PUNE INSTITUTE OF COMPUTER TECHNOLOGY

Information Technology Department

Cloud Computing Laboratory

Case Study No. : 01
Data Storage Security in Private Cloud

Name: Sumit Dattu Chavan
Roll No.: 33113
Contact No.: 7350242190
Email ID: beingsumitchavan@gmail.com
Class: TE9
Batch: L9
Subject: Cloud Computing Laboratory

1. What is data storage in private cloud?

- Private cloud storage is a type of storage mechanism that stores an organization's data at in-house storage servers by implementing cloud computing and storage technology.
- Private cloud storage is similar to public cloud storage in that it provides the usability, scalability and flexibility of the storage architecture. But unlike public cloud storage, it is not publicly accessible and is owned by a single organization and its authorized external partners. Private cloud storage is also known as internal cloud storage.
- Private cloud storage works much like public cloud storage and implements storage virtualization across an organization, providing a centralized storage infrastructure that can only be accessed by the authorized nodes.
- Private cloud storage operates by installing a data centre, which houses a series of storage clusters that are integrated with a storage virtualization application. Administrative policies and a management console provide access to the different storage nodes and applications within the organization's network. The applications or nodes access the private storage through file access and data retrieving protocols, while the automated storage administrator application allocates storage capacity to them on run time.
- Private cloud storage has a multitenant architecture, where a single storage array can house storage space to multiple applications, nodes or departments.

2. Examples of data stored on cloud (success stories).

- **The New York Times:**
  Since 1979, the company has delivered newspapers at home. Between 2006 and 2009, the newspaper failed in its attempt to digitize home delivery, but in 2017 the CIS system was completely migrated to global cloud computing, and the system was renamed as Aristo. Now, Aristo is part of the digital subscription platform of the New York Times, generating more than 500 million dollars per subscription and processing around 6.5 million transactions during the first year.

- **Netflix:**
  In 1997, the company rented and sold DVDs within the United States through its digital platform. Due to shipping problems, the decision was made in 2008 to make the leap to the cloud, a transition that took 7 years. However, despite the wait, it was thanks to its migration to cloud computing that Netflix was able to launch its streaming platform globally, used by millions of people today.

- **General Electric:**

General Electric, which in 2017 decided to host more than 2,000 applications and services in the cloud, helping them to optimize and redirect resources, in what has been one of the company's biggest transformations, according to its CTO and vice president.

- **Pearson:**
  Pearson, the educational content multinational, which, thanks to a hybrid cloud infrastructure, has managed to redirect resources and focus them on the development of new educational projects.

- **Airbnb:**
  Airbnb, a company that, a year after its launch, and due to problems with its original provider, decided to migrate all its services and functions to AWS, marking the beginning of the success it currently enjoys.

3. **Procedures/ways to upload data to cloud (any applications designed).**
   The following are different procedures or the applications to upload data to cloud:

   - **App Engine (GAE) NodeJS with JSON API for smaller files:**
     You can launch a small NodeJS app on GAE for accepting smaller files directly to GCS ~20MB pretty easily. I started with the NodeJS GCS sample for GAE on the GCP GitHub account here. This is a nice solution for integrating uploads around 20MB. Just remember the nginx servers behind GAE have a file upload limit.

   - **Firebase on GAE with JSON API and Resumable uploads for large files:**
     Cloud Storage for Firebase allows you to quickly and easily upload files to a Cloud Storage bucket provided and managed by Firebase. While not very elegant with no status bar or anything fancy this solution does work for uploading large files from the web.

   - **gsutil from local or remote:**
     gsutil makes it easy to copy files to and from cloud storage buckets. gsutil makes it just easy to automate backup of directories, sync changes in directories, backup database dumps, and easily integrate with apps or schedulers for scripted file uploads to GCS.

   - **Cyberduck (MacOS) or any application with an S3 interface:**

Enjoy a client ftp type experience with Cyberduck on MacOS for GCS. Cyberduck has very nice auth integration for connecting to the GCS API built into the interface. After authenticating with auth you can browse all of your buckets and upload to them via the Cyberduck app.

