credentials, comprising both private and public keys used for interactions with external APIs. These credentials play a critical role in authenticating the service account and granting it authorization to access resources within Google Cloud Platform (GCP). Notably, when service account keys are not downloaded, the private key remains confined within the GCP environment, limiting service interactions. Conversely, the act of downloading the private key increases the risk of exploitation, as it represents the most sensitive component of the service account credentials. Without access to the private key, the authentication of the service account and subsequent access to GCP resources becomes unattainable.

To address the holistic challenges in this thesis, it's crucial to emphasize the importance of securing service account keys and limiting access to authorized users. This led to the proposal of a key rotation process to achieve our research objectives. The approach taken in this study involves both qualitative and quantitative methods. This includes a thorough literature review and interviews with cloud professionals, allowing us to gain insights into the threats through content analysis and a SWOT-based assessment. This method is aimed at mitigating the risk of service account key exploitation.

TABLE OF CONTENTS

FIGURES

TABLES

ABBREVIATIONS

CSP:	Cloud Service Provider
GCP:	Google Cloud Platform
IAM:	Identity and Access Management
API:	Application Programming Interface
VM:	Virtual Machine
gRPC:	Google Remote Procedure Call
IAP:	Identity Aware Proxy
DCs:	Domain Controllers
gCloud:	Google Cloud
CSB:	Cloud Storage Broker
AE:	Authenticated Encryption
DEM:	Data Encapsulation Mechanism
CI/CD:	Continuous Integration Continuous Deployment
GKE:	Google Kubernetes Engine
SIEM:	Security Information and Event Management
SOP:	Standard Operating Procedures
IaaS:	Infrastructure as a Service
PaaS:	Platform as a Service
SaaS:	Software as a Service
RBAC:	Role-Based Access Control
ITSM:	IT Service Management
CM:	Configuration Management
IaC:	Infrastructure as Code

1 Introduction

Cloud computing is an emerging revolutionary technology that is changing the way of building and hosting the services application and managing the data within the organization by ensuring confidentiality, integrity, and availability of the information are maintained securely [1]. Cloud computing is considered the future of computing systems, envisioned as a secure and customizable way of accessing and operating various cloud-based applications and data hosted within the cloud platform. The cloud platform provides a myriad of services such as data storage, code deployment, log management, caching services, and databases, among others, where cloud-based activities are handled by the CSP (Cloud Service Providers). Cloud resources offer the flexibility of scalability, reliability, productivity, and efficiency by reducing the organization's expenditure [2]. Additionally, cloud users can store their data and applications in remote servers with a guarantee of being accessible from anywhere, irrespective of the user's location [3]. Even though cloud technology promises advantages in several areas for users, it faces some challenges in the security and privacy of resources and information within the cloud environment. In addition, insider threats are growing security concerns that hinder the organization from adapting to cloud technology [4]. These threats can target an organization, for example, from an external or internal basis.

Internal security threat is the kind of threat that arises inside the organization. Insider threat is caused by malicious users who can intentionally or unintentionally compromise the information and assets belonging to the organization [5]. During their tenure in the organization, the users will have legitimate access to the cloud services based on their roles and responsibilities. However, after they have ended their association with the organization, they may try to access the services to malign their past organization by compromising confidentiality, integrity, and availability [6]. Insider threat is among one the growing threats to the cloud industry. The malicious user can be consultants, employees, or support people accessing the cloud platform. In addition, the cloud platform can be accessed via a user login and service accounts [7].

Cloud Service accounts are special accounts intended to represent non-human users who need to authenticate and access data using cloud APIs. A private key is generated when a service account is created. These keys are downloaded to the user's local computer, which are stored forever. Users can access data using the cloud APIs using this service account and private key.

The problem arises when the user role is changed or the user is a former employee since the service account key has a long expiry date. There is a potential threat that these service accounts will be used to compromise confidentiality, integrity, and availability of the information and resources within the cloud environment. *This thesis studies the use of the cloud service account and provides recommendations on the service account's key rotation process*. A service account is a unique account identified by its email address. It is provisioned to make authorized API calls to perform specific cloud operations on behalf of the user or a program [7]. Unfortunately, many organizations have a ”set it and forget it” [8] attitude when creating and configuring the service account. These are often left unmonitored and mostly configured with excessive privileges. This thesis focuses on the insider threats in the Cloud Platform, which may arise due to the unmanaged service accounts [9] keys.

1.1 Motivation

Service accounts have access to critical services and data while flying beneath the radar of IT governance. They take a long time to find and control, so they are prone to human error when handled manually. As a result, the author witnessed service account sprawl in almost all medium to big businesses, maintaining the unmanaged, uncontrolled increase of their privileged account attack surface [10].

Here is where the survey [11] results become interesting: one-third of security professionals believe service accounts are only altered or never rotated after a security event. Organizations are aware of the high risk of maintaining and securing service accounts, yet they are not adequately protecting them. Due to the long non-expiring nature of the service account key, there is a risk of compromising the confidentiality, service, and integrity of the data and resources within the cloud environment. Usually, the key pairs are, for example, configured to expire after ten years [12]. However, a formal employee will have the private key available, authenticating to a cloud environment using the private key, this scenario is classified as an Insider threat. It requires a prevention policy either by designing the prevention method or policy implementation document with best practices for handling the user-managed service account. Rather than using the system accounts, it is recommended to use a service account to run the application services [13]. If the service account is compromised, the losses will be limited compared to a system account.

1.2 Problem Statement

Most organizations working with cloud platforms tend to have a build and forget mindset. In this thesis, we will consider the security of the service accounts. Service accounts are unique accounts and differ from individual accounts as they are used to provide access to one or more Cloud APIs. Therefore, the service account can be an identity to distinguish apps running on our Virtual Machine(VM) instances from other services on the Google Cloud.
An example of this can be a custom-written application that reads and writes files to Cloud Storage, requiring authentication to Cloud Storage API to perform its tasks. This can be achieved by creating a service account and granting it the Cloud Storage permissions; the application needs to get updated to pass the service account details to the API. This leads to seamless authentication to the API without storing the credentials in the code, instance, or any docker image. However, creating a service account leads to the generation of the private key [14], which is stored forever on the user's system, which the user can then use along with the service account to access the data in the cloud. This research addresses how to secure the service account by dynamically performing the key rotation process for service accounts so there is no dependency on the static keys. The problem with using a private key is that there is no provision for key rotation, which can lead to security issues in compromised service account keys or if the user has changed the assignment. Even if the concerned user has a role change, they will still have the previous private key stored in the local system, and the same can be used for malicious attacks.

1.3 Research Questions

Based on the research problem statement as discussed above, this research aims to attempt to answer the following question:

1. What is the security posture of service accounts in organizations adapting to a cloud infrastructure?
2. How can the key rotation process secure service-account private keys so that publicly available cloud APIs are not exploited?
3. How to ensure that service account keys are not compromised?

1.4 Research Objectives

This research aims to address the research questions by achieving the following objectives:

Objective 1: Review the literature on state of the art in cloud computing security and risks associated with service accounts in cloud infrastructure with the most current active research areas of development and technology and open problems that define the research directions in this area.
Objective 2: Conduct qualitative data analysis by interviewing Cloud professionals, investigating security, service account controls, main challenges, and recommendations from the interview by conducting content and SWOT analysis.
Objective 3: Conduct quantitative data analysis by creating the prototype of the service account key rotation process based on the data collected from interviews with professionals in different domains in cloud technologies and security.
Objective 4: Highlight the limitation, recommendations, and future enhancements based on the findings and analysis of the collected data from qualitative and quantitative analysis.

1.5 Research Limitations

As with most research, this research also suffers from certain limitations. A few of the research limitations have been discussed below:

- Due to the relatively new existence of cloud computing services, the nature of threats to the service accounts is still not explored completely. Therefore, there are not many resources or, more importantly, reliable resources available to conduct the research. In addition, though people have written about cloud security and how to eliminate the threats, there is little about internal security threats around cloud service accounts to the cloud as it is relatively new and unexplored.
- Despite many efforts being made towards securing the cloud by the organizations, they have ignored the internal security threat from their employees due to its stigma, as it also questions the organization's credibility.
- Several other factors may not have been considered while this research was conducted.
- In some cases, organizations refuse to talk about the cases of internal security threats that they have faced as it will require the questioning of their employees and will bring attention to the organization's functioning and the security loopholes.
- The time zone over which the research has been conducted is relatively small. Therefore, it may not represent all the issues or causes behind the internal security

threats. The research could have been more longitudinal to depict all the facets of the problem properly.

- In the context of this thesis, the limitations of Google Cloud Platform (GCP) have been thoughtfully integrated as a key component of the research framework. By considering GCP as a use case, the study acknowledges the real-world challenges and constraints that may arise within this specific cloud computing environment, providing a comprehensive and practical perspective for the research findings and conclusions.

Getting security-related data from big or so-called reputed organizations is tough as they do not disperse the information regarding their internal processes to outside sources. Thus, our research only depends on the data available from other research, an interview conducted earlier, or articles on the internet. Though all these give quite a good idea about the issue, it lacks the practical examples department.

1.6 Conclusion of Introduction

The introduction provides an overview of the significance of cloud computing in modern technology, emphasizing its benefits in terms of scalability, cost-efficiency, and accessibility. However, it also highlights the growing concern of insider threats within cloud environments, particularly focusing on the security risks associated with unmanaged service accounts. These accounts, which often go unnoticed, pose a serious security risk due to their long-lasting private keys and the potential for misuse by former employees. The motivation section underlines the widespread issue of service account sprawl and the neglect of security measures, despite the awareness of these risks. The problem statement articulates the research's focus on securing service accounts through dynamic key rotation to prevent security breaches and insider threats. The research questions and objectives are outlined, emphasizing the need to assess the security posture of service accounts, develop a key rotation process, and ensure key integrity. Finally, the limitations of the research are acknowledged, including the challenges of gathering data on internal security threats and the scope of the study, which primarily relies on available resources and interviews.

2 Background

2.1 Google Cloud Platform And Service accounts

Cloud Identity and Access Management(IAM) is used to manage access to diverse resources; it does so by defining identities and assigning responsibilities to the resources accessible. For example, compute Engine VM instances, Google Kubernetes Engine [15], Storage buckets [16], and the organizations, projects, and folders used for resource organization are all Google Cloud resources.

Users are not provided direct access to any resource under IAM; instead, permissions are first divided into roles. These roles are subsequently assigned to the members who have already been authenticated. In the IAM, policies are used to define and enforce the responsibilities assigned to members, and subsequently, these policies are applied to resources. If a member who has already been authenticated tries to access a resource, the IAM will review the linked policy to see if the user should be granted access.

2.2 Service Accounts In Cloud

Google Cloud Platforms(GCP) has service accounts similar to many other cloud providers. These distinct accounts provide access to one or more Google Cloud APIs [17]. They differ from individual accounts in that they are used to provide access to one or more Google Cloud APIs. A service account is an identifier that distinguishes apps operating on our VM instances from other Google Cloud services. A custom-written application that reads and writes files to Cloud Storage and requires authentication to the Cloud Storage API to execute its functions is an example of service account usage [18]. Authentication operation can be accomplished by creating a service account and granting it Cloud Storage rights. Then, the application must be changed to transmit the service account details to the API. This enables seamless API authentication without storing the credentials in the code or instance [19].

