Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CSE4011 – Virtualization
(E1 Slot)

Project Report on:

STORAGE VIRTUALIZATION AND CLOUD BACKUP

Submitted by:

Yashvi Thakkar
16BCE0867

Rishab Gupta
16BCE0757

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

DECLARATION

I hereby declare that the project entitled **“Storage Virtualization and Cloud Backup”** submitted by me to the School of Computer Science and Engineering, Vellore Institute of Technology, Vellore-14 towards the partial fulfillment of the requirements for the course CSE4011- Virtualization is a record of bonafide work carried out by me under the supervision of **JOTHI K.R.** I further declare that the work reported in this project has not been submitted and will not be submitted, either in part or in full, for any other course or purpose of this institute or of any other institute or university.

Signature

Yashvi Thakkar

16BCE0867

Rishab Gupta

16BCE0757

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

CERTIFICATE

The project report entitled “**Storage Virtualization and Cloud Backup**” is prepared and submitted by **Yashvi Thakkar(16BCE0867), Rishab Gupta (16BCE0757)** , has been found satisfactory in terms of scope, quality and presentation as partial fulfillment of the course CSE4011-Virtualization in Vellore Institute of Technology, Vellore-14, India.

Guide

(Name & Signature)

ACKNOWLEDGEMENT

The project “**Storage Virtualization and Cloud Backup”** was made possible because of inestimable inputs from everyone involved, directly or indirectly. I would first like to thank my guide, Prof. Jothi K.R., who was highly instrumental in providing not only a required and innovative base for the project but also crucial and constructive inputs that helped make my final product. My guide has helped me perform research in the specified area and improve my understanding in the area of web development and internet of things and I am very thankful for her support all throughout the project.

I would also like to acknowledge the role of the HOD, **Prof Santhi V** , who was instrumental in keeping me updated with all necessary formalities and posting all the required formats and document templates through the mail, which I was glad to have had.

It would be no exaggeration to say that the Dean of SCOPE, Prof Saravanan R, was always available to clarify any queries and clear the doubts I had during the course of my project.

Finally, I would like to thank Vellore Institute of Technology, for providing me with a flexible choice and execution of the project and for supporting my research and execution related to the project.

TABLE OF CONTENT

S.N **Topic**

LIST OF TABLES

TITLE

LIST OF ABBREVIATIONS

ABBREVIATION	EXPANSION
SMI	Storage management initiative
CIM	Common information model
GPS	Geographical Positioning System
API	Application programming interface
GCP	Google cloud platform
GIS	Geographical Information System

ABSTRACT

It is very important to store the date securely on the cloud. Moreover storing in an encrypted way, that too from one's phone will ease out the entire process. Many cloud-based capacity arrangements give reinforcements to individual information. While being very helpful, there are still a few issues. There's no unwavering quality keep an eye on the information being put away state in the event of debacles or the supplier goes liquidation, information shouldn't be lost. Also privacy is an important issue when it comes to confidential data. We need to be sure that nobody can view our personal files. Therefore, the goal is of this project is to attack these problems. This can be achieved by a secure cloud backup system which is easily available and is handy to use. Google Cloud Storage Platform will be used to analyze storage virtualization benefits and further a case study will be provided how Google Cloud is efficient enough to store data and helps us in valuing a reliable, robust and a steady source of backup.

CHAPTER 1

INTRODUCTION

PROBLEM STATEMENT

Cloud backup, generally called online support, is a methodology for help up information that joins sending a duplicate of the information over a restrictive or open system to an off-website server. Cloud support courses of action engage endeavors or individuals to store their information and PC records on the Internet utilizing a gathering expert network, instead of securing the data locally on a physical plate, for instance, a hard drive or tape reinforcement.

Virtualization when all is said in done is the division of a gadget's capacities from its physical components. For example, server virtualization isolates calculation and I/O from the plastic and metal server, thusly giving managers a chance to run a few virtualized servers on a solitary physical server. Capacity virtualization is comparable in that a unit's physical drive is isolated from its capacity, which is to store information. However, while this idea applies to a few stockpiling ideas -, for example, SANs, RAID and slight provisioning - the expression "stockpiling virtualization" is commonly used to allude to a procedure by which a few physical plates seem, by all accounts, to be a solitary unit. Virtualized stockpiling is commonly square measurement instead of report level, implying that it would seem that an ordinary physical drive to PCs.

Information security has reliably been a basic issue in data progression. In the coursed figuring condition, it winds up being especially bona fide in light of the way that the information is masterminded in better places even in all the globe. Information security and security attestation are the two standard parts of client's worries over the cloud advancement. Ignoring the way that different systems on the concentrations in scattered preparing have been broke down in. the two scholastics and undertakings, information security and security insurance are contorting up persistently basic for the future improvement of coursed enrolling progression in government, industry, and business.

Encryption is the way toward ensuring individual information by using a "mystery code" to scramble it with the goal that it can't be perused by any individual who doesn't have the code key. Today, tremendous measures of individual data are overseen on the web and put away in the cloud or on servers with a progressing association with the web. It's almost difficult to work together of any sort without individual information winding up in an arranged PC framework, which is the reason it's essential to realize how to help keep that information private.

In conventional on location reinforcement frameworks security is fundamentally a physical concern – guaranteeing information is supported up in more than one area if there should be an occurrence of equipment misfortune or disappointment and confining access to the physical reinforcement media to just confided in workers. In cloud reinforcement, security concerns are unique. In many cloud applications, for instance, G Suite (when known as Google Apps), Office 365 and Salesforce, data is made in the cloud and after that copied to the support provider.

Cloud fortification providers have their very own security set up to guarantee the security of the physical servers, anyway information might be helpless while it is in travel. This is the reason information encryption is the most fundamental key to cloud security. encoded information can't be gotten to in a decipherable configuration, even in case it is blocked while in exchange on the web.

90% of associations state they have worries about cloud security and 45% refer to security as the fundamental obstruction to additionally cloud selection, with unapproved access to information being the primary security concern. 65% of those studied additionally perceive that encryption is the best security control for cloud information. Information ought to be encoded both while in travel and once it achieves the servers of the cloud supplier and stays away. Putting away the information in encoded group implies that if an unapproved individual figures out how to accomplish physical or electronic access to these reinforcement servers, the real information will even
now be out of reach.

CHAPTER 2

LITERATURE SURVEY

Table 1.1 displays the literature survey.

Paper	Methods Used	Parameters considered	Conclusion
[1] Managing data storage systems in virtual systems based on storage awareness	Managing data storage in virtual systems using Storage Management Initiative Specification (SMI-S), and Common Information Model (CIM) technologies	Storage devices: Symmetrix or Clarrion VMware, VMware Virtual Server	Data storage on virtual system is efficient and reliable. Two interfaces which take up the role of communicate with the data storage system and other store and retrieve data.
[2]Apparatus and method for constructing storage virtualization network	In-band virtualization and out-band virtualization.	Hardware processor to execute computer readable instructions, Storage device to store area information for the first area.	A method for managing a storage virtualization network has been proposed which has a secure communication channel as well.
[3] Storage performance testing to evaluate moving data among arrays	Duplicating host input/output (I/O) requests from the host to form a first set of the host I/O requests for processing on the production LUN on the source array	Host accesses a production LUN on a source array, a test LUN on a target array	A technique to evaluate of moving logical storage unit is successfully devised and analyzed. The LUC is an array stored on a virtual platform.

