A SURVEY ON SECRET IMAGE SHARING SYSTEM CONCEPTS AND METHODOLOGY

Supervised by
Dr. Bashar M. Nema

Written by
Maha Ali Hussain and Ali Manji Naji

Table of contents:

Introduction

Because it allows for data sharing capabilities to be shared across a network, the cloud provides several benefits to users. Cloud computing is now being used for saving and collaboration by IT firms and other industries. The cloud provides storage area based on the needs of the individual and their enterprise.

Cloud storage allows users to upload and download images, videos, and other types of material to and from the cloud. They can gain access to such information from any location in the world at any time via cell devices or personal computers.

When it comes to storing and exchanging information in the cloud, security is the number one concern. Users want their data to be protected so that it cannot be accessed by anyone other than the intended recipient(s). Therefore, encryption techniques are used to safeguard user data from being intercepted or accessed by third parties without the user's permission. When data is encrypted, it is converted to an encrypted format known as ciphertext, and when data is decrypted, it is converted back to its original form known as plaintext

Cryptography made use of three different sorts of algorithms to ensure data security are listed below:

1. Hash Functions (HF): HF ensures that messages transmitted with other clients are neither manipulated or tainted with viruses.

2. Symmetric Key Algorithms (SKA): Symmetric key cryptography is any cryptographic algorithm that is based on a shared key that is used to encrypt or decrypt text/cyphertext.

3. Asymmetric Key Algorithms also known as public-key cryptography: is a process that uses a pair of related keys -- one public key and one private key to encrypt and decrypt a message and protect it from unauthorized access or use.

2. CLOUD COMPUTING ARCHITECTURE

Cloud Computing (CC) offers a versatile foundation for storing information, records, and applications throughout the system. It allows several users to share to and access tasks simultaneously while requiring them to use the same OS, browsers, or application.