If the user's service accounts have the necessary IAM permissions, those service accounts can create and manage instances and other resources. However, service accounts can modify or delete resources only if the user grants the necessary IAM permissions to the service account at the project or resource level. Users can also change the service account associated with an instance [20]. For example, an instance can have only one service account, and the service account must be created in the same project.

Compute Engine instances can use one of two service account types:

- User-managed service accounts
- Google-managed service accounts

2.2.1 User-Managed Service Accounts

User-managed service accounts include new service accounts [21] that users explicitly create and the Compute Engine default service account.

2.2.1.1 New Service Accounts

Users can create and manage their service accounts using Cloud Identity and Access Management. After creating an account, grant the IAM roles and set up instances to run as the service account. Apps running on instances enabled with the service account can use the account's credentials to make requests to other Google APIs [21].

2.2.1.2 Compute Engine Default Service Account

New projects come with the Compute Engine default service account, identifiable using this Email:

```
[PROJECT_NUMBER]-compute@developer.gserviceaccount.com
```

Google creates the Compute Engine default service account and automatically adds it to the user project, but the account is completely under the user's control. The Cloud IAM project editor role is used to create the Compute Engine default service account. However, users can modify the service account's roles to securely limit which Google APIs can access. In addition, users can delete this service account from their project, which might cause applications that depend on their credentials to fail. However, if the user accidentally deletes the Compute Engine default service account, they can recover it within 30 days.

To summarize, the Compute Engine default service account has the following attributes:

- Automatically created by the Google Cloud Console project and has an auto-generated name and email address.
- Automatically added to user's project with the Cloud IAM project editor role.

- Enabled all instances created by the gcloud command-line tool and the Cloud Console by default. Users can override this by specifying another service account or explicitly disabling service accounts when creating the instance.

2.2.2 Google-Managed Service Accounts

Google creates and manages these service accounts, automatically allocated to a user's project. Each of these accounts represents a distinct Google service, and each has access to the user's Google Cloud project to some extent.

2.2.2.1 Google APIs Service Account

Aside from the default service account, all Compute Engine-enabled projects have a Google APIs service account, which the email address can identify:

```
[PROJECT_NUMBER]@cloudservices.gserviceaccount.com
```

This service account is intended to perform internal Google processes on behalf of the user. The account is held by Google and is not displayed in Cloud Console's Service Accounts section. However, the project editor role is granted to the account by default and displayed in the IAM section of Cloud Console. When the project is deleted, this service account is also deactivated. On the other hand, users can change the responsibilities assigned to this account, including canceling all access to the user's project.

Certain resources rely on google managed service accounts and their default editor permissions. For example, cloud-managed instance groups and autoscaling require this account's credentials to create, destroy, and manage instances. However, assume that the user revokes or adjusts the service account's rights to no longer allow the user to create instances. In that circumstance, managed instance groups and autoscaling will cease to function.

The user should not modify this service account's roles for the above reasons.

2.2.2.2 Compute Engine System Service Account

Every project that uses the Compute Engine API has a Compute Engine System service account, as represented below:

```
service-[PROJECT_NUMBER]@compute-system.iam.gserviceaccount.com
```

This service account is intended for Compute Engine to execute service on the user's project. The role is based on the Service Agent IAM Policy that users have been granted on their Google Cloud Project. Compute Engine uses this service account to access the customer-owned service account on VM instances. Although Google controls this account, it is unique to the user's project and found in the Cloud Console's Service Accounts and IAM sections. In addition, the compute.serviceAgent role is automatically granted to the account on the user's project by default.

This service account is only deactivated when the user's project is deleted. Users can change the responsibilities assigned to this account and revoke the account's access to the user's project. Compute Engine cannot access the identities of users' service accounts on users' VMs if the rights for this service account are revoked or changed, and this can cause applications running inside users' VMs to go down.

When a user configures an instance to run as a service account, the IAM roles that the user authorizes to the service account determine the service account's level of access. If the service account does not have any IAM roles, it will not use any API calls on that instance.

Furthermore, the default OAuth scopes for requests performed through the gcloud tool and client libraries are determined by the instance's access scopes. As a result, when using OAuth to authenticate, access scopes could potentially restrict access to API operations even more. However, they do not apply to other authentication protocols like gRPC [22].

Setting the complete cloud-platform access scope on the instance is the ideal strategy, followed by using IAM roles to safely limit the service account's access.

Essentially:

- IAM limits API access based on the IAM roles assigned to the service account [21].
- When using OAuth to authenticate, access scopes may be used to restrict access to API functions further.

Below are detailed descriptions of both access scopes and IAM roles.

Users can choose from many access scopes, but users can also set the `cloud-platform` access scope, which is an OAuth scope for all Google Cloud services, and then securely limit the service account's access by granting it IAM roles.

```
https://www.googleapis.com/auth/cloud-platform
```

For example, if the user enabled the `cloud-platform` access scope on an instance and then granted the following predefined IAM roles [21]:

- `roles/compute.instanceAdmin.v1`
- `roles/storage.objectViewer`
- `roles/compute.networkAdmin`

Then the service account has only the permissions included in those three IAM roles. Therefore, despite the Google Cloud access scope, that account cannot perform actions outside these roles.

The user gives the instance a more restrictive scope, such as the Cloud Storage read-only scope, and gives the service account the roles/storage.ObjectAdmin administrator role requests from the gcloud tool and client libraries will not manage Cloud Storage objects from that instance by default, even if the user gave the service account the roles/storage.ObjectAdmin role. This is because the read-only scope of Cloud Storage prevents the instance from manipulating Cloud Storage data.

2.3 IAM Roles

Users must grant the appropriate IAM roles to a service account to allow that service account access to relevant API methods.

For example, users can grant a service account the IAM roles for managing Cloud Storage objects, Cloud Storage buckets, or both, limiting the account to the permissions granted by those roles.

IAM roles are account-specific. That means after the user grants an IAM role to a service account, any instance running as that service account can use that role. Also, keep in mind that:

2.3.1 Service Account Hierarchy

If there is no predefined IAM role for the access level user wants, the user can grant one of the primitive roles, such as project editor, or create and grant custom roles.
While the IAM roles assigned to a service account determine its access level, the access scopes of an instance determine the default OAuth scopes for requests performed using the gcloud tool

and client libraries on the instance. As a result, when using OAuth to authenticate, access scopes may limit access to API operations even more.

These service accounts are associated with keys used for authentication with the cloud. When these keys do not expire and are stored on a person's system, they pose insider threats. These scenarios occur when a person leaves the organization and still has the keys on their system and can still be used to access the cloud services by the user. This can lead to unintentional or malicious attacks on the services resulting in the loss of confidential data.

Another point is that GCP APIs are publicly accessible, so it becomes even more important to secure the service accounts by putting proper measures. A solution is to rotate the keys periodically or attach some expiry date. This can limit the possibility of keys being used maliciously or leaked. Though key rotation seems very simple in theory, its implementation while keeping flexibility and user's ease of use in mind is not an easy task to achieve. The authorThe author proposed a way to achieve the same below in the solutions section of our research.

Service accounts are used- As we saw, service accounts are certain kinds of accounts used to depict a non-human user, which then undergoes authorization and authentication to access data in Google APIs. Typical use cases of service accounts are to run workloads on Virtual Machines, run workloads on workstations or data centers that are on-premises and that call Google APIs, and run workloads that are not particularly bound to any human user's lifecycle. Some of the examples where service accounts are used can be described below:

- Web app that accesses GCP resources- Suppose our users are hitting a web app authorized to use the IAP (Identity Aware Proxy) of Cloud [23]. Here they do not need access to any GCP resources, but they only need access to the app that uses the resources by GCP. This web app uses a service account for accessing the services. In this scenario, we create a service account in the project hosting the app, give it the permissions it needs, and then configure the app to use the service account credentials.

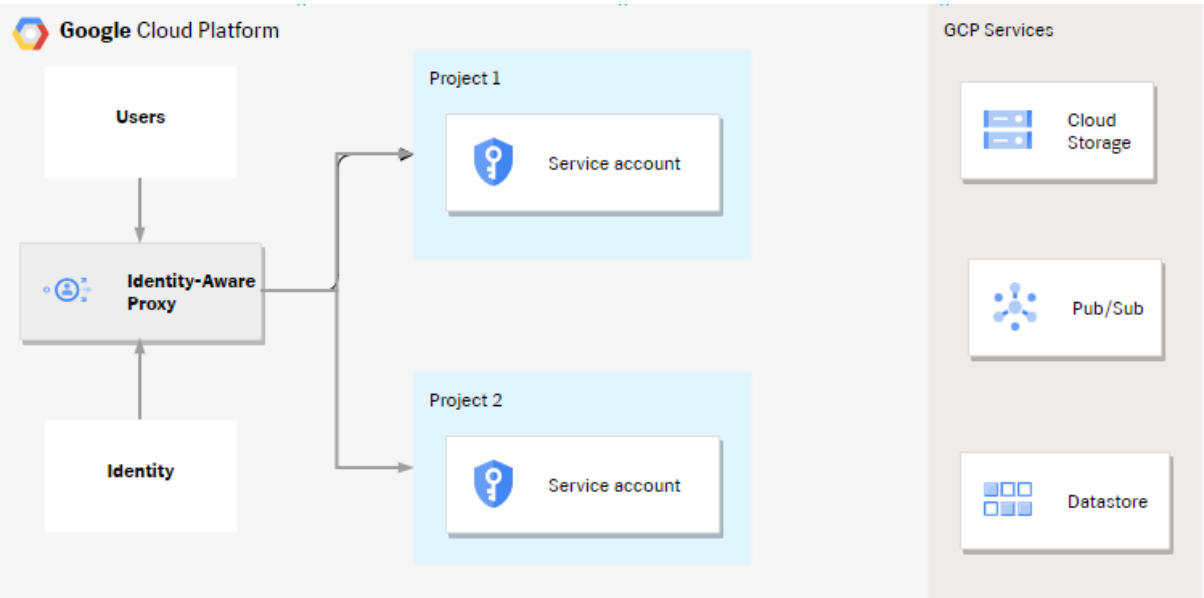

Figure 1 - Application accessing GCP resources [24]

Big query usage mapping to different DCs (Domain Controllers)- In such a scenario, users from departments fire queries to the shared dataset, as the queries must be cross-charged. The application uses a Virtual Machine with a service account with permission to query the dataset.