[4] On construction of a distributed data storage system in cloud	Hadoop distributed system was used and a synchronized Android application was made which provided a data storage medium.	Implements a resource monitor of machine status factors such as CPU, memory and network usage help to optimize the virtualization system and data storage system.	High perfomance, load balancing and able to be replicated that provides data storage for private cloud was deployed.
[5] Scalable and secure high-level storage access for cloud computing platforms	Trusted component processes the message by authenticating the client virtual machine and locating an internal mapping between the client virtual machine and an associated customer-specific set of backend storage resources to which the requested storage object operation	Backend storage system, Hypervisor, Client Virtual Machine, Cryptographic communication	The proposed system provides cloud computing platforms and applications, and more specifically to methods which are scalable and secure high-level storage access for cloud computing platforms
[6] ID Based Cryptography for Cloud Data Storage	Cryptographic stream by ID based storage. IBC-PKG assigned to each cloud storage client.	Cryptographic keys, storage environment, security, IBC secret key, prevent unauthorized access	ID based cryptography provides secrecy on public servers and facilitates controlled data access, thereby also preventing unauthorized access.
[7] Cryptographic Cloud Storage	Microsoft Azure, Amazon Web Services and many other cloud storage services are surveyed by testing ad storing large amount of data	Cloud provider, Cloud Architecture, Storage cloud, Storage service provider	An overview of recent advances in crypto-graphy motivated specifically by cloud storage and provide benefits of various architectures

[8] An analysis on Data accountability and security in cloud	Analysis of four models - RSA based system, Privacy model, Cloud computing data security model, cloud information account-ability framework by developing Light Weight framework for accountability and security.	Privacy manager cloud, RSA based storage security system, Cloud computing data security model, Cloud information account-ability framework	Light weight framework provides data security by auditing and logging in features. All four models have been incorporated to make one more accountable and secure one.
[9] Cloud computing data storage security framework relating to data integrity, privacy and trust	The functioning of forensic virtual machine, malware detection and real time monitoring system is worked upon	Basic encryption and decryption algorithm, performance of providing secure cloud storage	Data security framework provided here is grandparents and thereby reduces data security threats in cloud environment.
[10] Anonymous Cloud: A Data Ownership Privacy Provider Framework in Cloud Computing	Data ownership and privacy provided by implementing an anonymizing circuit based on Tor	A tune able parameter k controls a trade off between the degree of anonymity and computational overhead imposed by the system	Anonymous authentication based on public key cryptography safely links jobs and data to customers for billing purposes without revealing these associations to untrusted computation nodes.
[11] Cloud Computing Security: Amazon Web Service	Working of Amazon Web services especially by highlighting its security and storage features by real time testing	Security and storage research in the field of cloud security	AWS is the most trusted cloud service provider with excellent features and account-ability. It provides network scalability, disaster recovery, backup and encrypted data storage features.

[12] Storage Virtualization of files	Secure file storage is performed on IBM cloud by various private and public keys	Data encryption and decryption techniques like RSA, SHA 256 are analyzed	This paper highlights the importance data encryption and file storage in cloud comp-uting, here performed on IBM cloud.

Table 1.1 Literature Survey

The paper[1] talks about how we manage data storage systems in virtual system based on storage awareness. In this paper data has been managed using storage management initiative specs. It was realized how data storage on virtual system is efficient and reliable, without interfaces which take up the role of communication with the data storage system and other storage mediums and retrieve data.

Paper [2] talks about the Apparatus and method for constructing storage virtualization network. In-band and out-of-band virtualization schemes are used for this. In-band virtualization is constructing storage virtualization network. The data flow separated from the control flow is carried out in out-of-band virtualization.

Capacity execution testing to assess moving information among arrays[3] is a procedure to assess of moving legitimate capacity unit is effectively concocted and examined. The LUC is a cluster put away on a virtual stage. This should be possible by copying host input/yield (I/O) demands from the host to shape a first arrangement of the host I/O demands for preparing on the creation LUN on the source exhibit.

Development of an appropriated information stockpiling framework in cloud [4] utilizes development of a conveyed information stockpiling framework in cloud and executes an asset screen of machine status factors, for example, CPU, memory and system utilization help to streamline the virtualization framework and information stockpiling framework.

In the paper [5] Scalable and secure abnormal state stockpiling access for distributed computing stages utilizes a Trusted segment forms the message by confirming the customer virtual machine and finding an inner mapping between the customer virtual machine and a related client explicit arrangement of backend stockpiling assets to which the mentioned stockpiling object activity to give A review of late advances in cryptography propelled explicitly by distributed storage and give advantages of different models.

ID Based Cryptography for Cloud Data Storage[6] is a technique in visualization shows that ID based cryptography provides secrecy on public servers and facilitates controlled data access, thereby also preventing unauthorized access. It considers various aspects of the system such as Cryptographic keys, storage environment, security, IBC secret key, prevent unauthorized access.

Microsoft Azure, Amazon Web Services and many other cloud storage services are surveyed by testing ad storing large amount of data and the main key focus was on storage services. This has been featured in Cryptographic Cloud Storage [7] An outline of late advances in cryptography persuaded explicitly by distributed storage and give advantages of different structures has been given.

An analysis on Data accountability and security in cloud [8] that showed how light weight framework provides data security by auditing and logging in features. All four models have been incorporated to make one more accountable and secure one by analyzing them. Analysis of four models - RSA based system, Privacy model, Cloud computing data security model, cloud information account has been carried out the their ability to framework by developing Light Weight framework has been proved to provide optimum accountability and security.

Mysterious confirmation dependent on open key cryptography securely connects occupations and information to clients for charging purposes without uncovering these relationship to untrusted calculation hubs should be possible by dissecting information possession and protection given by executing an anonymizing circuit dependent on Tor. This is discussed in Anonymous Cloud: A Data Ownership Privacy Provider Framework in Cloud Computing. [10]

In [11] Cloud Computing Security: Amazon Web Service we find that AWS is the most believed cloud specialist co-op with brilliant highlights and responsibility. It gives arrange adaptability, catastrophe recuperation, reinforcement and scrambled information stockpiling highlights. Amazon Web Services is a backup of Amazon that gives on-request distributed computing stages to people, organizations and governments, on a metered pay-as-you-go about it. Working of Amazon Web administrations has been featured particularly by featuring its security and capacity includes by continuous testing.

This paper [12] Storage Virtualization of files highlights the importance data encryption and file storage in cloud computing, here performed. It considers data encryption and decryption techniques like RSA, SHA 256 which haven been covered in the paper.