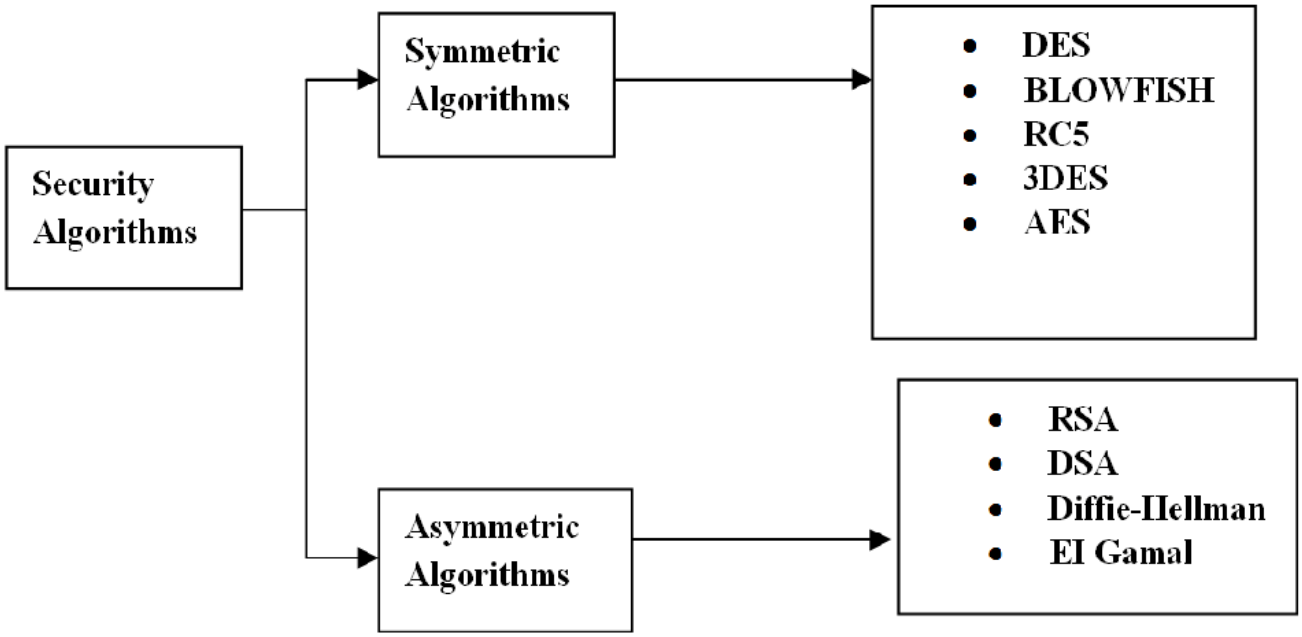
- **Cloud Function (GCF):**
  You can also configure a Google Cloud Function (GCF) to upload files to GCS from a remote or local location. This tutorial below is just for uploading files in a directory to GCS. Run the cloud function and it zips a local directory file and puts the zip into the GCS stage bucket.

- **Cloud Console UI:**
  The UI works well for GCS administration. GCP even has a transfer service for files on S3 buckets on AWS or other s3 buckets elsewhere. One thing that is lacking in the portal currently would be object lifecycle management. This is nice for automated archiving to cold line cheaper object storage for infrequently accessed files or files over a certain age in buckets.

4. Security algorithm in place for data security in cloud (list , brief differences , latest standard followed).

- The security algorithms in place for data security in cloud are broadly classified into two types. They are as follows:

a. Data Encryption Standard (DES) Algorithm:



The Data cryptography standard (DES) is a symmetric- key block cipher discovered as FIPS46 within the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). In encryption site, DES takes a 64- bit plaintext and creates a 64-bit ciphertext, after that the decryption site, it takes a 64-bit ciphertext and creates a 64-bit plaintext. Each encryption and decryption technique is used for the same 56-bit cipher key.

b. Blowfish Algorithm:

One of the most common public algorithms provided by Bruce Schneier, Blowfish algorithm, is a symmetric key algorithm, which functions almost like DES Algorithm, in which the key is small and can be decrypted easily. However, in the Blowfish algorithm, the size of the key is massive, and it can differ from 32 to 448 bits. Blowfish also consists of 16 rounds and can encrypt data having multiple sizes of eight, and if the size of the message is not multiple of eight, then bits are protected. In the Blowfish algorithm also, 64 bits of plain text is separated into two parts of the message as size 32 bits' length. One part acquires as the left part of the message, and another one is the right part of the message.

c. MD5 (Message-Digest Algorithm 5):