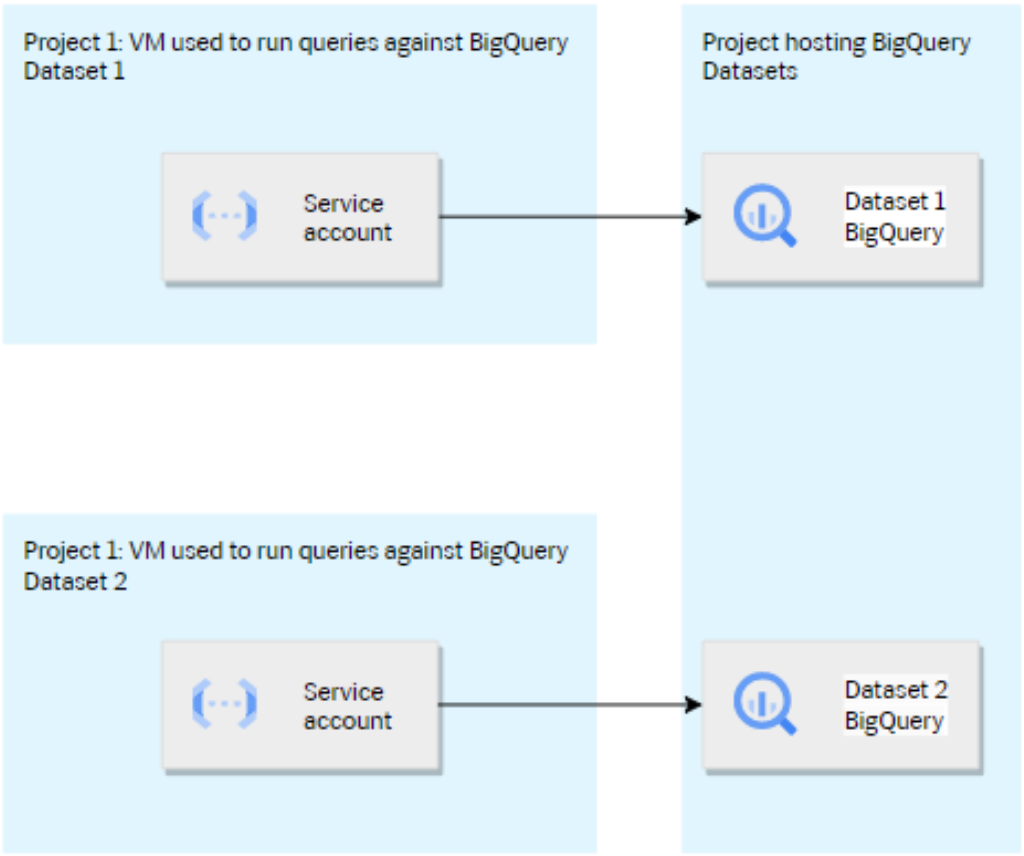

Figure 2 - Big Query usage to different cost centers with cross charging [24]

Service accounts for operations and admin activities- A system administrator or operator who manages operations like resource provisioning or auditing in a central manner across the whole GCP environment. The user will require several service accounts with suitable permissions to carry out multiple tasks. According to the hierarchy, these accounts will have privileges and permissions to complete various tasks and follow the permission level. While using service accounts, care should be taken to prevent malicious attacks.

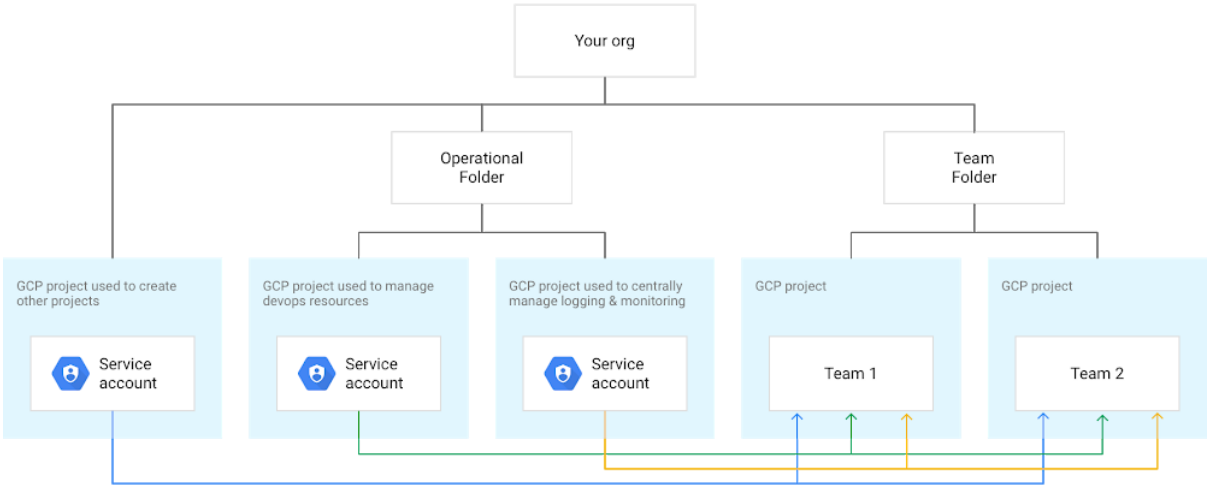

Figure 3 - Management of service accounts used for admin and operations [24]

2.3.2 How Service Accounts Are Created In GCP

Service accounts in Google Cloud are created and managed using the console of the Google Cloud, Cloud IAM or Identity and Access Management API, and the gCloud(Google Cloud) CLI tool. Whenever a new Cloud project is created, Google Cloud automatically has one service account for Compute Engine and one for the App Engine. Therefore, to control the access to the resources, we can have 98 additional service accounts in our Google Cloud project apart from the above-mentioned service accounts.

Permissions required for management of service accounts- To allow a user to manage service accounts, one of the following roles needs to be granted:

- Service Account User (roles/iam.serviceAccountUser): This role grants anyone using it the authorization to obtain, list, or impersonate a service account.
- Service Account Admin (roles/iam.serviceAccountAdmin): Like any admin user, this role has Service Account User permissions and gives authority to create, update, remove, and set or get the service account's Cloud IAM.

We can also use primitive roles in Cloud IAM to manage service accounts. However, the already defined roles are suggested to prevent unwanted access to other resources in the Google Cloud.

Creating a service account is similar to adding members to a project. However, unlike projects, service accounts belong to applications and not individual end-users. Here for demonstration of service account creation, the authorthe author used sa-name as the name of the service account we provide. This is unique and will also appear in the email address attached to the service account. It can update service accounts with other APIs and remain unchanged after creation.

Other required values are:

- The service account's sa-description is an optional description.
- sa-display-name is a non-formal name for the service account.
- Project-id is the ID of the user's GC project.

  To enable a user to create a service account, the user must have at least the role of Service Account admin or Editor primitive. Following are the steps for creating a service account using the console-
- Navigate to the page where the service accounts are in the Cloud console.
- Select a project and click open
- Select Create Service Account
- Put the service account name, an optional description, and the select role we want to give to the service account, and then save.

  We can also use the gcloud command to create a service account as below:

```
gcloud iam service-accounts create sa-name \
--description=”sa-description” \
--display-name=”sa-display-name”
```

After creation, the service account needs to be assigned one or more roles.

2.4 Service Account Security Threat

A private key is generated by creating a service account, which is forever stored. Users can access data in the cloud API using the service account and the private key. As this private key is not meant to be expired, and there is no system in place for the process of key rotation as well, there will be issues when the user's role changes or the user leaves the organization. Due to the non-expiring nature of the service account key, there is a risk of compromising the confidentiality, service, and integrity of the data and resources within the cloud environment. Usually, the key pairs are configured to expire after ten years; however, the formal employee will have the private key available, which can be used to authenticate to the cloud environment using the private key. This scenario is classified as an Insider threat. It requires a prevention policy either by designing the prevention method or policy implementation document with best practices for handling the user-managed service account.

3 Literature Review

Cloud computing is gaining momentum, making its presence felt in every industry nowadays. Organizations are more inclined to the cloud provide services than ever. It changes the way organizations have been radically handling their resources. Although various security threats are associated with cloud infrastructure [25], this thesis contributes to the security threat associated with a service account and how organizations handle the key rotation process, which could compromise CIA traits. Thus, the literature review discusses the finding within those areas.

3.1 Databases

The literature search was conducted mostly through Google Scholar and Lulea University of Technology databases. For example, web of Science, IEEE, Mendeley, Scholarly, and ScienceDirect were all used for the search. Most of the time, peer-reviewed, highly cited journals, books, and conference articles are prioritized. Furthermore, certain white papers were studied to understand better current industry practices in Cloud computing and cyber security.

3.2 Past Studies On Similar Topics

”Insider threat detection: Where and how data science applies” [26], Derek Lin asserts that Human user accounts and service accounts behave differently. Knowing the account's nature aids teams in developing more accurate statistical indicators. For example, a common anomaly detection signal is whether an account has accessed an asset for the first time. However, linking a service account to new assets for software upgrades is not uncommon. This indicator will cause a high percentage of false positives if it is not used in the context of the account type. It is not unexpected that just part of the service accounts is tracked and known in large IT infrastructures. The analysis aims to mine the data for unknown service accounts. For example, one way to investigate the textual data in Active Directory (AD) is by looking for more accounts with account features similar to those described in the AD's key-value attribute descriptions and those in the known service accounts. Another way to classify accounts is based on behavioral cues. Service accounts are more likely to generate a big volume of events than human user accounts, have regular activities or are active throughout the day, etc.

”Key Rotation for Authenticated Encryption.‘‘ [27] Systems utilize authenticated encryption (AE) algorithms to safeguard data while it is being stored cryptographically. These schemes ensure high message secrecy as well as ciphertext integrity. The latter allows active attackers manipulating ciphertexts to be detected. In addition, when data is held for an extended period, systems must allow key rotation, which involves shifting encrypted data from an old key to a new one. In some cases, key rotation is required by law, such as the payment card industry data security standard (PCI DSS) [28], which specifies how credit card data must be protected. Key rotation can also be used to disable data access and revoke previously compromised keys. However, the level of security given by this commonly used AE-hybrid technique has never been evaluated, much less formalized in a security model based on real-world security concerns. Furthermore, whether AE-hybrid rotates keys is debatable because the DEM(Data Encapsulation Mechanism) key remains unchanged. One of the main justifications for implementing such a method in the first place was to provide security, yet it is unclear what security is supplied if significant compromises occur. On the other hand, the technique is quick and only requires a little data transmission between the client and the data store, and it looks to fit current regulatory standards.

‘‘Non-human Account Management. ” [29] the author highlights vulnerability mitigation: Many organizations are concerned about service accounts because they are frequently created with a static password that any system administrator can read if it is not encrypted. A hostile actor can then use these accounts interactively and possibly for lateral movement to other systems inside the business. Service accounts can be protected by incorporating data loss prevention measures, such as authentication monitoring for abnormalities. However, migration static service accounts to APIs, which often impose a stringent security and monitoring regime, is a better practice.

‘‘Service account keys as secrets” [30] GKE workloads could be authenticated to Google Cloud APIs using one of two methods: storing service account keys as Kubernetes secrets [31] or utilizing the ‘’node’s IAM service account. In terms of management and security, both of these techniques have shortcomings. A Cloud IAM service account, an identity that an application can use to call Google APIs, can be used to make a Google API request. A user might create individual IAM service accounts for each application as an application developer, then download and save the keys as a Kubernetes secret that users manually rotate. Not only is this time-consuming, but service account keys only last ten years (or until you manually rotate

them). An unaccounted-for key could give an attacker extended access in case of a breach or compromise. Using service account keys as secrets is less than optimal for authenticating GKE workloads due to this potential blind spot and the management cost of key inventory and rotation.