CHAPTER 3

DESIGN OF PROPOSED SYSTEM AND IMPLEMENTATION

3.1 Architecture of the proposed system

This project consists of three modules:

1. Backup module : This consists of a backup.sh file which will carry out a timely backup of the files stored in the backup folder. The time is specified by the user using the crontab command.

2. Restore module: This module consists of a restore.sh file which will carry out the restore whenever the potential user in need of it. Restore module performs a backup by default as a safety feature in order to protect the files.

3. Google Cloud Platform: This provides individual users with a interoperability key and with this key the file which is being backed up is encrypted and decrypted.

Google Cloud Platform is a suite of dispersed figuring administrations that keeps running on a similar foundation that Google utilizes inside for its end-client items, let’s say for example, Google Search and YouTube. Close by a lot of the board devices, it gives a progression of particular cloud administrations including registering, data accumulating, data examination and AI. Enrollment requires a charge card or ledger subtleties. Google Cloud Platform gives Infrastructure as an organization, Platform as an organization, and server less figuring situations. After the declaration of App Engine has been made, Google has added adaptable cloud administrations to it's stage.

Google Cloud Platform incorporates the Google Cloud Platform open cloud framework, just as G Suite, undertaking adaptations of Android and Chrome OS, and application programming interfaces (APIs) for AI and endeavor mapping administrations. It is given by Google and a standout amongst its best item is the capacity highlight of Google cloud stage. The different functionalities give by Google cloud storage models are :

Circulated stockpiling - Object amassing with combined edge holding to store unstructured information.

Cloud SQL - Database as a Service dependent on MySQL and PostgreSQL.
Cloud BigTable - Managed NoSQL database association.
Cloud Spanner - Horizontally flexible, fervently trustworthy, social database association.
Cloud Datastore - NoSQL database for web and advantageous applications.
Storage Disk - Block storing up for Compute Engine virtual machines.
Cloud MemoryStore - Managed in-memory information store dependent on Redis.

3.2 Module description

3.2.1 Google Cloud Platform

Google Cloud Platform (GCP) is a suite of cloud computing services. It is given by Google and it keeps on running on a similar framework that Google utilizes inside for its end-client things, such as Google Search and YouTube. Alongside a huge amount of chairmen's contraptions, it gives a development of disengaged cloud associations including computing, data storage, data analytics and machine learning. In this endeavor we are using Google Cloud Platform to process a perfect fortification and store the records in a can which involves a secured customer delivered key.

Creating a Google Cloud Platform account and logging onto it(Fig 3.2.1)

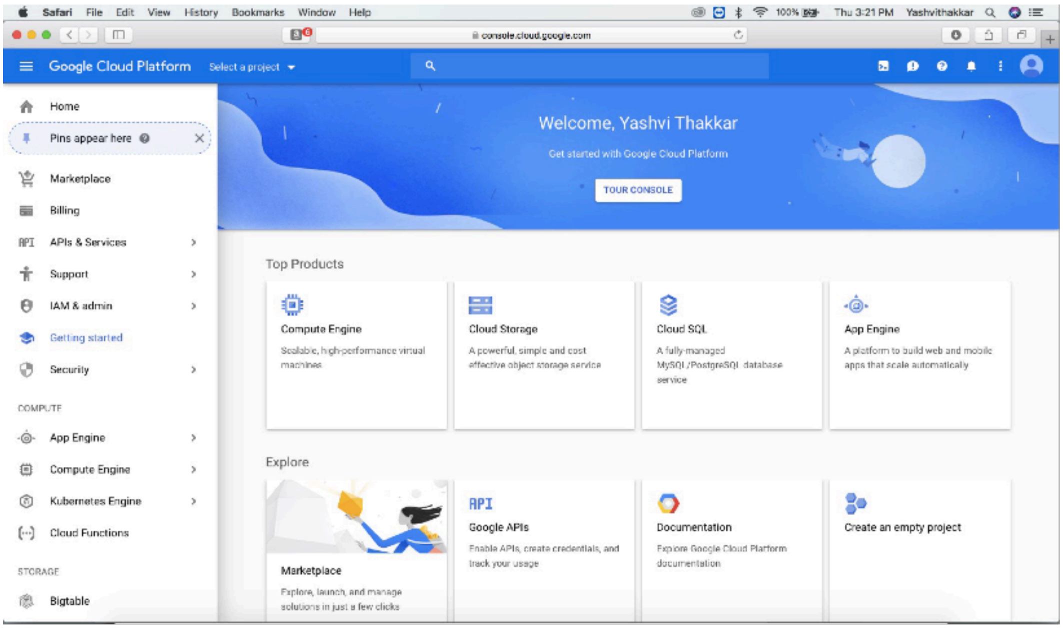

Safari File Edit View History Bookmarks Window Help
100% Thu 3:21 PM Yashvithakkar
console.cloud.google.com
Google Cloud Platform
Select a project
Home
Pins appear here
Marketplace
Billing
APIs & Services
Support
IAM & admin
Getting started
Security
COMPUTE
App Engine
Compute Engine
Kubernetes Engine
Cloud Functions
STORAGE
Bigtable
Welcome, Yashvi Thakkar
Get started with Google Cloud Platform
TOUR CONSOLE
Top Products
Compute Engine
Scalable, high-performance virtual machines
Cloud Storage
A powerful, simple and cost effective object storage service
Cloud SQL
A fully-managed MySQL/PostgreSQL database service
App Engine
A platform to build web and mobile apps that scale automatically
Explore
Marketplace
Explore, launch, and manage solutions in just a few clicks
API
Google APIs
Enable APIs, create credentials, and track your usage
Documentation
Explore Google Cloud Platform documentation
Create an empty project