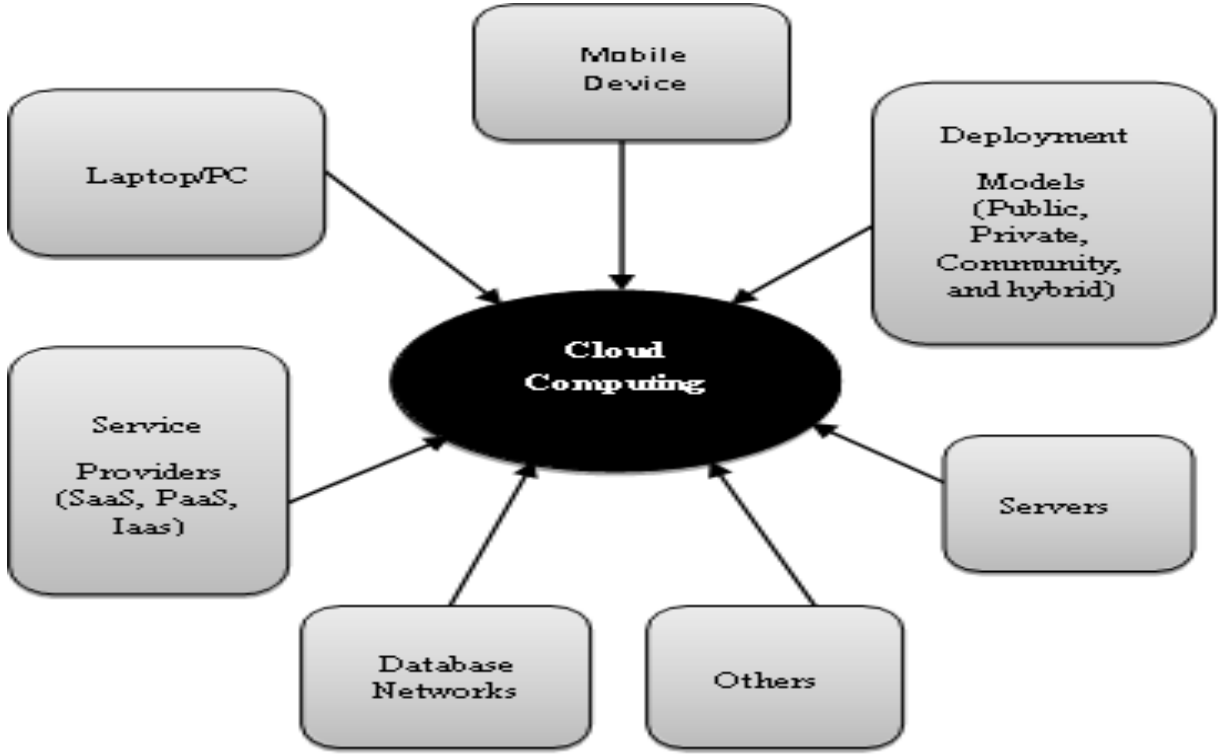

Figure 1: Architecture of Cloud Computing

Cloud computing is founded on two models: customer interface and service model. Models are the building blocks of cloud computing [3]. The multiple service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). In this sort of approach, cloud service providers give all of their services to a bunch of alternative customers.

- SaaS (Software as a Service): the user gets the complete type of software when he asks service from the provider. The service is provided to multiple users at the same time by a specific instance of the service running on the network, according to this paradigm. SaaS is now offered by a wide range of corporations, like Google, Microsoft, Zoho, Salesforce, and others, as well as by individuals.

- PaaS (Platform as a Service): To deliver a PaaS service, the supplier must just give the user with a software platform or a special type of technology. The user can design his as well as her own increased interest program or service from scratch. It is driven by the platform's service providers. The primary requirements of every application are manageability and scalability.

Examples include the LAMP system (PHP, Ruby, MySQL, Linux, and Apache), and other programming languages. Currently one of the main, Windows Azure, and Google's App Engine are just a few of the well-known instances of cloud computing.

- IaaS (Infrastructure as a Service): Infrastructure as a Service (IaaS) is an abbreviation for Platform as a Service. As part of the Infrastructure as a Service model, network operators offered additional storage and processing capabilities to a variety of clients on a subscription basis. To satisfy the workload, computing and storage hardware are gathered and made accessible to the public in IaaS data center space through the use of the internet. The user can write his who has her own software, and have it run on the cloud infrastructure; he or she can also store his or her own apps or data in the cloud infrastructure. Amazon, cloud render farms, GoGrid, Window server, 3 Tera, and so on are examples of cloud computing services.

2.1 Deployment models

• Public Cloud - A open secured cloud storage site that is accessible to anybody with a connection to the internet. It is available to any well-known group or association that offers cloud-based services and products.

• Private Cloud - A cloud infrastructure is only accessible by a limited number of people or corporations. In cloud computing, a private cloud is a protected area where only one organization can work, and the tools charged by a private cloud are only available to that group.

• An organization's hybrid cloud is occurs when two separate clouds are used together. A cloud structure made up of two or more other clouds (public, private, or community). With a cloud infrastructure, you can join two clouds and have your data replicated to a public cloud service.

2.2 Advantages/ disadvantages of cloud

Cloud computing has numerous advantages, including, Figure 2:

1) Data backup and restoration: it is much easier to store and retrieve that data utilizing the cloud.

2) The ability for groups of people to share information swiftly and easily on the cloud via shared storage.

3) Excellent accessibility: Cloud computing enables us to access and save information from any location, at any time, in any part of the .

4) Low maintenance expenses: Cloud computing helps firms save money by lowering their equipment / software maintenance fees.

5) Mobility: Cloud computing enables us to access all cloud data from anywhere at any time using a mobile device.

6) Unlimited storage capacity: The cloud provides us with an enormous amount of storage space for storing our vital data such as documents, photographs, audio, video, and other types of media in a centralized location.

7) Data security: Cloud computing has several advanced security features and ensures that data is stored and handled in a safe and secure manner.