‘‘A New Approach to Constructing Decentralized Identifier for Secure and Flexible Key Rotation” [32] , the authors highlight issues associated with key rotation in cloud-hosted blockchain technology. The blockchain platform provides a new root-of-trust feature for entity identification and access control, which multiple players run. Each entity creates and registers its unique identification and credential (public key) on the blockchain, allowing any entity to get the public key of any other entity. When the corresponding private key is compromised, a key rotation should be conducted to generate and register a new key pair. However, the current method for cryptographically linking a decentralized identifier to a public key introduces a severe security flaw that leads to identity theft and many IDs for the same entity. However, the method provided is dedicated to blockchain technology but drives the same concept for implementing a similar technique for cloud service account key rotation.

”User Blocking Considered Harmful? An Attacker-controllable Side Channel to Identify Social Accounts” [33] presents a practical attack on the service accounts. The attack uses the commonly used user-blocking technique, exploiting the fact that certain pages return different web content depending on whether or not a user is barred from another user. The key insight is that an attacker-prepared account can store an attacker-controllable binary state of blocking/non-blocking concerning any arbitrary user on the same service; if the user is logged in to the service, this state can be retrieved as one-bit data using a standard cross-site timing attack when the user visits the ’ ’attacker’s website. Furthermore, we show that an attacker with a set of managed accounts can achieve total and flexible control over the data spilled over the side channel by building on this primitive. Web-based social service Accounts are becoming a more important component of the modern ’ ’web’s authentication system. Spoofing is still possible, and one method is to create an account that attempts to imitate ’ ’one’s identity; however, examining the account content will usually disclose whether it is a spoofed account. Another option is to utilize a stolen account. However, the victim user should be concerned about far more serious issues than privacy leaking in this situation.

‘‘Unified Cloud Access Control Model for Cloud Storage Broker.” [34] Multi-cloud storage mitigates the risks and obstacles of outsourcing data to the cloud, such as vendor lock-in and data protection (CSPs), by storing data across several Cloud Service Providers. Cloud Storage Broker is one of the services that provides multi-cloud storage solutions (CSB). CSB is a software-as-a-service (SaaS) cloud storage service provider that maintains the relationship between one or more cloud service providers and their customers. It offers customers value-added cloud storage services, such as identity management and data encryption, without requiring them to manage their data across several CSPs. However, multi-cloud storage architecture has various issues for CSB to overcome to securely govern buckets, passwords, and client data on the cloud. Data from various CSPs CSB is in charge of completing the joint mission by setting the cloud computing responsibility model resources in several CSPs to ensure they could not be harmed and be open to the public. However, there are no standards in the cloud. Incompatible cloud application programming and computing Each CSP’s interface (APIs) add to the system’s complexity. Managing cloud resources and access control across various CSP platforms. Cloud Storage Broker (CSB) provides value-added cloud storage services by leveraging multi-cloud storage architecture for enterprise use. However, it poses significant issues for approved CSB stakeholders in managing resources and access control across multiple Cloud Service Providers (CSPs). Following the privilege separation idea and the least privilege principle, the paper presents role-based access control for CSB stakeholders to access cloud resources by providing necessary rights and an access control list for cloud resources and CSB stakeholders, respectively.

‘‘Cloud Password Manager Using Privacy-Preserved Biometrics‘‘ [35], using a password for identity verification is a standard authentication for cloud-hosted website login. Many people prefer to use a single password for all web services, which is dangerous since all web service accounts can be compromised if one password is exposed. It is inconvenient for the identity principle to remember multiple passwords for different web services. The security-convenience issue can be resolved by using a password manager to store and retrieve passwords. An identity principal only has to remember one password (called a master key), which is used for logging into a password manager. The password manager will automatically log into numerous web services. An attacker can mimic a legitimate user by using a password stolen from an online service provider. Biometrics-based authentication systems and biometric password managers have been developed to address this problem and avoid data leakage that is either inadvertent or corrupted.

3.3 Cause Of Internal Security Threat

Service account exploitation will occur when the previous employees' credentials remain valid even after the user has changed job responsibilities or left the organization. Cloud services providers face issues with access management of employees as the RSA private keys [36] are downloaded to the employees' systems and can be used later by them. These keys possess a long expiry date or key rotation and can be used even after the employees have left. Due to these keys being present on the user's local machine long after leaving the company, they can access the cloud APIs and services using them [37], which is unauthorized access to the cloud and should be prohibited. Therefore, it is important to prevent unauthorized access via these service accounts by designing the policy of configuring the expiry date and creating new keys for the service accounts over a regular interval of time.

3.4 Effect Of Compromised Service Account

Access to the APIs or services of the Cloud by past employees is comparable to access by malicious agents. Past employees can intentionally or unintentionally cause a leak of critical information, leading to financial losses and loss of reputation or an organization [38]. Furthermore, the former can decide to sell the company's critical data to third-party sources for financial gains or cause disruption to the cloud services. User credentials after leaving the organization are undesirable and can pose a serious threat. Hence the organization must implement a preventive mechanism for service account exploitation.

3.5 Proposed Solution based on literature review

The author proposes using service accounts with proper key expiry and rotation policies instead of user accounts to prevent insider threats to cloud computing services. Service accounts are different from user accounts as these are a special kind of account that does not represent any particular user or human user. Instead, these accounts are used to authenticate and authorize the cloud APIs to be accessed.

Service accounts found uses in workload running in VMs, workstations, and tasks unrelated to individual users.

Like in user accounts, when a service account is created, a private key is generated, and these keys are also downloaded to the user's local computer and stored forever. Users can access

data in the cloud API using this service account and private key. The problem arises when the user role is changed, or the user is a former employee. Since the service account key is not configured to expire and be renewed over the period, there is a potential threat that these service accounts will be used to compromise confidentiality, integrity, and availability of the information and resources within the cloud environment. To overcome this, the author proposes that unauthorized key use can be prevented by designing the prevention policy method so that expiry configuration and key rotation are in place. This will ensure that the users cannot access the services they could earlier after their role change or exit from the organization.

Another way the author has proposed to prevent Internal threats in the cloud computing environment is to use a flag or key associated with each user's account and store them somewhere. Whenever any user leaves the organization, his/her flag should be set accordingly. This method will require extra effort in storing the keys and user details and checks at attempted login. The author has examined the article's viability, advantages, and disadvantages of these solutions.

3.6 Summary of Literature review

The literature review delves into the complexities of cloud computing security, focusing on the significant issue of service account management and the associated risks to confidentiality, integrity, and availability (CIA) within cloud environments. It draws from various past studies to highlight the unique challenges posed by service accounts, which often possess long-lasting private keys and can be exploited by former employees. The review emphasizes the need for proper key rotation policies and highlights that while service accounts differ from human user accounts, they still require effective access management. The proposed solutions include implementing key expiry and rotation policies for service accounts and utilizing flags or keys associated with user accounts to prevent unauthorized access after role changes or departures from the organization. These approaches are seen as crucial for addressing insider threats in cloud computing, ultimately safeguarding critical data and resources while enhancing cloud security.

4 Research Methodology

In this chapter, we are looking at the research methodology applied in the thesis project. This chapter outlines the strategy for the research, the research method, the approach taken for conducting the research, data collection methods, ethical considerations, and the limitations of the research.

4.1 Research Environment

The research was conducted in conjunction with a company and with the aid of external overs ight from company personnel. GCP environment of the company was used to get the understanding of the cloud infrastructure, how they are used within the organization, what insider does the current implementation face and what are the challenges faced by other similar cloud hosting companies across different domains.

4.2 Research Strategy

To accomplish this, we realized that a literature study is not enough. For example, organizations currently deploy many services in the cloud platform through the CI/CD (Continuous Integration Continuous Deployment) [34] process. As a result, managing service accounts and their credentials is a tedious task for administrators. In addition, almost every organization suffers from service account sprawl, which allows their privileged account attack surface to grow unmanaged and uncontrollably. Thus, after investigating, it is obvious to get feedback from the expert panels to understand how cloud professionals and organizations control service accounts, manage them, and reduce the risk of security threats.

4.3 Research Method

After considering several research methods for gathering expert viewpoints, the authore chose the qualitative [39] and quantitative [40] research methods. The research proposal and literature review findings created the interview questionnaires. Discussing your early thoughts with the professionals to create the best learning atmosphere and interview process is critical.

Qualitative research data is deep or rich, whereas quantitative data is more efficient. In addition, qualitative data has a lesser tendency to be generalized and is more extensive, whereas quantitative data is more fit for testing hypotheses but can sometimes miss details contextually. This study uses questionnaires designed to obtain information from cloud professional participants. Before the face-to-face and online meetings, questionnaires were sent out as written interviews.

Quantitative research is objective, and it needs accurate measurements & analysis of the concepts. Examples include surveys and questionnaires. In this thesis, based on the best practices determined from the literature review, findings from the SWOT analysis, and observation of how organizations have configured the cloud infrastructure, the experimental prototype is developed, which would reduce the risk associated with service accounts and the automating the key rotation process.

4.4 Data Collection And Tools

To collect data for the research, we referred to multiple sources instead of depending on a single source to improve the reliability of our research. First, we referred to the past research conducted on cloud computing and the security issues that plague it. We also saw the documents and papers written on the Google Cloud Platform and its official documentation. These documents give the researcher an idea about the security mechanisms from the providers' point of view.

We conducted sessions with participating organizations using cloud services that have either faced internal security threats in the past or braced themselves by having proper defense mechanisms to counter the same. In addition, many employees of the organizations were also interviewed, with the organization's knowledge, regarding the security loopholes and measures taken to fix them. The interview was in-depth for this research because they gave a personal view of the research topic. Furthermore, in-depth interviews uncover the participating member's views and opinions on the individual research topic. Also, these interviews are personal and often offer a different perspective regarding the subject. The participants were selected based on their familiarity with cloud computing, with a preference for familiarity with the Google Cloud Platform.

Questionaries:

1. What is your role in the organization?

2. How long have you been employed by the company and in your present position?
3. Do you use Google Cloud computing services to fulfilling your business needs? What are the business areas where you use Cloud computing services?
4. Do you have a proper framework in place for handling Insider Threats from the organization's point of view?
5. Are your team and you aware of the security concerns relating to the GCP Service accounts?
6. Have you ever faced incidents in your organization related to service account compromised?
7. If yes, what measures were taken by you to tackle them?
8. How do you test the security of your organization or the cloud services that are being used and accessed by service accounts?
9. How often service account keys are rotated and renewed?
10. What improvements, in your opinion, should be made to the present security system in order to cope with the security challenges that arise from the use of service accounts in the business, especially Insider Threats?
11. What role does the Cloud provider play in assuring the service account and key rotation mechanism's security?
12. Do you believe that ensuring the security of service accounts and implementing key rotation processes is just the responsibility of cloud service providers, or should it be a collaborative effort between the provider and the organization?