Fig 3.2.1

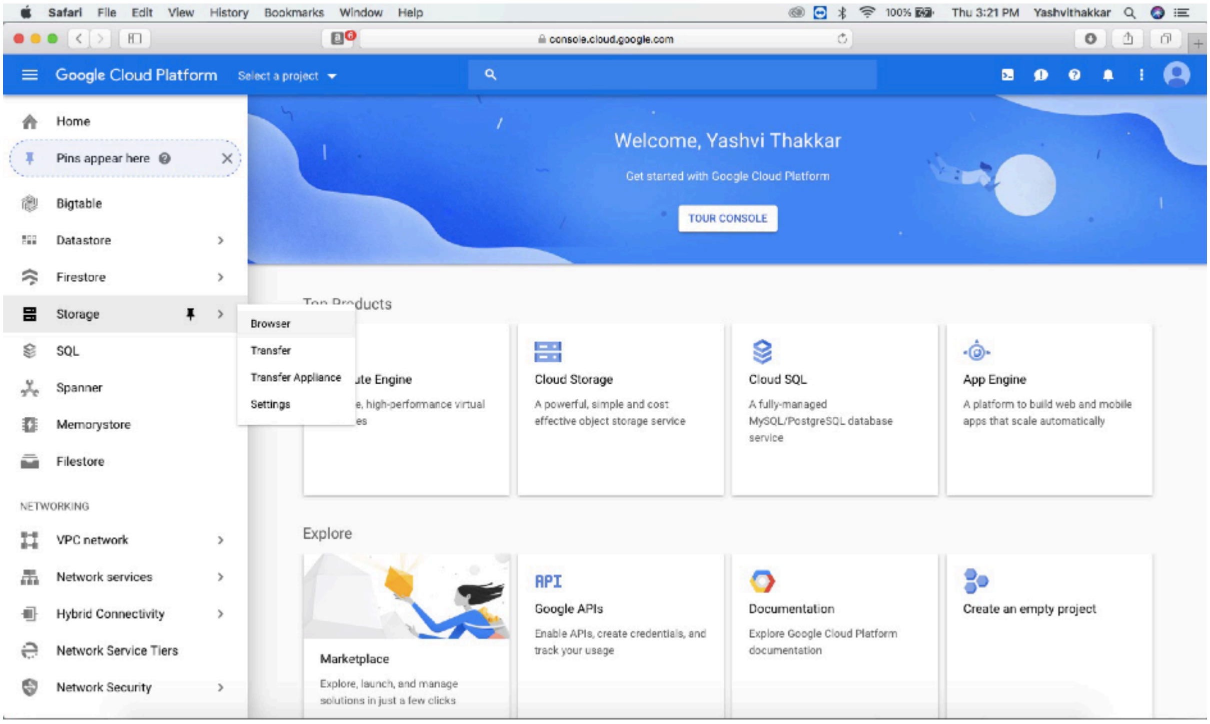
Google Cloud Platform Login

Create a new project say My First Project (Fig 3.2.2)

Fig 3.2.2. Creating First Project

Go to the Storage option on the left hand side menu. (Depicted in Fig 3.2.3)

Fig 3.2.3. Going to Storage Menu



Welcome, Yashvi Thakkar

Get started with Google Cloud Platform

...ute Engine
...e, high-performance virtual ...es

Cloud Storage
A powerful, simple and cost effective object storage service

Cloud SQL
A fully-managed MySQL/PostgreSQL database service

App Engine
A platform to build web and mobile apps that scale automatically

Marketplace
Explore, launch, and manage solutions in just a few clicks

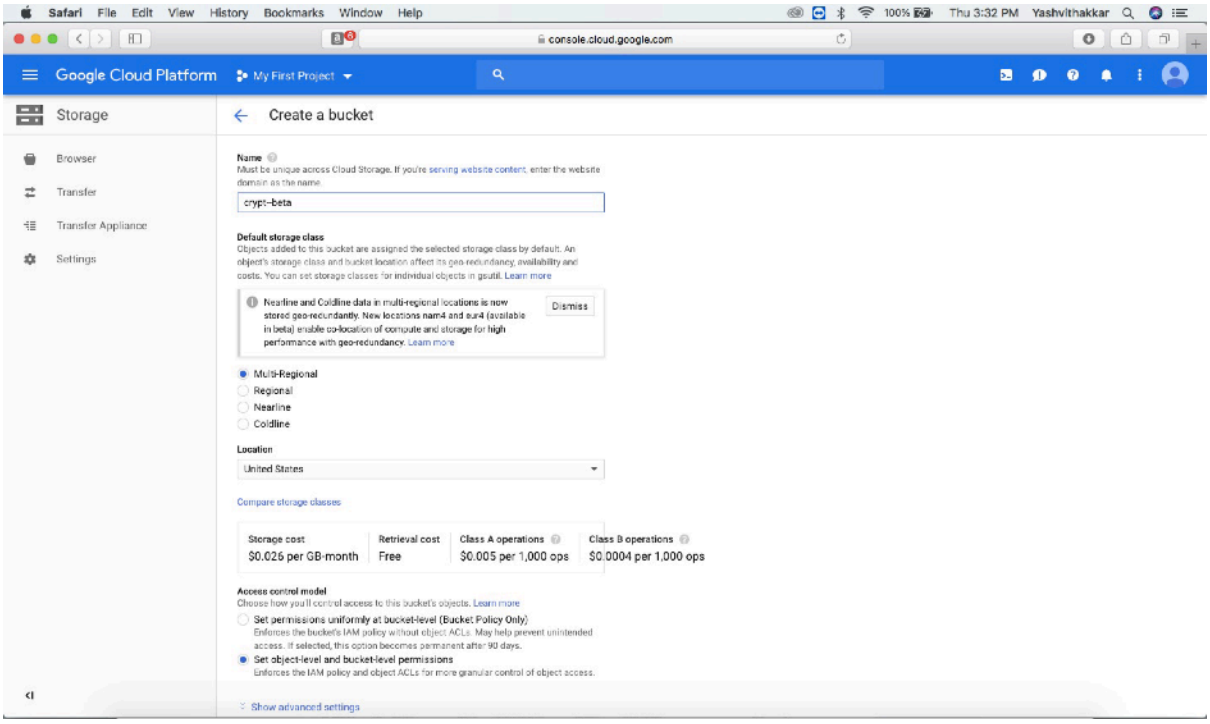
Google APIs
Enable APIs, create credentials, and track your usage

Documentation
Explore Google Cloud Platform documentation

Create an empty project

Create a new bucket, which is used to backup files at a particular time and help in recovery of the files as well. Select Coldline as the default storage class since files are going to be backed up from computer storage. Data will be accessed infrequently (i.e, not more than once per year). Typically coldline storage class is for disaster recovery, or data which is archived and may or may not be needed at some future time. This has been shown in the figure below. (Fig 3.2.4)

Fig 3.2.4. Creating a bucket name crypt-beta



Create a bucket

Name
Must be unique across Cloud Storage. If you're serving website content, enter the website domain as the name

crypt--beta

Default storage class
Objects added to this bucket are assigned the selected storage class by default. An object's storage class and bucket location affect its geo-redundancy, availability and costs. You can set storage classes for individual objects in gsutil. Learn more

Nearline and Coldline data in multi-regional locations is now stored geo-redundantly. New locations nam4 and eur4 (available in beta) enable co-location of compute and storage for high performance with geo-redundancy. Learn more

● Multi-Regional
○ Regional
○ Nearline
○ Coldline

Location
United States

Storage cost	Retrieval cost	Class A operations	Class B operations
$0.026 per GB-month	Free	$0.005 per 1,000 ops	$0.0004 per 1,000 ops

Access control model
Choose how you'll control access to this bucket's objects. Learn more

○ Set permissions uniformly at bucket-level (Bucket Policy Only)
Enforces the bucket's IAM policy without object ACLs. May help prevent unintended access. If selected, this option becomes permanent after 90 days.
● Set object-level and bucket-level permissions
Enforces the IAM policy and object ACLs for more granular control of object access.

