CASE STUDIES AY 2021-2022

Case Study 1

Name of Assignment - Data storage security in private cloud

Roll No.- 33358

Batch- N11

Contact No.- 8766925932

Email Id- rapendse2002@gmail.com

ID card-

1. What is data storage in a private cloud?

   Private clouds are single-tenant solutions. A company owns and operates the servers, or leases dedicated servers from a datacenter. A private cloud's hardware can be stored on-site at a company's property, or housed in a datacenter. In strictly regulated industries, such as finance and healthcare, a private cloud is a compliance necessity.

   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.

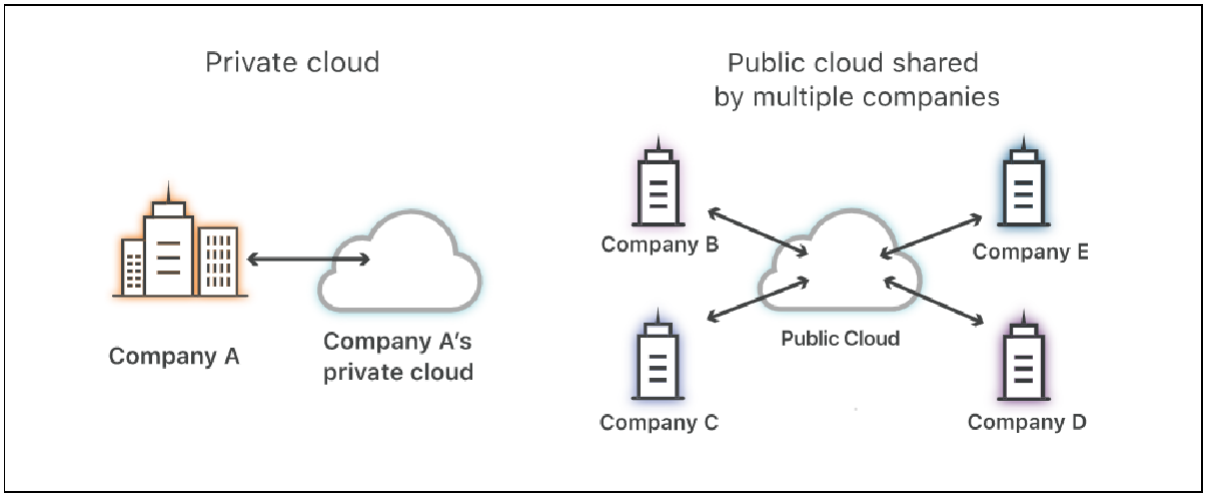
   Private cloud storage is similar to public cloud storage in that it provides the usability, scalability and flexibility of the storage architecture. But unlike public cloud storage, it is not publicly accessible and is owned by a single organization and its authorized external partners. Private cloud 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 center, 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) Some examples

are:

- Westinghouse Lighting

  Westinghouse Lighting is one of the most prominent names in the manufacturing industry of lighting equipment. It shifted towards a data backup service a few years back and saw a massive improvement in its business.

  The company claims that it has saved more than $50,000 by using cloud-based backup services instead of traditional on-site backup solutions. Similarly, an improvement of 45% was reported in terms of backup time management.

- Euronet Worldwide Inc

  A well-established secure electronic payment services provider, Euronet Worldwide, reported 50% improvement in its backup efficiency by deploying a Copy Data Storage Platform to save their data and applications.

  Moreover, Euronet went through a huge disaster that could have resulted in data losses. Instead, it was able

to restore the majority of the data and keep the sensitive financial information of the millions of users protected.

- Berger Schatz

  Berger Schatz is another law firm that moved from the conventional tape drives backup to cloud. As a result, it saw a significant drop of 65% in its backup costs and significantly improved backup time management. Furthermore, the recovery time was greatly reduced, which enhanced the firm's performance.

3. Procedures/ ways to upload data to cloud (are there any applications designed)

Some popular applications:

- Dropbox

  Dropbox is one of the best Android apps for people who work online or do a lot of business over the Internet, simply because it's one of the most popular. Many of us already use the Dropbox feature for PC's to share information and now the service spreads among Android devices. Dropbox users are granted 2GB of free space initially with the ability to move up to as much as 16GB. Any type of file that is stored on a computer or phone can be saved to Dropbox including Word documents, pictures, and even videos.

- Amazon Cloud Drive

  While the Amazon Cloud Drive mostly supports uploading photographs, the future is seemingly endless. Users may be able to preserve some of their purchased videos or e-books for access on any device, giving them another option besides their Amazon account. The free version of Amazon's cloud service includes 5GB of storage for JPG, BMP, PNG, GIF and other file types. It should be noted that MP3 music files purchased from Amazon aren't counted towards the data storage limits.

- OneDrive

  OneDrive is operated by Microsoft which means it should stick around for a while and also offers more support for Excel, PowerPoint, and other Office documents that might be stored on a smartphone. New OneDrive users are granted 7GB of storage for photos and specifically Microsoft Office file types (.doc, .ppt, .xls, etc.). Thus, if you work a lot with documents and need to keep them always with you, OneDrive might be your choice.