These questionnaires were semi-structured and often served as a guiding tool for the researcher while they were had their interaction with the concerned parties. 24 cloud professionals from Architect, DevOps, SecOps, and SRE (Site Reliability Engineer) backgrounds were selected. Out of which 18 responded, the questionnaire was shared with them during the interview process via face2face, MS Teams, and Zoom interviews. Response from the participants is documented in the word document tool due to the flexibility of organizing and sharing the information.

4.5 Ethical Considerations

This study has been subjected to some ethical issues. To address these issues, all the participant organizations had provided written consent regarding their involvement in the research by providing a signed Consent and Briefing document. In addition, other participating members

were also requested to give a signed Debriefing and withdrawal letter. These letters provided assurance that the organizations and members had agreed to participate in the study.

Another point is that all the participating members were given complete information about the study's objectives. Additionally, they received assurances that the information they provided would be kept private and that the research would only be used for academic purposes. The participants were not pressurized for their participation, nor were they harmed either verbally or physically during the entire course of the research. Organizations were approached cordially for their participation, and no pressure was created on them to disperse information that they were not entitled to officially. Official channels were used to communicate with the organizations, and no unfair means or channels were used to get the information regarding the research. All the conditions were checked to maintain a calm and professional environment with the organizations or individual participant members.

4.6 Summary of Research Methodology

The research methodology chapter outlines the approach used to investigate the security challenges related to service accounts in cloud computing environments. The research strategy combines both qualitative and quantitative methods, with a focus on understanding the experiences and practices of cloud professionals and organizations in dealing with service account security. Data collection involved a multi-faceted approach, including a review of past research, official documentation, and in-depth interviews with cloud professionals from various organizational roles. Ethical considerations were addressed through informed consent and assurances of data privacy, with participants willingly sharing their insights and experiences. This comprehensive research methodology enabled the collection of valuable data and insights into the complex realm of service account security and key rotation in cloud computing environments.

5 Research Result

The following section presents the research results as the first content and SWOT analysis based on the qualitative research analysis, followed by the experimental prototype for performing the key rotation technique for service accounts. The final section also includes the result obtained by running the code snippet in the google cloud lab environment.

5.1 Content Analysis

In this research, content analysis has been utilized to analyze the data gathered from the interviews. As Moore and McCabe [41] have stated, the data is arranged in themes and sub-themes in the content analysis approach. This arrangement makes the data to be comparable. The prominent feature of content analysis that gives it an edge over other methods is simplifying the collected data in a reduced format. This data reduction benefits the researcher from being measured using quantitative methods.

In this research, we used the purposive sampling method, where we selected the samples as a mix from different organizations that services from different cloud providers [42] . Another thing that was kept in mind to have a varied sample of data was to study organizations with different focuses on their security, such as organizations that need a high security to those that do not have rigorous security needs. Therefore, the variety in the data samples was introduced with the help of choosing various questions in the survey conducted that had been forwarded to various organizations.

Apart from these benefits, content analysis also gives the researchers the ability to organize the data in a structured way to achieve the research objectives. Thus, qualitative data can also be utilized in this manner. However, the disadvantage of using content analysis for the detailed analysis of the collected data is that it is prone to human errors. As the researcher can and they do misinterpret the gathered data, the objectives gained or conclusions drawn can be unreliable or false.

The following was identified directly through the interview:

Organization Unit	Defined pillars	Action needed

Cloud Architect	Security best practices, the implementation phase, and integration with the external database.	Zero trust architecture is the mechanism to update the service account credentials from the external source.
DevOps Engineer	Dynamic renewing of the credential of the service account.	RBAC, MFA, password policy for newly issued credentials.
SRE Engineer	Inventory of the service account of each team and associated keys. On-demand renewal of the key based on service accessibility.	Scheduler to execute the script for service account key rotation.
Cloud Engineer	Service account privileges are managed through RBAC configuration. Different service accounts are created for each cloud environment, such as dev, test, QA, and prod.	IaC (Infrastructure as a Code) for configuring the RBAC permission and maintaining each script for each environment.
Release Engineer	Non-interactive login of service accounts for quick fixes in the prod environment. Audit logging and automated script for renewal of service account.	Security monitoring of service account activity and behavior. On-demand of periodic key rotation of the service account.
SOC Analyst	Particularly for the service account, we are keeping a record of the purpose of the service account and its details. This information is locked down, which protect from getting into attacker or unauthorized user.	24/7 security monitoring and building alerts for any suspicious activity. Access to the security analyst to restrict the further use of the service account.

Table 1 Qualitative content analysis

It was identified that among the respondents are Site Reliability Engineer, DevOps Engineer, Site Cloud Solution Architect, Solution Architect, Senior Architect, Senior DevOps Engineer, Cloud Engineer, SecOps Engineer, SRE Engineer, Cloud Infrastructure Architect, and Senior DevOps Engineer. It was found that most respondents have five or more years of experience, while the rest have less than five years of experience. It was found from the interview that most respondents said that they use GCP services, while others said that they use GCP services occasionally for a few assignments but not on a full scale.

During the interviews, it was identified that all of the respondents are aware of the security issues often associated with Service Accounts. In addition, almost all the respondents have dedicated teams who monitor the service accounts for any vulnerability.

During the interview, respondents shared various ways they implement security measure, which is as follows:

- Multifactor Authentication (MFA)
- Splunk SIEMs tool
- Role-based Access Control (RBAC)
- Single Sign-on (SSO)
- Monitoring Audit logs
- GPOs in places
- Intrusion Prevention Systems (IPS)
- Intrusion Detection Systems (IDS)
- Granular access management
- G-suit access management
- Web Traffic Filtering
- Pattern-matching Single-log (non-SIEM)

All the respondents mentioned that they do not have any dedicated framework but have dedicated teams who monitor for any security breaches. However, one respondent said that they are working on Zero trust architecture.

Ten respondents said they had not witnessed any insider attacks, while six said they had witnessed some insider attacks in their organization.

The respondent said that they change the g-suite admin password regularly when an admin employee leaves the company or team, change their passwords frequently, threat intelligence gathering and act based on the defined SOPs (Standard Operating Procedures), Create Alert and inform the Infosec team, rely on automation of process and procedures, report to companies phishing mailbox.

During the interview, all the respondents indicated that they conducted an Exit interview and procedure to terminate access as the primary measure to handle insider threats. Apart from that, the following were mentioned by multiple respondents:

- Pre-access general security-awareness training
- Pre-access role-based security training
- Change management (CM)- ITSM tool
- Periodic and consistent review of access

- Separation of duties and least privilege policies

Monthly general security awareness sessions on current topics or threats

The majority of the respondents identified the following:

- Role-Based Access Control (RBAC) - Google IAM service
- Organization Single-sign-on
- 2-factor authentication
- SecOps team is sealed down with locked entries with restricted access to the premises to secure the assets and information
- Office Infrastructure is equipped with physical control
- While one respondent said that they have no physical controls implemented currently.

The majority of the respondents identified the following:

- Enforcing RBAC
- Creating automated or web-based tools instead of direct administrative access
- Enforcing vital education and background requirements, strict access control and monitoring, an incident response plan covering insider threat, exit interviews, the procedure to terminate access, and periodic and consistent access review.

All respondents indicated that they had dedicated teams to test their organization's security, which is done at regular intervals. If any loophole is identified, it is fixed on a priority basis.

5.2 SWOT Analysis On Company

SWOT [43] is an acronym for strengths, weaknesses, opportunities, and threats related to Company AB (China Euro Vehicle Technology) organization, as most of the participants for the interview belonged to Company. Due to the service account being an internal component of the cloud architecture, the research focused on weaknesses throughout the SWOT analysis. Finding these can assist in locating potential improvement areas. By doing this, businesses may create strategies to address and manage their weak points.

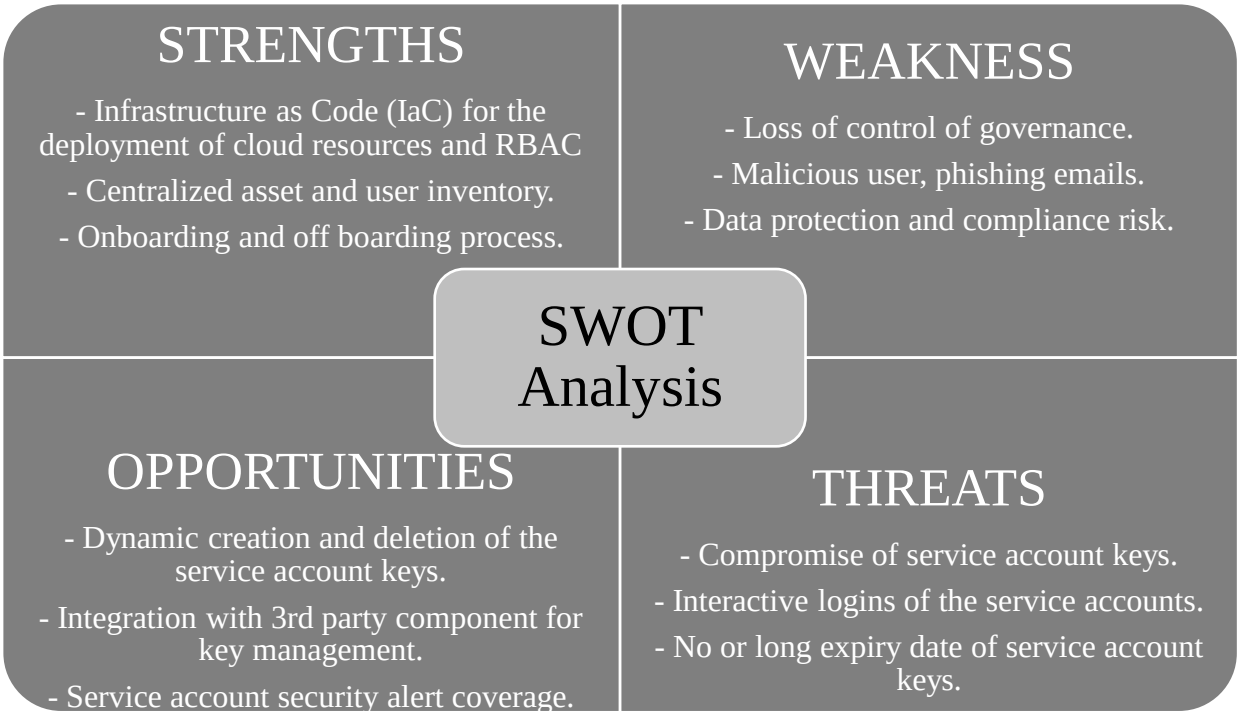

Table 2 Company SWOT Analysis

5.2.1 Weaknesses In Company

1. *The loss of control of governance – Managing roles and permission of service account (Review)*

As Cloud and DevOps engineers mentioned, the lack of adapting a standard framework or process that reviews the roles and permission of the service account leads to a lack of governance to manage the service accounts. The client, contracting a Cloud Computing service, provides part of the infrastructure governance. Hence, there shall be an automated process to handle central service-account permissions and need regular review and essential rotation techniques.