3.1.2. Backup Module

This consists of a backup.sh file which will carry out a timely backup of the files stored in the backup folder. The time is specified by the user using the crontab command. The product utility cron is a period based job scheduler in Unix-like computer operating frameworks. Individuals who set up and keep up programming conditions use cron to plan occupations (directions or shell contents) to run intermittently at fixed occasions, dates, or interims. It normally robotizes framework support or organization—however its universally useful nature makes it helpful for things like downloading documents from the Internet and downloading email at customary interims. Cron is most appropriate for planning tedious assignments. Booking one-time undertakings can be practiced utilizing the associated at utility.

3.1.3. Restore Module

This module consists of a restore.sh file which will carry out the restore whenever the potential user in need of it. Restore module by default performs a backup. On running the restore file, al the files backed up in the bucket named crypt-beta on Google Cloud Platform will be decrypted and restored in the folder named backup. As soon as the restore command is encountered, it will ask the user for affirmation. If it's a "y" then it will proceed to restore otherwise it will terminate. After restoring, it backs them up again and, internally to prevent any loss of files, data etc. After restoring them, it will provide the details of the number of files and their storage space. Once simultaneous restoring and internal backup is complete, a completed message will be displayed.

ANALYSIS AND DESIGN

3.3 Brief introduction

gsutil is a Python application that gives one access A chance to distributed storage from the order line. gsutil instrument is utilized for coding slam records through which we can store documents on this container when a client sets a specific time for reinforcement. gsutil utilizes the prefix gs://to demonstrate an asset in Cloud Storage: gs://[Bucket-Name]/[Object_Name]

3.4 Code

Code:
Backup.sh

```
echo "Starting backup"

cd '/Users/Yashvi/Desktop/Virtualization'
source venv/bin/activate
gsutil rsync -D -d -r b gs://crypt-16bce0867/backup

echo "Complete."
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"backup.sh" 7L, 161C
```

Restore.sh

```
#!/bin/bash
read -p "Are you sure you want to restore? (y/n) " RESP
if [ "$RESP" = "y" ]; then
  echo "Restoring Data"
  gsutil rsync -d -r gs://crypt-16bce0867/backup backup
  echo "Syncing with backup"
  sh backup.sh
  echo "Restored Data"
else
  echo "Exiting"
fi
~
~
```

```
~
~
~
~
~
~
~
~
~
~
"restore.sh" 11L, 267C
```

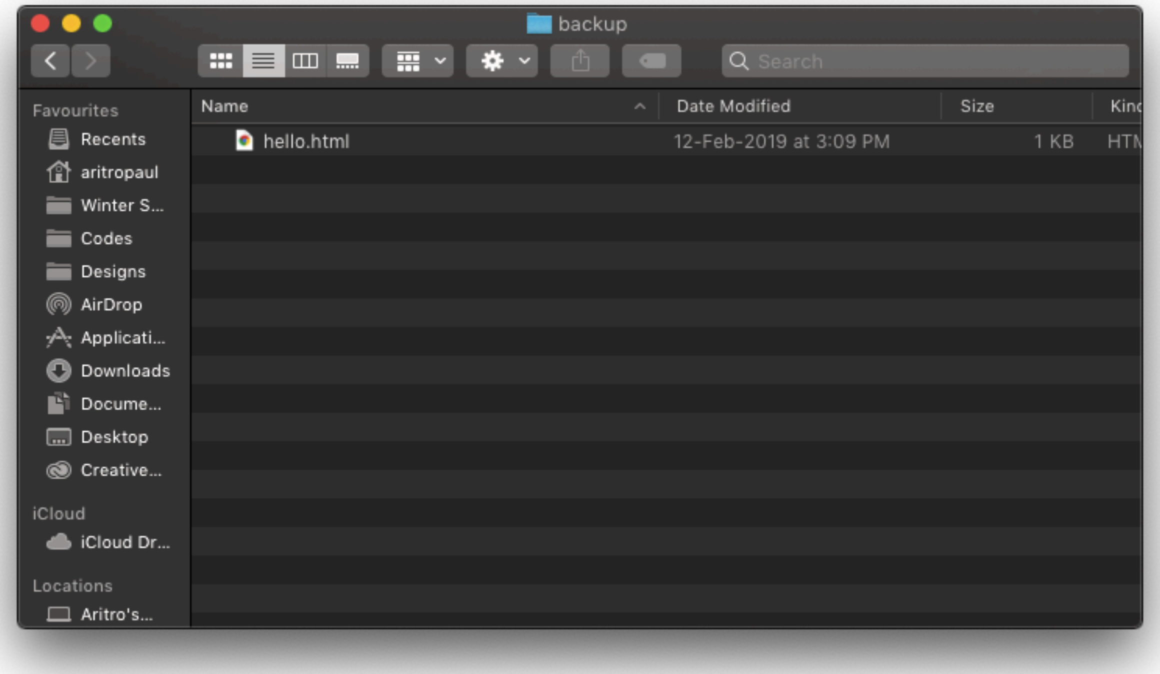
These two files facilitate the backup and restore functionalities of all the files stored in a folder named Backup. The codes in these files are in shell programming. Using Cron scheduler, we schedule the backup and restore files on a timely basis and these files get encrypted and stored in a secure manner in a bucket in one’s personal Google Cloud account.