Message-Digest Algorithm 5 (MD5) is a cryptographic hash algorithm that can be used from an arbitrary length string to create a 128-bit string value. Though insecurities with MD5 have been identified, it is still widely used. MD5 is most commonly used for checking file integrity. It's also used in other security protocols and applications like SSH, SSL, and IPSec, however. Some applications reinforce the MD5 algorithm by adding a salt value to the plaintext, or by applying multiple hash functions.

d. Triple Data Encryption Standard (3DES):

3DES is based on the DES algorithm. Making use of Triple-DES is very easy to modify existing software. It also has the advantage of proven reliability and a longer key length that eliminates many of the attacks that can be used to reduce the time it takes to break DES. It takes three 64-bit keys, for a total 192-bit key length. In Stealth, you type in the entire 192-bit (24 characters) key rather than entering each of the three keys individually. The Triple-DES DLL then breaks the user-provided key into three subkeys, padding the keys if necessary, so they are each 64 bits long. The procedure for encryption is the same as regular DES, but it is repeated three times, hence the name Triple DES.

e. Advanced Encryption Standard (AES):

Advanced Encryption Standard is the new encryption suggested by NIST to replace DES. AES comprises three cipher blocks: AES-128, AES-192, and AES-256. AES-128 uses a 128-bit key length to encrypt and decrypt a message block, while AES-192 uses a 192-bit key length, and AES-256 a 256-bit key length for encrypting and decrypting messages.

f. Rivest-Shamir-Adleman (RSA) Algorithm:

RSA is a Public Key algorithm that provides security by encrypting and decrypting the data so that only authorized users can access it. RSA stands for Ron Rivest, Adi Shamir, and Len Adleman, who first described it in 1977. The data is encrypted, and the ciphertext is then stored onto the cloud. When a user needs the data, the user places a request to the cloud provider, then authorizes the user and provides him the data.

g. Digital Signature Algorithm (DSA):

The digital signature algorithm (DSA) refers to a digital signature standard. The National Institute of Standards and Technology (NIST) introduced it in 1991 as a better method for creating digital signatures. Along with RSA, DSA is considered one of today's most preferred algorithms for digital signatures. DSA does not encrypt message digests using a private key or decrypt message digests using the public key.

h. Diffie Hellman Key Exchange (D-H):

Whitfield Diffie and Martin Hellman discovered Diffie Hellman key algorithm substitute. It is a technique for exchanging securely by using cryptographic keys over a public network and was the primary specific sample of public-key cryptography. These two users do not need any prior knowledge about secrets sharing information between them.

i. El Gamal Encryption:

The El Gamal encryption system is an asymmetric key encryption algorithm for performing public-key cryptography, which is based on the Diffie–Hellman key exchange process by using cryptography. Taher El Gamal illustrated it in 1984. El Gamal encryption is protected in the free GNU Privacy Guard software, latest versions of PGP, and other cryptosystems. The Digital Signature Algorithm is detailed about a variant of the El Gamal signature scheme, which should not be confused with El Gamal encryption.

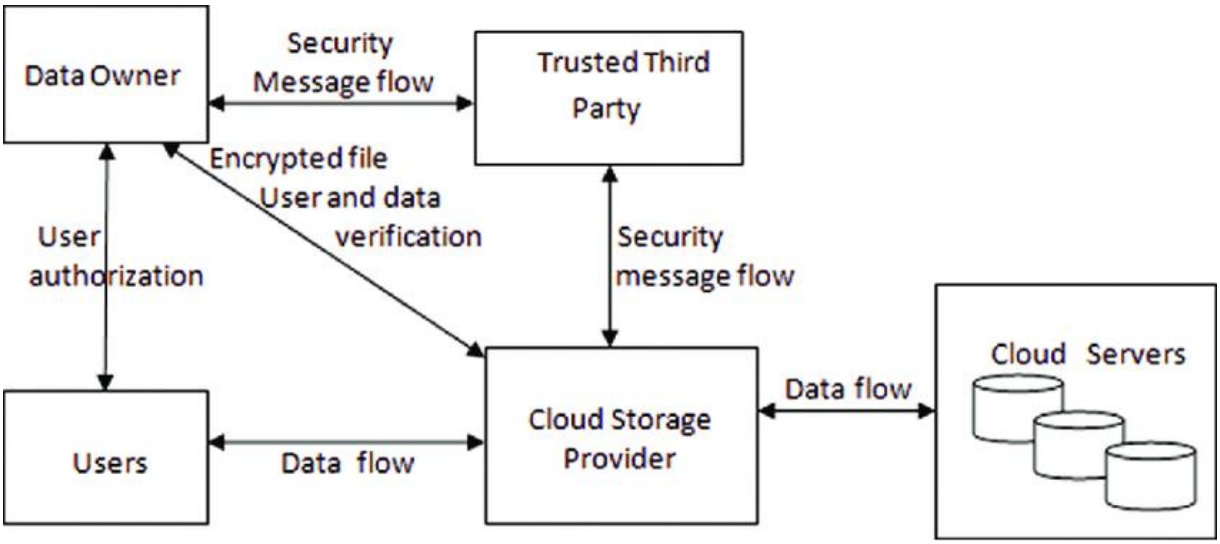
- Brief differences between different security algorithms:

Algorithms / Parameters	DES	3DES	AES	Blowfish	RSA	Diffie-Hellman
Encryption technique	Asymmetric key	Asymmetric key	Asymmetric key	Asymmetric key	Symmetric key	Symmetric key
Keys used	Same key used for encryption and decryption.	Same key used for encryption and decryption.	Same key used for encryption and decryption.	Same key used for encryption and decryption.	Different key used for encryption and decryption.	Key exchange.
Throughput	Lower than AES.	Lower than DES.	Lower than blowfish.	Very High	High	Low
Encryption ratio	High	Moderate	High	High	High	High
Key Lengths	56 bits.	112 to 168 bits.	128,192 or 256 bits.	32 bits to 448 bits.	>1024 bits	Key exchange management.
Rounds	16	48	10,12,14	16	1	56
Tunability	No	No	No	Yes	Yes	Yes
Security against	Brute force attack	Brute force, choosen-plain text, known plain text.	Chosen plain, known plain text.	Dictionary attacks	Timing attacks.	EavesDropping.
Flexibility support	No	Yes	Yes	Yes	Yes	No
Modification	No,DES does not support any modification	The key size is increased from 56 to 168 bits	128,192 or 256,Its structure was flexible to multiples of 64	Key length in blowfish should be multiples of 32	Key length in RSA algorithm can be 256 ,512,1024,2048, 4096 bits	No modification in key length.
Created by	IBM	IBM	Vincent Rijmen , Joan daeman	Bruce Schiener	Ron Rivest,Shamir & leonard Adleman	Whitfield diffie, Martin Hellman
Year	1970	1978	1978	1993	1978	2002
Structure of the Algorithm	Feistal structure	Feistal structure	Feistal structure	Feistal structure	Feistal structure	Tree based
Cloud Compatibility	Yes (Generally not used)	Yes	Yes	Yes	Yes	Yes
Algorithm used in Cloud	Not used in Cloud (it is prone to many attacks and easy to break)	Not used in Cloud (it is prone to many attacks and easy to break)	Google Drive, OneDrive, Dropbox	Mozy Backup, Foopchat, GigaTribe	Amazon web Services, RSAWeb	CurveCP
Application	Smart Card	Microsoft OneNote,Outlook 2007	Password Manager	IDS Server,Sql Server 2000	Online Credit Card Security System,RSA Signature Verification	In many Protocols like SSL,SSH,IPSec

- Latest Standards used in Cloud security:

- The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations. Although it is highly efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy-duty encryption purposes. Though AES is more secure than RSA in same bit size, AES is symmetrical encryption. AES is used by popular cloud platforms like Google cloud, AWS, etc.
- Homomorphic algorithm is the most suitable algorithm in cloud computing environment to secure their valuable data in an open network. The ability of homomorphic algorithm to perform operations on encrypted data enables high security than other algorithms such as RSA, DES, AES.

5. Diagrammatic representation of Data storage security in private cloud.



- As its name implies, private clouds grant a business private access to dedicated infrastructure resources within a cloud. As is the case for public cloud, there are both advantages and disadvantages with this infrastructure.
- A private cloud offers the most control over security parameters because all security efforts are done in-house, or are outsourced to a managed security provider. The security tools available with a private cloud include greater levels of authentication, API-enabled protection, additional layers of automation, and the potential for scalability if required.
- Private clouds have the ability to spread the workload over multiple servers but are limited by the amount of server space a company owns or operated.

6. Conclusion:

Hence, I understood what is data storage security in private cloud. Also, I learnt about:

a. Various ways to upload data on cloud.
b. Security algorithms for data security on cloud.
c. Private cloud security architecture.
d. Examples (success stories) of data stored on cloud.