2. *IT true to the supplier – IAM service (availability)*

Based on the response of Cloud providers ensuring the security of the Cloud services, there shall be an agreement between the cloud provider and the customers to ensure an appropriate mechanism for the availability of the IAM service. The service level agreement (SLA) must be essential in this situation to protect the client's interests. SLA shall incorporate legal entitlement for service disruptions, insider threats, and data security.

3. *Isolation of environments and data – Right service accounts assigned to respective projects.*

As observed from the interview with Cloud Architect, sharing resources is one of the essential characteristics of cloud computing.

Several clients can, for example, share the same physical server. If the separation of the environment is not effective enough, invasions between clients could occur.

In the case of an environment shared between several tenant customers, two kinds of attacks are possible; the first of the Guest-hopping type and the second against direct hypervisors is lying. Therefore, different service accounts shall be used for different projects and customers from the security of the service-account perspective.

4. *Compliance risks – Service account management based on the location of service*

From the discussion, we could observe that the cloud platform is used across domains such as Automotive, finance, telecom, etc. However, compliance with data privacy laws and regulatory standards such as PCI DSS and ISO 27001 can become very complicated by outsourcing certain core services and processes.

Service providers may impose restrictions on conducting an audit of their infrastructure based on the geographical location of the service and data center operation.

5. *Data protection – RBAC*

From the interview with the SecOps engineer, it was observed that RBAC is part of the automation process to ensure who has access to view the permission of the service account. This will enable the correct service account to be used to access the data within the cloud platform. For cloud computing service customers, data protection is challenging. It is challenging to secure data that is spread across multiple locations. Making sure that the data is processed correctly is also complicated because the control over transferred data is beyond the reach of its owner.

6. *Dangerous or incomplete deletion of data – Employee contract termination.*

Almost all the interview responses had exit interviews and audit logs of the former employee monitored for a limited amount of time for behavior analysis. One of the interviews mentioned that unknown service accounts were identified with escalated permissions not belonging to any service in the cloud. This leaves an option to have an automatic un-provisioning of the service accounts when not in use. In the past, securely deleting data has been a challenging problem that required creating a number of procedures to guarantee that the data was completely gone. Additionally, Cloud Computing makes extensive use of the reuse of hardware resources. For

instance, a new client may be given access to a storage area that previously housed data belonging to a different client. If the old data has not been completely destroyed, there may be a danger of loss of confidentiality as a result.

7. Malicious users: 2- factor authentication

During the interview, it was observed that not all organizations had adapted 2-factor authentication. Cloud computing needs high-level user profiles for its administration, and it is recommended to have multifactor authentication in place for such logins. A system administrator will have full privileges on different resources from different clients. A malicious user who successfully compromises system security and enters an admin session Administrator will gain access to any customer information. The malicious user can abuse the service account permissions and privileges if this goes unidentified or undetected.

The risks associated with data security in the cloud do not fall outside the scope of internal risks formed globally, but they present vulnerabilities and must be considered. When considering data security. These risks include phishing, privileged access to the cloud, and the source or origin of the data itself.

8. Phishing Email requesting access to a cloud platform or service account

As mentioned by Senior DevOps Engineer, they are often common across phishing emails requesting login details as a cloud provider and so on. One of the indirect risks to data outsourced to a cloud is phishing. Although generally considered impossible today to break the PKI public key infrastructure. It is possible to trick end users by misappropriating their credentials in the cloud. In case of such an incident, there shall be a mechanism to change the certificates of the service account. One way to minimize the impact would be to provision the credentials dynamically for the service account.

9. Cloud provider personnel with privileged access -

Another potential risk mentioned by cloud architects to a service account in the cloud relates to inappropriate access to sensitive service account credentials by cloud personnel. Whether in the cloud or not, the sub-processes can bypass the typical controls that organizations IT generally apply through physical and logical controls. This risk has two main factors: first, keys are downloaded to the user's local computer when the service accounts are created, and the privileged access cloud service provider data center personnel. The assessment of this risk involves an extensive change in the security practices and standards of the Cloud Service Provider so that this provider's staff with privileged access cannot access customer data.

Having third-party software such as VaultDB [44], cloud provider-independent, would address this issue.

10. Responsibility of Cloud provider and the service consumers

As mentioned by Cloud Architect, the cloud provider is responsible for maintaining its integrity and security for all foundational devices and services such as physical compute, storage, and network service. However, there are a few areas where the responsibility becomes collective and shared between the provider and the customer, which can be divided depending on the deployment model, such as IaaS, PaaS, and SaaS, as customers choose. For example, the SaaS deployment model is a platform wholly managed by the cloud provider. Therefore, the cloud provider is responsible for end-to-end security, including the security of back-end, front-end service, and protection against potential risks and threats.

5.3 Proposed Solution - Key Rotation Process

The following section describes the experimental steps demonstrating the service account key rotation process. An experiment is conducted in GCP (Google Cloud Platform) with the user having IAM permission roles/iam.serviceAccountAdmin. Every stage of the experimental method yields a result. Since the prototype is developed in python, it could be reused across all operating system platforms.

5.3.1 Experimentation

- Set up a separate project for shared resources.
- Create a bucket in the project, but do not make it public.
- Create an IAM group for developers that needs to download the service account keys on a daily basis.
- Grant storage.objectViewer read access to the developer group through Cloud IAM

The authorThe author created a key rotator project using python to rotate the keys for a Google Cloud Platform service account. This key rotator will work on the local machine and needs to be run periodically. Here we assume that we already have a service account on GCP, and we can download the serviceAccountAdmin.json file we will use. The various steps in the rotator are as below-

i) At first, we will create a new method in our python project that will return the credentials from the serviceAccountAdmin.json file as per the below code:

```
#!/bin/python3

import json
import base64
import googleapiclient.discovery
from datetime import datetime
from pathlib import Path
from google.oauth2 import service_account

def get_json():
""" Returns absolute path for json file """
json_file = "serviceAccountAdmin.json"
mypath = Path().absolute()
file_path = (mypath / json_file)
return file_path

def credential():
""" Returns credential handle """
file_path = get_json()
print("file path", file_path)
credentials = service_account.Credentials.from_service_account_file(file_path)
print("---------credential start----------")
print(credentials)
print("---------credential end----------")
return credentials
```

Figure 4 - Return service account credentials

ii) Next, we are going to write another method that will get the credentials from the credential() method, and it will also delete the old keys for the service accounts as follows-

```
def private_key_id():
""" read private_key_id from json file """
f = open(get_json())
json_data = json.load(f)
#print("private_key_id: " + json_data['private_key_id'] )
return json_data['private_key_id']

def KeyRotate(service_account_email,project_name):
"""
Scans the keys for given service account, compares the key to the given json file
Rotate the key when the key matches.
Note that some keys are system managed key and can not be deleted
"""
credentials = credential()
service_account_email = service_account_email
iam_service = googleapiclient.discovery.build('iam', 'v1', credentials=credentials)
serviceaccounturl = 'projects/' + project_name + '/serviceAccounts/' + service_account_email
request = iam_service.projects().serviceAccounts().keys().list(name=serviceaccounturl)
listofkey = request.execute()
print("------------------Listing all keys start------------------------")
for each in listofkey['keys']:
print(each)
print("------------------Listing all keys end-----------------------")

for each in listofkey['keys']:
#print("".join(each['name']))
#print(private_key_id())
if private_key_id() in "".join(each['name']):
print("delete key: " + each['name'])
request = iam_service.projects().serviceAccounts().keys().delete(name=each['name'])
try:
request.execute()
print("Service key deleted: ", each['name'])
except Exception as e:
print(e)
print("Exception on deleting :" + each['name'])
print("Service key is managed by workload it can't be deleted")
# function call for create new service key
CreateNewGCPKey(credentials, service_account_email)
return print("")
```

Figure 5 - Delete old service account keys

iii) As the old service account keys have been deleted, we will now write a new method that will create and write into the .json file a new service account key, as below:

```
def CreateNewGCPKey(credentials, service_account_email):
""" Generates new key to given service account and dumps data to json """
service_account_email = service_account_email
iam_service = googleapiclient.discovery.build('iam', 'v1', credentials=credentials)
request = iam_service.projects().serviceAccounts().keys().create(
name='projects/-/serviceAccounts/' + service_account_email,
body={'privateKeyType': 'TYPE_GOOGLE_CREDENTIALS_FILE'})
key = request.execute()
key = base64.b64decode(key['privateKeyData'])
deckey = json.loads(key)
with open('NewGCPServiceAccountFile.json', 'w') as outfile:
json.dump(deckey, outfile)
return print("New Service account created for " + service_account_email)
```

Figure 6 - Create and write new service account keys to JSON file

iv) As this whole key rotation process is manual, we can use Scheduler or write a Scheduler in Python as below or use Windows Scheduler for tasks or by creating a .exe file from the project.

Here the author written a Scheduler in Python as below:

```
def main():
""" main """
service_account_email = "ltu-sa-key@sre-investigation.iam.gserviceaccount.com"
project_name = "sre-investigation"
print(" [%s]\n" % str(datetime.now()), '\nGCP key rotation starting...')
KeyRotate(service_account_email,project_name)
print('End.. GCP key rotation\n')

main()
schedule.every().day.at("00:00").do(main)
while True:
"""Checks whether a scheduled task
is pending to run or not """
schedule.run_pending()
time.sleep(1)
# Task scheduling
schedule.every(5).minutes.do(main)
```

Figure 7 - Scheduler for automatic service account key rotation

5.3.2 Experiment Result

The experiment results indicate that, for enhanced security, daily rotation of service account keys is essential. The "serviceAccountAdmin.json" file houses the credentials of these service accounts. The experiment results are summarized as follows:

(i) Code Execution: During the experiment, the code successfully retrieved the credentials from the "serviceAccountAdmin.json" file.

(ii) Old Credentials Deletion: The experiment demonstrated the capability to delete the outdated credentials effectively, thereby mitigating security risks.

(iii) New Credentials Creation: As part of the experiment, new credentials were generated for each service account key stored in the "serviceAccountAdmin.json" file. These new credentials were then written back into the respective JSON files.

Automation Through Scheduling: To automate this key rotation process, a scheduler was implemented. The scheduler consistently rotated the keys every day at 00:00 hours, ensuring that security measures remained up-to-date.

These experiment results affirm the feasibility and effectiveness of the key rotation mechanism in maintaining the security of service accounts within a cloud environment.