IMPLEMENTATION

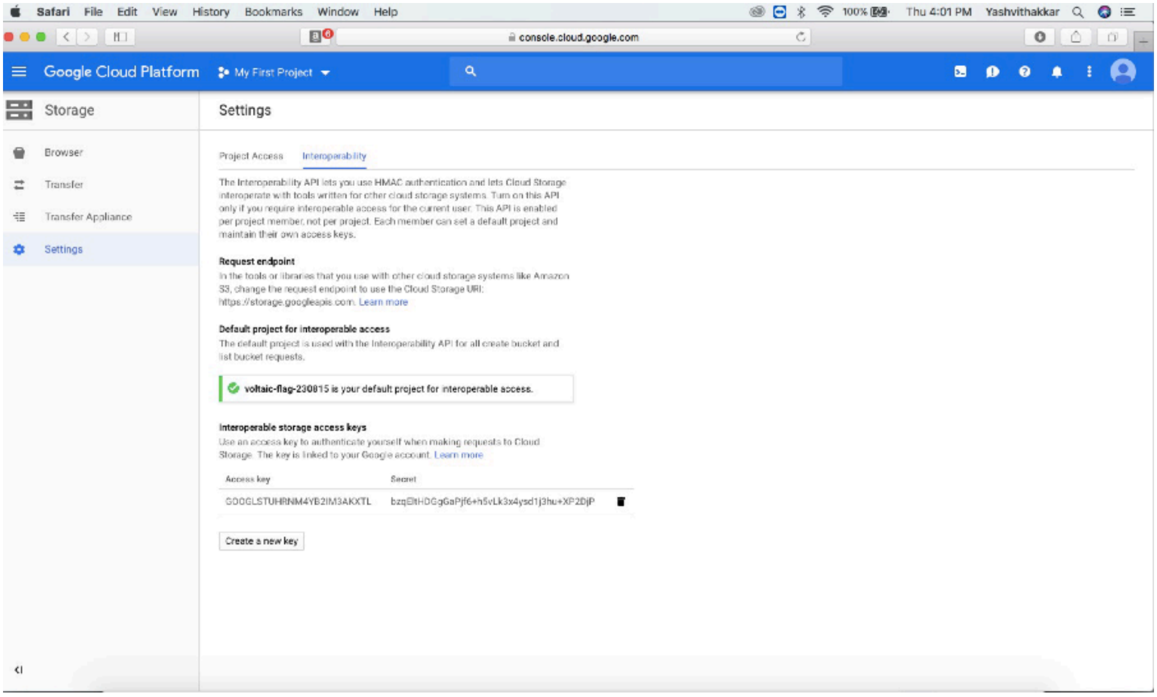
3.5 Methodology

Running backup.sh on terminal. In a backup folder, helloe.html is there. It needs to be backed up in the bucket named crypt-beta on Google Cloud Platform. (Depicted in figure 5.1.1)

Fig 5.1.1 Backup Folder



Google Cloud Platform will encrypt the file using a unique access key, provided to individual users and hence nobody can access it unless the user himself/herself. In the screenshot given below, the unique secret key is shown. (Fig 5.1.2)



Settings

Project Access Interoperability

The Interoperability API lets you use HMAC authentication and lets Cloud Storage interoperate with tools written for other cloud storage systems. Turn on this API only if you require interoperable access for the current user. This API is enabled per project member, not per project. Each member can set a default project and maintain their own access keys.

Request endpoint

In the tools or libraries that you use with other cloud storage systems like Amazon S3, change the request endpoint to use the Cloud Storage URI: https://storage.googleapis.com. Learn more

Default project for interoperable access

The default project is used with the Interoperability API for all create bucket and list bucket requests.

voltaic-flag-230815 is your default project for interoperable access.

Interoperable storage access keys

Use an access key to authenticate yourself when making requests to Cloud Storage. The key is linked to your Google account. Learn more

Access key	Secret
GOOGLSTUHRNM4YB2IM3AKXTL	bzqEltHDGgGaPjf6+h5vLk3x4ysd1j3hu+XP2DjP

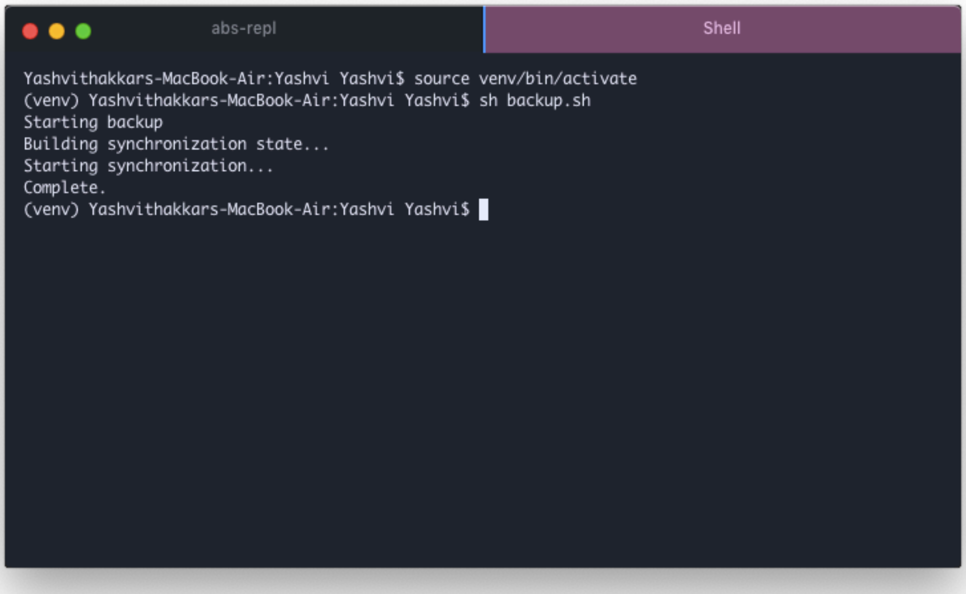
Create a new key

Fig 5.1.2 Generating interoperability key on GCP

3.6 System Testing

Testing of this system is carried out by running it various times and formulating the desired outputs.

Running the backup.sh file on terminal. Before running the backup.sh file, virtual environment is activated. Once complete is shown, the file will be uploaded in the bucket on Google Cloud Platform. This has been shown Fig 5.2.1.



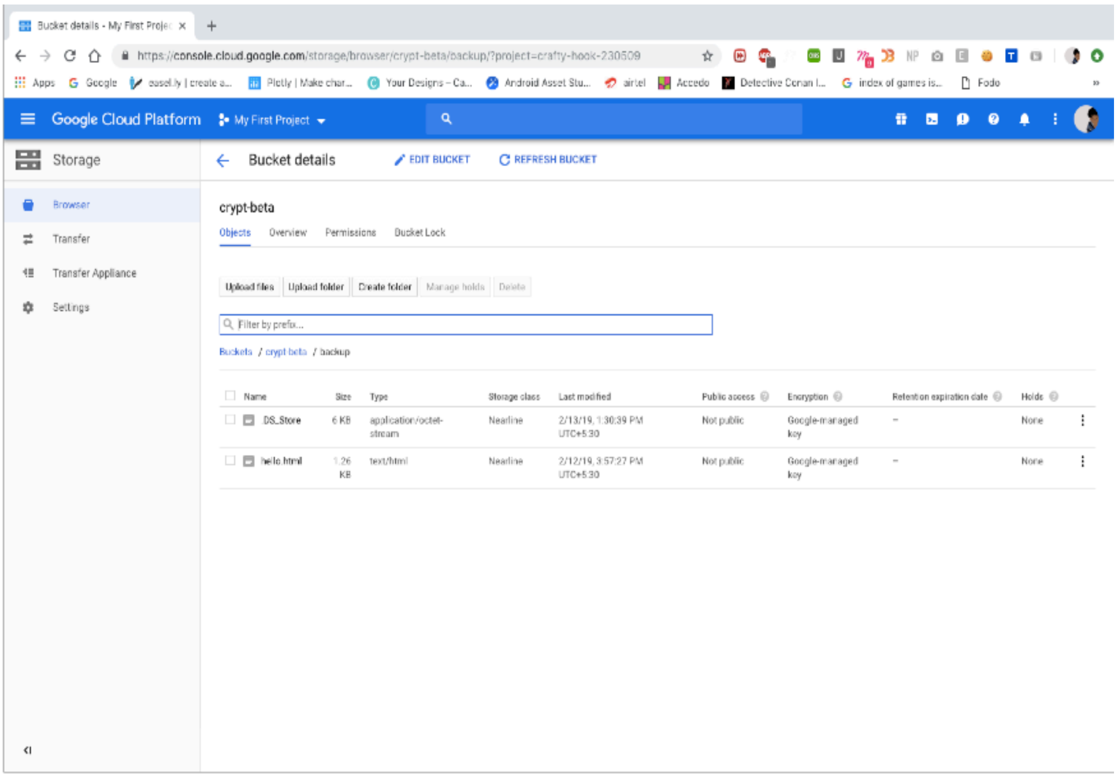
```
Yashvithakkars-MacBook-Air:Yashvi Yashvi$ source venv/bin/activate
(venv) Yashvithakkars-MacBook-Air:Yashvi Yashvi$ sh backup.sh
Starting backup
Building synchronization state...
Starting synchronization...
Complete.
(venv) Yashvithakkars-MacBook-Air:Yashvi Yashvi$
```