- Google Drive

  Again, familiarity usually breeds success. Thus Google Drive is constantly integrating their service with the Google+ accounts and other services that they'll own in the future. Many online companies are working with Gmail, Google Docs, and other services that can be best stored and viewed right within Google Drive. Google has merged their services to include 15GB of storage across Gmail, Google Docs, Google Drive, Google +, and Google photos and also supports virtually every file type including PDF's and Microsoft Office documents.

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

Security Algorithms:

- 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. The public key is known to all cloud users, whereas Private-Key is known only to the user who initially owns the data. The Cloud service provider performs encryption, and the Cloud user/cloud customer performs decryption. Once the data is encrypted with the Public Key, it can be decrypted with the corresponding Private Key.

- 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 the encryption site, DES takes a 64- bit plaintext and creates a 64-bit ciphertext, after that the decryption site 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. The encryption process is made of two permutations (P-boxes), that we tend to call initial and final permutation, and sixteen Feistel rounds. Each round transmits a different 48-bit round key generated from the cipher key encryption.

- 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. Each cipher encrypts and decrypts data in 128-bit blocks, using 128, 192, and 256-bit cryptographic keys.

  Symmetric, also known as a secret key, ciphers use the same key for encryption and decryption, so both sender and receiver have to know the same secret key — and use it —. Top Secret information requires either

key lengths of 192 or 256 bits. Ten rounds are available for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for a 256-bit key. A round consists of several processing steps involving the substitution, transposition, and mixing of the plaintext input to transform it into the final ciphertext output.

- Digital Signature Algorithm (DSA)

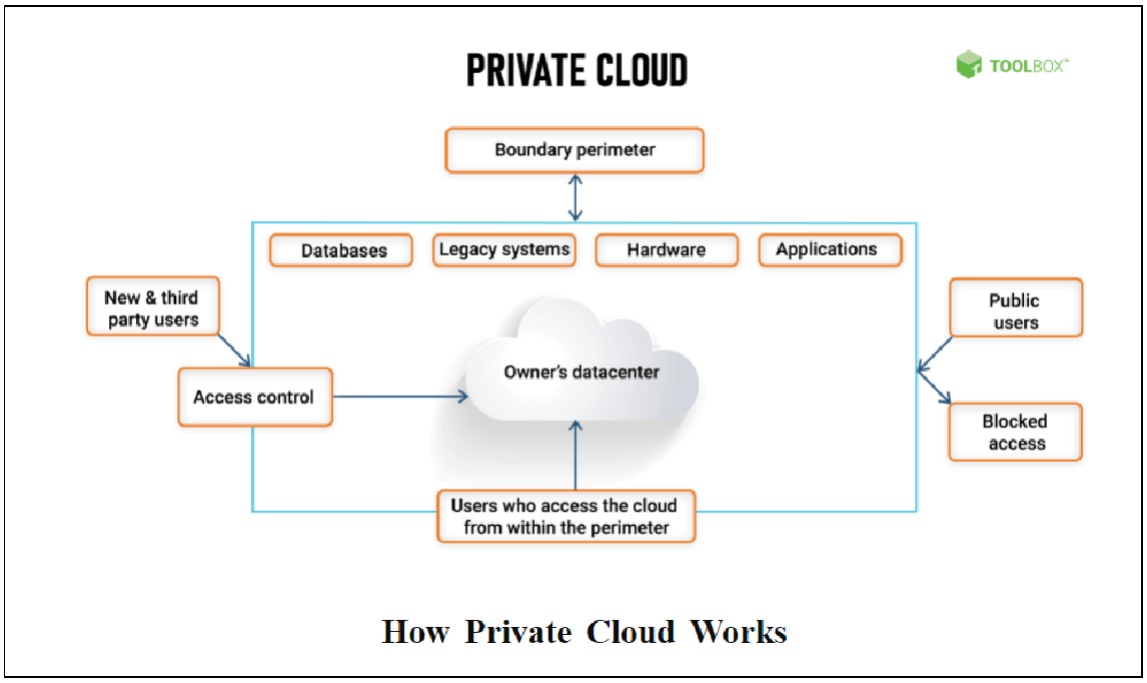
  The digital signature algorithm (DSA) refers to a digital signature standard. The National Institute of Standards and Technology (NIST) introduced it in 1991 as a

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. Rather, it uses unique mathematical functions to create a digital signature consisting of two 160-bit numbers originating from digests of the message and the private key. DSAs use the public key to authenticate the signature, but when compared with RSA, the authentication process is more complicated.

- Triple Data Encryption Standard (3DES)

  3DES is based on the DES algorithm. Making use of Triple-DES makes it 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.

5. Diagramatic representation of Data storage security in private cloud



How Private Cloud Works

6. Conclusion

We studied and learnt about data storage security in the private cloud and the different security algorithms which are in place.