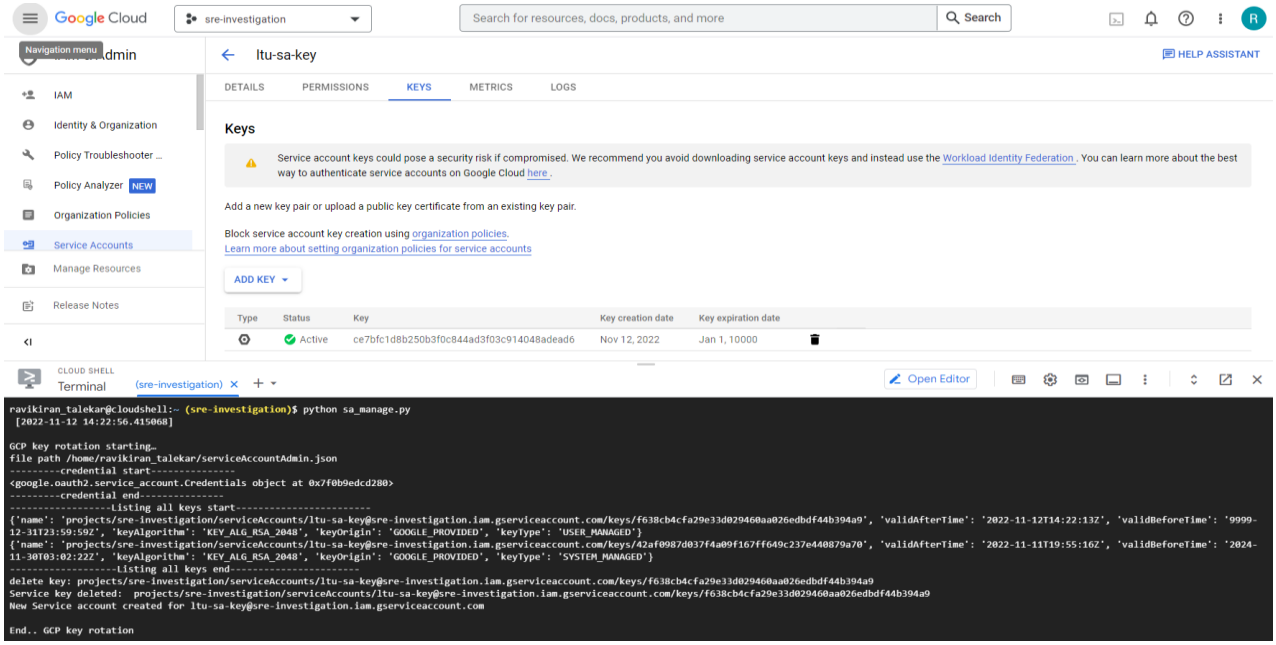

Figure 8 Result of key rotation program

5.4 Summary of Research Result

In the research results chapter, the study employs content analysis to extract valuable insights from interviews with a diverse sample of cloud professionals from various organizations. The analysis reveals a comprehensive understanding of service account management practices and security measures, such as multifactor authentication, role-based access control, and audit log monitoring. Weaknesses in cloud service providers and organizations, particularly in governance, security, and data protection, are identified through a SWOT analysis. The study emphasizes the importance of service account key rotation as an essential security measure, providing a detailed experimental process for key rotation and demonstrating its successful execution. The experiment underscores the need for daily key rotation for enhanced security. The automation of this process through scheduling ensures consistent and up-to-date security practices. Overall, the research results offer crucial insights into addressing service account security challenges in cloud environments and propose a practical solution for maintaining their integrity.

6 Conclusion And Recommendation

6.1 Contributions:

The scope of this thesis includes security considerations for the service account and recommendations for technical solutions to tackle the issues related to insider threats associated with the service account.

The main contributions of this theses are:

1. The study focuses on understanding the organization's security posture and security considerations cloud professionals take during cloud infrastructure implementation.
2. The study proposes the recommended solution for securing the service account keys from insider threats based on data collection.
3. The study increases the organization's security posture by securing the cloud platform from internal threats.
4. The study recommends the existing security requirements to tackle the issue of Insider threats due to abuse of the service accounts.

6.2 Conclusion

After an extensive review of the literature in the area of insider threat for the service account in cloud infrastructure, and surveying through a questionnaire was deployed to achieve research objectives, after which methodology of developing the manual and automatic key rotation process for the service account in the cloud infrastructure was proposed.

This research study is carried out to bridge the existing research gap in the security features of cloud computing. A thorough analysis of more than thirty research papers was done to arrive at the research gap and find solutions. We identified two sub-areas for research around the prevention of exploitation of the service account keys: manual key rotation and automated key rotation. The research has come out with some usable outcomes toward improvement/enhancement in the security features of the service account in Cloud Computing.

As a qualitative method, the interview process gave insight into the organizational view regarding the cloud security and management of the service account. For example, it was

observed that during the initial implementation state of the cloud infrastructure, the management of the service account is not taken into consideration. The problem arises as the product grows, and handling the service account and key rotation process becomes a tedious task.

Based on the research, to prevent malicious users who no longer needs access to service accounts several measures are to be considered:

First and foremost, it's crucial to manage service account keys according to best practices. This includes limiting the amount of keys and service accounts in use, rotating keys on a regular basis, and allowing only authorized workers access to keys and service accounts.

Second, you can limit access to GCP resources by using access controls and permissions. This may involve setting up audit logs to keep track of activity and using IAM policies to control which service accounts have access to which resources.

Third, when an employee leaves the company, it is advised to promptly withdraw their access to service account keys. To accomplish this, either delete the service account or rotate the key that is connected to the former employee.The key rotation of service accounts in the cloud platform is of great concern to many organizations. Here the authorthe author seen that to use service accounts in the Google Cloud Platform without compromising the security of the data. We must ensure that the keys used are regularly rotated or expired. The authorThe author explored various methods that can be used for either manual or automated key rotation for key rotation.

- *Manual Key rotation:* A method for manually rotating the service account keys. Assuming that the service account has previously been created and is active, this approach can be utilized independently.
- *Automated Key rotation:* The above method can be used with a cloud service or Windows scheduler. Kubernetes secrets also play a vital role in storing and managing the key rotation process.

6.3 Discussion

For organizations that relies on cloud services for their operations, the security of cloud infrastructure is crucial. To avoid unauthorized access, service account keys must be securely stored since they are used to access cloud resources. Despite the fact that cloud service

providers like Google Cloud Platform (GCP) provide key management services, it is still required to employ external solutions for key rotation and keep an eye on how they are being used.Google Cloud Platform offers a number of services, including Cloud Functions, Application Default Credentials, and Key Management Service (KMS), all of which can be used for key rotation. Despite the fact that these services are helpful, an outside key rotation solution is necessary for a number of reasons:

Vendor lock-in can happen if you only use Google's services for key rotation. This implies that you might have to start again with your key rotation policy if you ever decide to move your infrastructure to a different cloud provider. You may make sure that your key rotation strategy is independent of any specific cloud provider by employing an external solution.

Customization: Google's services may not be sufficiently configurable for certain use cases because they are meant to be general-purpose. It is possible to customize external solutions to fit certain business needs and integrate them with already-existing infrastructure.

Compliance: For key management and rotation, several sectors are subject to severe regulatory compliance standards. In order to satisfy these criteria, external solutions might offer extra features like audit logging, access control, and compliance reporting.

Flexibility: External solutions give the key rotation procedure additional latitude and control. When working with complicated infrastructure, various cloud providers, or hybrid cloud setups, this can be crucial.It's crucial to keep track of the external service account key rotation because it makes sure everything is going according to plan. Without monitoring, the security of cloud resources may be jeopardized by unauthorized changes or suspicious activities. Audit logs, which capture key rotation events and other service account activities, can be used for monitoring. Security teams can be informed of any suspicious behavior or unsuccessful key rotation attempts by real-time monitoring, which can be set up. Key rotation policies can also be kept current with industry best practices and successful by undergoing regular review.

6.4 Recommendation:

Based on our research study and its conclusions, Here, we offer several suggestions that could be crucial in enhancing security and broadening the use of this technology that will change everything, as follows:

- Implement our proposed prevention algorithm against DDoS to improve/enhance network security.
- There are many efforts required by the GCP Service Providers, different Industries, and researchers to increase awareness and talk about the advantages of cloud computing technology to the consumers by conducting in-house training programs, seminars, and workshops.
- An organization needs to know what level of security GCP Service Provider offers. Also, it is required for the consumers to inculcate a culture of security consciousness. Therefore, the security features must be spelled out at the qualitative requirement stage before buying Google's services. In other words, cloud security is not an afterthought.
- There is a huge requirement on Google as a Cloud service provider to engage in and invest in finding research-based solutions to the quality and security of their service offerings to ensure the authentication, integrity, and confidentiality of data and communications.
- It is also considered appropriate for Cloud Service Providers like GCP to maintain a third-party authentication process for stronger authentication and authorization. Additionally, GCP should define the limit of services in the Service Level Agreement (SLA) to the user, which may be the basis of hours in a day, such as 6 hours, 12 hours, or 24 hours and maintained accordingly.
- It is advised from long-term experience that CSPs should stay focused on best practices for strict network policies, IDS, IPS, Firewall, Strong Authentication and Authorization, and strong encryption techniques at various levels such as individual users, organizations, and GCP levels.

6.5 Future Directions

Adopting cloud computing is imminent, unavoidable, and un-ignorable due to its sheer cost advantage to running any business enterprise. It is the cheapest way to achieve the virtual availability of all employees, system resources, and computing power. This thesis provides the basic research work needed to implement our proposed algorithms in the field of security of service accounts in cloud infrastructure. Implementing our proposed algorithm and current tools and techniques would be cost-effective and secure solutions to the problems of the cloud network. This research work would also act as a beckon for directing future research that may require renewed concentration on public cloud security threats to win organizations' trust to

migrate their business into the cloud. Our interview results could also be used in the future by the industry to enhance adaptation, propagate awareness, and thus improve cloud computing security.

The presented research work could be extended to explore more industries, and research could be undertaken to create a dynamic key rotation for the service account. It is envisaged that future research in this area would also include field testing of the solutions proposed, and a comparative analysis of various solutions could be done through testing and simulation on the existing cloud facilities, which the research could not achieve due to the non-availability of the IT resources and inadequate human resource and funding. Future research projects in this direction on a higher scale would enable us to reach solutions that would benefit the organizations immensely in terms of reduced cost of implementing and maintaining the security of service accounts in cloud infrastructure.

References

[1] Y. K. A.-N. M. Q. &. A.-S. Sinjilawi, ”Addressing Security and Privacy Issues in Cloud Computing,” *Journal of Emerging Technologies in Web Intelligence,* (2014).

[2] *Nkosi, Lucky & Tarwireyi, Paul & Adigun, Matthew. (2013). Insider threat detection model for the cloud. 2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference. 1-8. 10.1109/ISSA.2013.6641040..*

[3] *Christian Cachin, Idit Keidar, and Alexander Shraer. 2009. Trusting the cloud. SIGACT News 40, 2 (June 2009), 81–86. https://doi.org/10.1145/1556154.1556173.*

[4] *Al-Mhiqani, M. N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K. H., ... & Yunos, Z. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. Applied.*

[5] *Kandias, M., Virvilis, N. and Gritzalis, D The insider threat in cloud computing In International Workshop on Critical Information Infrastructures SecuritySpringer, Berlin, Heidelberg. 2011,* pp. 93-103.

[6] *Tchernykh, A., Schwiegelsohn, U., Talbi, E.G. and Babenko, M Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability Journal of Computational Science,* p. 36, 2019.

[7] [Online]. Available: Developer, Google GCP Service accounts Google 2020 https://cloud.google.com/iam/docs/service-accounts.

[8] [Online]. Available: Sutherland, Scott Invisible Threats: Insecure Service Accounts July 2010 https://blog.netspi.com/invisible-threats-insecure-service-accounts/.