Fig 5.2.1 Running backup.sh on Terminal

In the bucket named crypt-beta, the file hello.html is saved. It is encrypted using the secret key which is also known as the interoperability key provided by GCP. This has been depicted in the figure given below. (Fig 5.2.2)

Fig 5.2.2/ Backed up files stored in the bucket on GCP

As we can see, here after the backup.sh file is run in Terminal, it automatically fetches the files in the backup folder, encrypts it using the key defined by the user, further saved in the bucket named crypt-beta on Google Cloud Platform. Restore.sh has helps in restoring the files the saved on the Google Cloud platform in the bucket names crypt-beta. This file on while running on terminal, asks the user for a confirmation to restore the files. If the user selects "y" then it restores them in to the same folder named backup and carries out an in built backup of the files again so that even if the user deleted those files by any chance from his/her desktop, the files can be fetched from the Google cloud. This way the entire module functions. A mail is also sent



Name	Size	Type	Storage class	Last modified	Public access	Encryption	Retention expiration date	Holds
.DS_Store	6 KB	application/octet-stream	Nearline	2/13/19, 1:30:39 PM UTC+5:30	Not public	Google-managed key	–	None
hello.html	1.26 KB	text/html	Nearline	2/12/19, 3:57:27 PM UTC+5:30	Not public	Google-managed key	–	None

b y

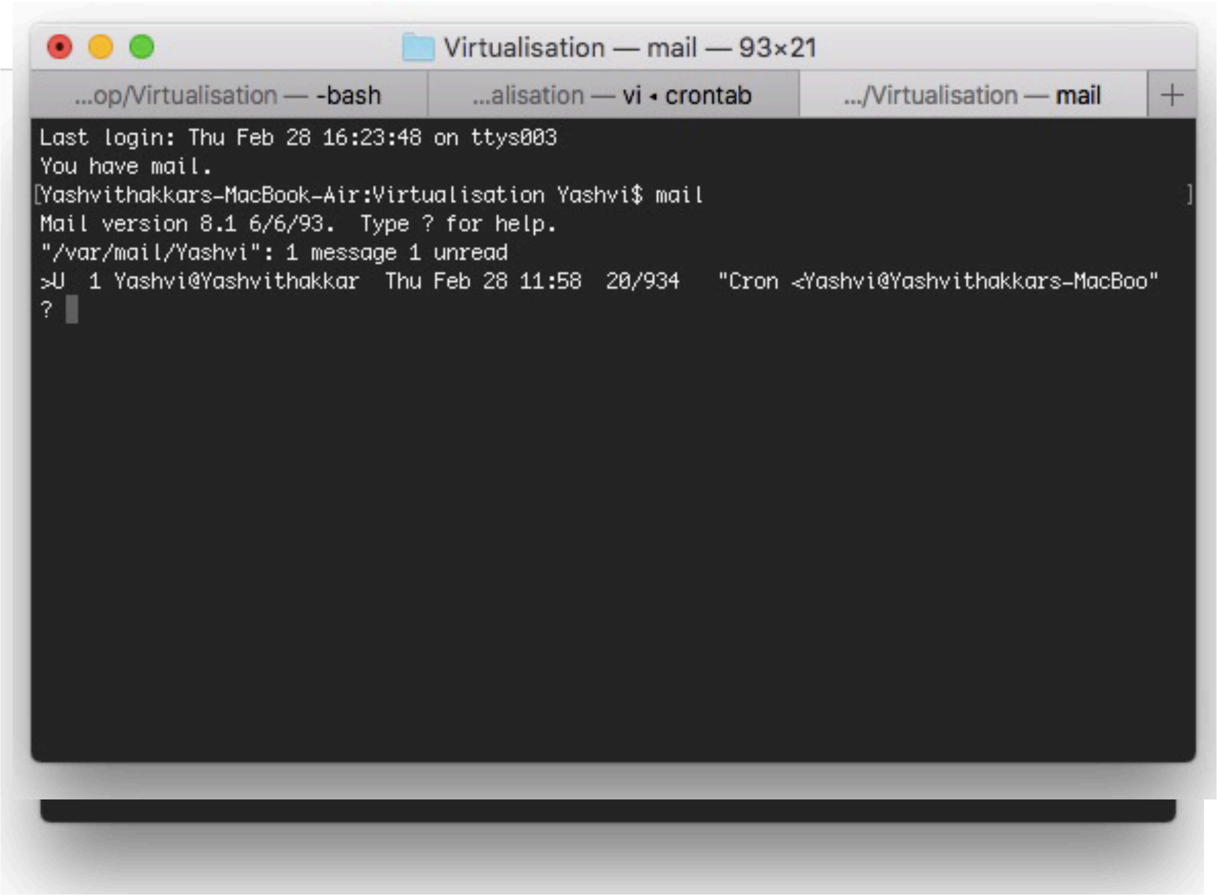
the cron on the terminal after every successful restoration of the files.

RESULT

3.7 SCREENSHOTS

At a decided time say 11:58 am at night, this backup will take place. Crontab work is utilized to plan occasions on an opportune premise. The product utility cron is a time sensitive activity scheduler in Unix-like PC working frameworks. Individuals who set up and keep up programming conditions use cron to plan occupations to run intermittently at fixed occasions, dates, or interims. Its configuration is: Minute Hour Day(Month) Month Day(Week). Utilizing order crontab – e we can set the time at which we need to set the day by day reinforcement. (Shown in Fig 6.1.1)