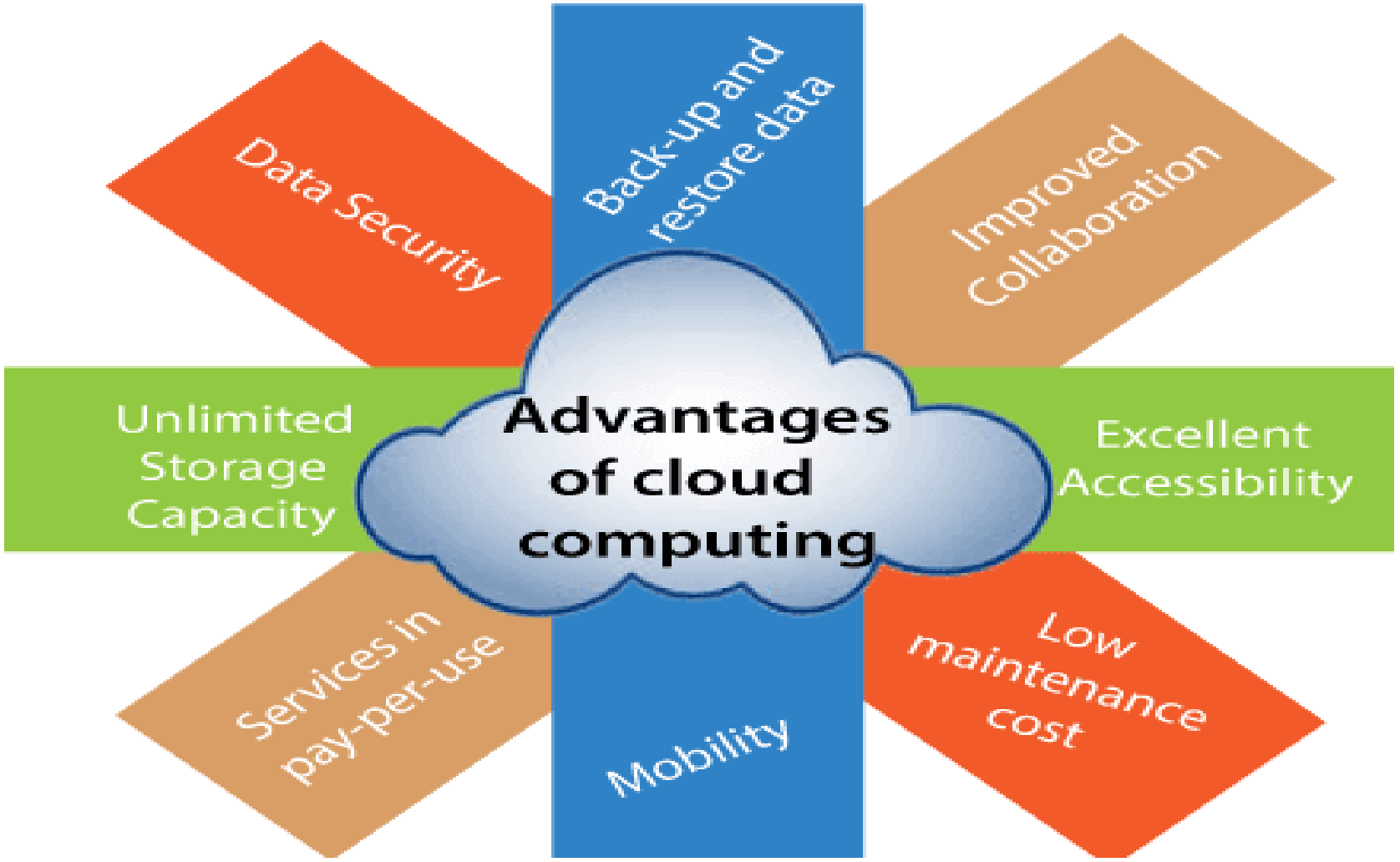

Figure 2: Advantage of Cloud Computing

2.2 Cloud Computing's Disadvantages:

1) cloud computing stores all data (images, audio, video, and so on) on a remote server, and we access this data through the cloud by connecting to it over an Internet connection. When you do not include reliable internet access, you will be unable to access this information.

2) Vendor lock-in: is the inability to switch vendors. When organizations shift their services from one vendor to another, they may encounter difficulties in the process.

3) Limited Control: public cloud is totally owned, maintained, and controlled by the service supplier, and as a result, cloud customers have less control over the operation and execution of services in a cloud environment.
4) Although cloud service providers adhere to the highest security standards when storing sensitive information, there is still a risk of data loss.

2.3 Applications of cloud

Cloud computing applications is utilized in a variety of industries ranging from small to major businesses.