[9] Ifrah, S Get Started with Google Cloud Platform (GCP). In Getting Started with Containers in Google Cloud Platform 2021 Apress, Berkeley, CA.

[10] *In Proceedings of the Sixth Workshop on Inclusive Privacy and Security (WIPS 2021): In Association with the Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)., Available at SSRN: https://ssrn.com/abstract=3875896 or http://dx.doi.org/10.21,* August 7, 2021.

[11] Thycotic Hackers and Security Pros at Black Hat 2019 https://thycotic.com/resources/black-hat-2019-hacker-survey-report/.

[12] [Online]. Available: Developer, Google 2020 Introducing Workload Identity: Better authentication for your GKE applications https://cloud.google.com/blog/products/containers-kubernetes/introducing-workload-identity-better-authentication-for-your-gke-applications.

[13] *Hossein Siadati and Nasir Memon. 2017. Detecting Structurally Anomalous Logins Within Enterprise Networks. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). Association for Computing Machinery, New York, N.*

[14] *Sabharwal, N. and Pandey, P "Automation with Jenkins and GCP-Native CI/CD Services" In Pro Google Cloud Automation 2021 ,* Vol. %1 av %2Apress, Berkeley, CA, pp. 221-299.

[15] *Andreas Tsagkaropoulos, Yiannis Verginadis, Nikos Papageorgiou, Fotis Paraskevopoulos, Dimitris Apostolou, Gregoris Mentzas, "Severity: a QoS-aware approach to cloud application elasticity", Journal of Cloud Computing, vol. 10, 2021.*

[16] *Bisong, E. (2019). Google Cloud Storage (GCS). In Building Machine Learning and Deep Learning Models on Google Cloud Platform (pp. 25-33). Apress, Berkeley, CA..*

[17] *Petrillo, F., Merle, P., Moha, N., & Guéhéneuc, Y. G. (2016, October). Are REST APIs for cloud computing well-designed? An exploratory study. In International Conference on Service-Oriented Computing (pp. 157-170). Springer, Cham..*

[18] *Serhane, Y., Sekkaki, A., Benzidane, K., & Abid, M. (2020). Cost Effective Cloud Storage Interoperability Between Public Cloud Platforms. International Journal of Communication Networks and Information Security, 12(3), 440-449..*

[19] *Mucchetti M. (2020) Cloud Shell and Cloud SDK. In: BigQuery for Data Warehousing. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-6186-6_22.*

[20] *Cauveri, A., & Kalpana, R. (2017, March). Dynamic fault diagnosis framework for virtual machine rolling upgrade operation in google cloud platform. In 2017 International Conference on Power and Embedded Drive Control (ICPEDC) (pp. 235-241). IEEE..*

[21] *Service accounts | Compute Engine Documentation - Google Cloud. https://cloud.google.com/compute/docs/access/service-accounts.*

[22] *Larsson, L., Tärneberg, W., Klein, C., Kihl, M., & Elmroth, E. (2021, June). Adaptive and Application-agnostic Caching in Service Meshes for Resilient Cloud Applications. In 2021 IEEE 7th International Conference on Network Softwarization (NetSoft) (pp. 1.*

[23] *Alimi, R. D., & Olufemi, O. G. Disaster Avoidance in Google Cloud Implementations. International Journal of Computer Applications, 975, 8887..*

[24] [Online]. Available: https://cloud.google.com/blog/products/identity-security/understanding-gcp-service-accounts-three-common-use-cases.

[25] *Ahmed, M., & Hossain, M. A. (2014). Cloud computing and security issues in the cloud. International Journal of Network Security & Its Applications, 6(1), 25..*

[26] *Lin, D. (2018). Insider threat detection: Where and how data science applies. Cyber Security: A Peer-Reviewed Journal, 2(3), 211-218..*

[27] *Everspaugh, A., Paterson, K., Ristenpart, T., & Scott, S. (2017, August). Key rotation for authenticated encryption. In Annual International Cryptology Conference (pp. 98-129). Springer, Cham..*

[28] *PCI Security Standards Council: Requirements and security assessment procedures. In: PCI DSS v3.2 (2016).*

[29] *Williamson, G. & Koot, A. & Lee, G., (2022) "Non-human Account Management (v3)", IDPro Body of Knowledge 1(7). doi: https://doi.org/10.55621/idpro.52.*

[30] Mike Danese, [Online]. Available: Mike Danese Introducing Workload Identity: Better authentication for your GKE applications Google 2019 https://cloud.google.com/blog/products/containers-kubernetes/introducing-workload-identity-better-authentication-for-your-gke-applications.

[31] *Buchanan, S., Rangama, J., & Bellavance, N. (2020). Inside kubernetes. In Introducing Azure Kubernetes Service (pp. 35-50). Apress, Berkeley, CA..*

[32] *C. -S. Park and H. -M. Nam, "A New Approach to Constructing Decentralized Identifier for Secure and Flexible Key Rotation," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3121722..*

[33] *Watanabe, T., Shioji, E., Akiyama, M., Sasaoka, K., Yagi, T., & Mori, T. (2018, April). User blocking considered harmful? An attacker-controllable side channel to identify social accounts. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P).*

[34] *Sukmana, M. I., Torkura, K. A., Graupner, H., Cheng, F., & Meinel, C. (2019, January). Unified cloud access control model for cloud storage broker. In 2019 International Conference on Information Networking (ICOIN) (pp. 60-65). IEEE..*

[35] *B. Yang, H. Chu, G. Li, S. Petrovic and C. Busch, "Cloud Password Manager Using Privacy-Preserved Biometrics," 2014 IEEE International Conference on Cloud Engineering, 2014, pp. 505-509, doi: 10.1109/IC2E.2014.91..*

[36] *Pavithra, S., Ramya, S., & Prathibha, S. (2019, February). A survey on cloud security issues and blockchain. In 2019 3rd International Conference on Computing and Communications Technologies (ICCCT) (pp. 136-140). IEEE..*

[37] *Lin, D. (2018). Insider threat detection: Where and how data science applies. Cyber Security: A Peer-Reviewed Journal, 2(3), 211-218..*

[38] *Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2021). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. Software and Systems Modeling, 1-21..*

[39] *Thunberg, S., & Arnell, L. (2022). Pioneering the use of technologies in qualitative research–A research review of the use of digital interviews. International Journal of Social Research Methodology, 25(6), 757-768..*

[40] *Bauer, G. R., Churchill, S. M., Mahendran, M., Walwyn, C., Lizotte, D., & Villa-Rueda, A. A. (2021). Intersectionality in quantitative research: a systematic review of its emergence and applications of theory and methods. SSM-population health, 14, 100798.*

[41] *Moore, D., McCabe, G., Duckworth, W. and Alwan, L., 2008. The practice of business statistics..*

[42] *Ilker Etikan, Sulaiman Abubakar Musa, Rukayya Sunusi Alkassim. Comparison of Convenience Sampling and Purposive Sampling..*

[43] i *Leigh, D. (2009). SWOT analysis. Handbook of Improving Performance in the Workplace: Volumes 1-3, 115-140.*.

[44] [Online]. Available: HashiCorp 2022 https://learn.hashicorp.com/tutorials/vault/getting-started-dynamic-secrets.

[45] G. SRE, ”Site Reliability Engineering,” Google , 2019. [Online]. Available: https://sre.google/.

[46] *GCP Service Accounts and Roles – Tech Notes. https://galinay.wordpress.com/2019/08/19/gcp-service-accounts-and-roles/.*

[47] nr https://medium.com/techking/key-rotation-in-google-cloud-3ee8ff0a7828.

[48] *Maxwell, J. A. (2008). Designing a qualitative study. The SAGE handbook of applied social research methods, 2, 214-253..*

[49] *Mitchell, N. J., & Zunnurhain, K. (2019, December). Vulnerability scanning with Google cloud platform. In 2019 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 1441-1447). IEEE..*

[50] *Poth, A., Werner, M., & Lei, X. (2018, September). How to deliver faster with CI/CD integrated testing services?. In European Conference on Software Process Improvement (pp. 401-409). Springer, Cham..*

[51] *Quick, J., & Hall, S. (2015). Part three: The quantitative approach. Journal of perioperative Practice, 25(10), 192-196..*

[52] *US20160364763A1 - System and method for presenting .... https://patents.google.com/patent/US20160364763A1/en.*

[53] *Aryotejo, G. and Kristiyanto, D.Y In Journal of Physics: Conference Series Hybrid cloud: bridging of private and public cloud computing 2018 IOP Publishing..*

[54] *Calheiros, R.N., Ranjan, R. and Buyya, R Virtual machine provisioning based on analytical performance and QoS in cloud computing environments International Conference on Parallel Processing 2021 .*

[55] *Cazacu, M., BODEA, C., DASCĂLU, M.I. and CUCU, C Using the Activity Theory to Identify the Challenges of Designing Elearning Tools based on Machine Learning for Security Operations Centers. eLearning & Software for Education, 2019.*

[56] *Chaudhury, P., Dhang, S., Roy, M., Deb, S., Saha, J., Mallik, A., Bal, S., Roy, S., Sarkar, M.K., Kumar, S. and Das, R ACAFP: Asymme A review on RSA algorithm. In 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON),* vol. IEEE, pp. (pp. 332-337), 2017.

[57] *Gurel, E., & Tat, M. (2017). SWOT Analysis: A Theoretical Review. The Journal of International Social Research, 10, 994-1006..*

[58] *Lwakatare, L.E., Kilamo, T., Karvonen, T., Sauvola, T., Heikkilä, V., Itkonen, J., Kuvaja, P., Mikkonen, T., Oivo, M. and Lassenius, C DevOps in practice A multiple case study of five companies. Information and Software Technology 2019 ,* pp. pp.217-230..

[59] *Mell, P. and Grance, T The NIST definition of cloud computing 2011.*

[60] *Velev, D. and Zlateva, P Cloud infrastructure security. In International Workshop on Open Problems in Network Security,* Vol. %1 av %2Springer, Berlin, Heidelberg., pp. (pp. 140-148), 2010, March.

Appendix

Interview Invitation

Subject: Invitation to participate in the research project titled: ‘‘Insider Threat For Service Account In Cloud Infrastructure.”

Dear (name of the participant),

You are invited to participate in my postgraduate research study on insider threat challenges for service accounts in cloud infrastructure. As a person directly involved in an esteemed organization’s decision-making process, we think you are in an ideal position to help us increase our understanding of the field.

The interview is very informal and should not take more than 30 minutes. The preferred interview platform is MS Teams, but alternative platforms could also be considered. The interview discussions published results, and participant responses from this study will be kept anonymous.

Each interview will be assigned a number code to help ensure that personal identifiers are not revealed during the analysis and write-up of findings. There is no compensation for participating in this study. Nonetheless, your contribution will be valuable for us as it will lead to a greater understanding of the threat associated with service accounts and the key rotation process.

If you are prepared to participate, kindly suggest a day and time that is appropriate for you, and I will try my best to conduct the interview in the given slot.

Kindly let me know if you have and questions, I will be happy to answer.

Respectfully,

Ravikiran