Fig 6.1.1. Saving a daily backup time on Terminal

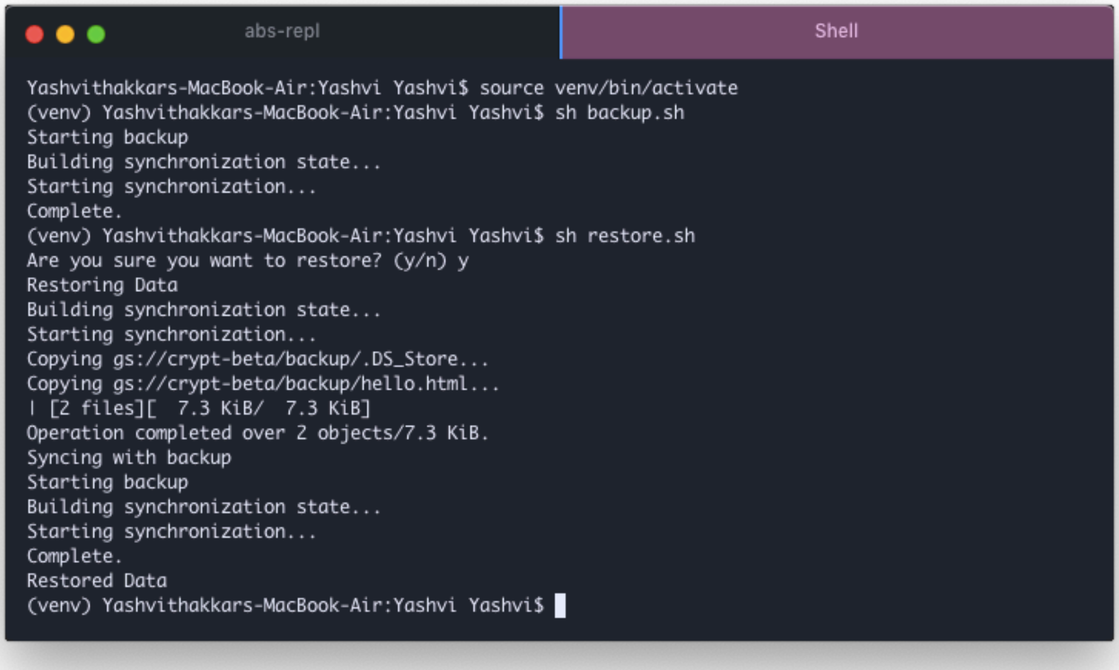

Virtualisation — mail — 93×21
...op/Virtualisation — -bash
...alisation — vi ◂ crontab
.../Virtualisation — mail
+

```
Last login: Thu Feb 28 16:23:48 on ttys003
You have mail.
[Yashvithakkars-MacBook-Air:Virtualisation Yashvi$ mail                                    ]
Mail version 8.1 6/6/93.  Type ? for help.
"/var/mail/Yashvi": 1 message 1 unread
>U  1 Yashvi@Yashvithakkar  Thu Feb 28 11:58  20/934   "Cron <Yashvi@Yashvithakkars-MacBoo"
? 
```

Here every morning at 11:58, backup will take place, with any source of internet connection. And as soon as you open the terminal, you will get a mail about the backup. (as shown below) The mail is from cron. This has been shown in the figure below. (Fig 6.1.2)

Fig 6.1.2 Running restore.sh on Terminal

On running the restore file, all the files backed up in the bucket name crypt-beta on Google Cloud Platform will be decrypted and restored in the folder named backup. As soon as restore command is encountered, it will ask the user for affirmation. If its a “y” then it will proceed to restore otherwise it will terminate. After restoring, it backs them up again, internally to prevent any loss of files, data etc. After restoring them, it will provide the details of the number of files and their storage space. Once simultaneous restoring and internal backup is complete, a completed message will be displayed. (This has been shown in figure 6.1.3)



```
Yashvithakkars-MacBook-Air:Yashvi Yashvi$ source venv/bin/activate
(venv) Yashvithakkars-MacBook-Air:Yashvi Yashvi$ sh backup.sh
Starting backup
Building synchronization state...
Starting synchronization...
Complete.
(venv) Yashvithakkars-MacBook-Air:Yashvi Yashvi$ sh restore.sh
Are you sure you want to restore? (y/n) y
Restoring Data
Building synchronization state...
Starting synchronization...
Copying gs://crypt-beta/backup/.DS_Store...
Copying gs://crypt-beta/backup/hello.html...
| [2 files][  7.3 KiB/  7.3 KiB]
Operation completed over 2 objects/7.3 KiB.
Syncing with backup
Starting backup
Building synchronization state...
Starting synchronization...
Complete.
Restored Data
(venv) Yashvithakkars-MacBook-Air:Yashvi Yashvi$ 
```

Fig
6.1.3 Mail sent by CronTab on successful restoration of files in backup folder from GCP

CHAPTER 4

4.1 CONCLUSION

Google Cloud Platform provides a secure and safer storage option. User can create buckets of their desired names. Backup and Restore modules will work on a timely basis by using gsutil and crontab commands. GCP internally encrypts and decrypts the files hence providing a better accountability and security of confidential data. Data can be stored on a virtual platform and backed up as well as restored in case of any disaster or abrupt losses.

4.2 REFERENCES

[1]: Labonte, K. S., Shajenko Jr, P., Dafoe, D. A., Wu, Y., & Kamra, A. (2015). U.S. Patent No. 9,081,594. Washington, DC: U.S. Patent and Trademark Office.

[2]: Zhou, D., & Xia, F. (2016). U.S. Patent No. 9,465,541. Washington, DC: U.S. Patent and Trademark Office.

[3]: Saad, Y., Natanzon, A. and Trachtman, M., EMC IP Holding Co LLC, 2018. Storage performance testing to evaluate moving data among arrays. U.S. Patent Application 10/007,626.

[4] : Yang, C. T., Shih, W. C., Huang, C. L., Jiang, F. C., & Chu, W. C. C. (2016). On construction of a distributed data storage system in cloud. Computing, 98(1-2), 93-118.

[5]: Protopopov, B., & Leschner, J. (2015). U.S. Patent No. 8,997,096. Washington, DC: U.S. Patent and Trademark Office.

[6]: Kaaniche, N., Boudguiga, A., & Laurent, M. (2013, June). ID based cryptography for cloud data storage. In 2013 IEEE Sixth International Conference on Cloud Computing (pp. 375-382). IEEE.

[7]: Kamara, S., & Lauter, K. (2010, January). Cryptographic cloud storage. In International Conference on Financial Cryptography and Data Security (pp. 136-149). Springer, Berlin, Heidelberg.

[8]: Hande, S. A., & Mane, S. B. (2015, May). An analysis on data Accountability and Security in cloud. In 2015 International Conference on Industrial Instrumentation and Control (ICIC) (pp. 713-717). IEEE.

[9]: Sirohi, P., & Agarwal, A. (2015, September). Cloud computing data storage security framework relating to data integrity, privacy and trust. In 2015 1st International Conference on Next Generation Computing Technologies (NGCT) (pp. 115-118). IEEE.

[10]: Khan, S. M., & Hamlen, K. W. (2012, June). AnonymousCloud: A data ownership privacy provider framework in cloud computing. In 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (pp. 170-176). IEEE.

[11]: Narula, S., & Jain, A. (2015, February). Cloud computing security: Amazon web service. In 2015 Fifth International Conference on Advanced Computing & Communication Technologies (pp.501-505). IEEE.

[12]: Neal R. Christiansen,Ravisankar V. PudipeddiScott A. Brender (2017, May). Storage Virtualization of files. Patent filed by Microsoft Licensing LLC- 2017