1. BM (Business contact management)
2. Google Docs and Google Apps are two of the most popular online services.
3. Office productivity software such as Office 365 and MS Office
4. Peachtree and QuickBooks are examples of Business Accounting Systems.
5. Online Storage management
6. Medical imaging and emergency care for patients
7. Business-to-business apps
8. Application for communication and collaboration
9. Email and Instant Messaging Programs
10. Customer Relationship Management software.

4. ALGORITHMS FOR ENCRYPTION

a. (Advanced Encryption Standard): They both use the same key. AES is one of the SKA algorithms. This method uses a key for encrypting and decoding. An arbitrary number of bytes can be used to represent a data block. Each block size is 16 bytes long. This is a 44 array. The State is a 4 x 4 array. All AES internal activities run on these States. This method is also iterative, with each round denoting a round. The total rounds for 128, 192, and 256-bit encryption are 10.

a. DES (Data Encryption Standard): is a frequently used cryptography scheme. IBM created this technology in the 1970s, and NIST bought it. The block Cipher Algorithm was created to encode and decode 64-bit data blocks. This method uses the 64-bit key. The input key for DES is 64 bits long, however it is basically 56 bits. DES converts plain text to cipher text in 16 iterations. DES converts 64-bit input to 64-bit output in stages. The receiver side decryption uses the same processes and a similar token.

c. 3DES (Triple Data Encryption Algorithm): 3DES was built to fix vulnerabilities in the DES algorithm without having to redesign the entire cryptosystem. DES uses a 56-bit key, that is enough to safeguard personal or corporate data. 3DES uses an EDE (Encrypt-Decrypt-Encrypt) three-key mode. 3DES triples the key length and uses a 168-bit key, almost double the length of a 56-bit key. It uses K1, K2, and K3 as 64-bit keys. The K1 key encrypts the items, the K2 key decrypts them, and the K3 key re-encrypts them.

d. RSA (Rivest-Shamir-Adleman) :Encrypts data blocks, digital certificates, and secure key . With this method, the key length is flexible. It employs number theory to generate public and private keys using two prime integers. These keys encrypt and decrypt data. The RSA procedure has three essential stages. The first generates keys, the second encrypts data, and the third decrypts it. However, this algorithm's design flaws make it unsuitable for business use. Using low RSA values weakens the encryption process, while using high values wastes time and slows down performance. Utilizing side channel techniques or probability sampling theory, anyone with a small key distribution value can encrypt and decrypt.

DIFFERENT ENCRYPTION ALGORITHMS

	Symmetric Encryption	Asymmetric Encryption
1	A single key is used to encrypt and decrypt data.	A key pair is used for encryption and decryption. These keys are known as public key and private key.
2	As it uses only one key, it’s a simpler method of encryption.	Thanks to the key pair, it’s a more complex process.
3	Symmetric encryption is primarily used for encryption.	Asymmetric encryption ensures encryption, authentication, and non-repudiation.
4	It provides faster performance and requires less computational power compared to asymmetric encryption.	It’s slower than symmetric encryption and requires higher computational power because of its complexity.
5	Smaller key lengths are used to encrypt the data (e.g., 128-256-bit length).	Usually, asymmetric encryption methods involve longer keys (e.g. 1024-4096-bit length).
6	Ideal for applications where a large amount of data needs to be encrypted.	Ideal for applications where a small amount of data is used by ensuring authentication.
7	Standard symmetric encryption algorithms include RC4, AES, DES, 3DES, and QUAD.	Standard asymmetric encryption algorithms include RSA, Diffie-Hellman, ECC, El Gamal, and DSA.

6. UPLOADING IMAGE IN CLOUD

Mobile devices are used to upload images to the cloud. The speed at which images/files are uploaded and downloaded is determined on the transmission rate used by the user. Different networks have varying upload/download data rates and speeds.

7. SECURE CLOUD SHARING WITH CRYPTOGRAPHY

the original image is supplied into the encryption process. The image is subjected to encryption techniques, which conduct substitution and different changes. This key is a certificate authority that is used to turn an actual image into an encrypted image using the cipher (encrypted) image conversion algorithm. The image is encrypted and uploaded to the cloud, where it can be shared with other customers. The encrypted image is decrypted at the receiver using side decryption. The encrypted image is subjected to a decryption process. The cipher image is converted into a main image in this procedure, which is the inverse of encryption.

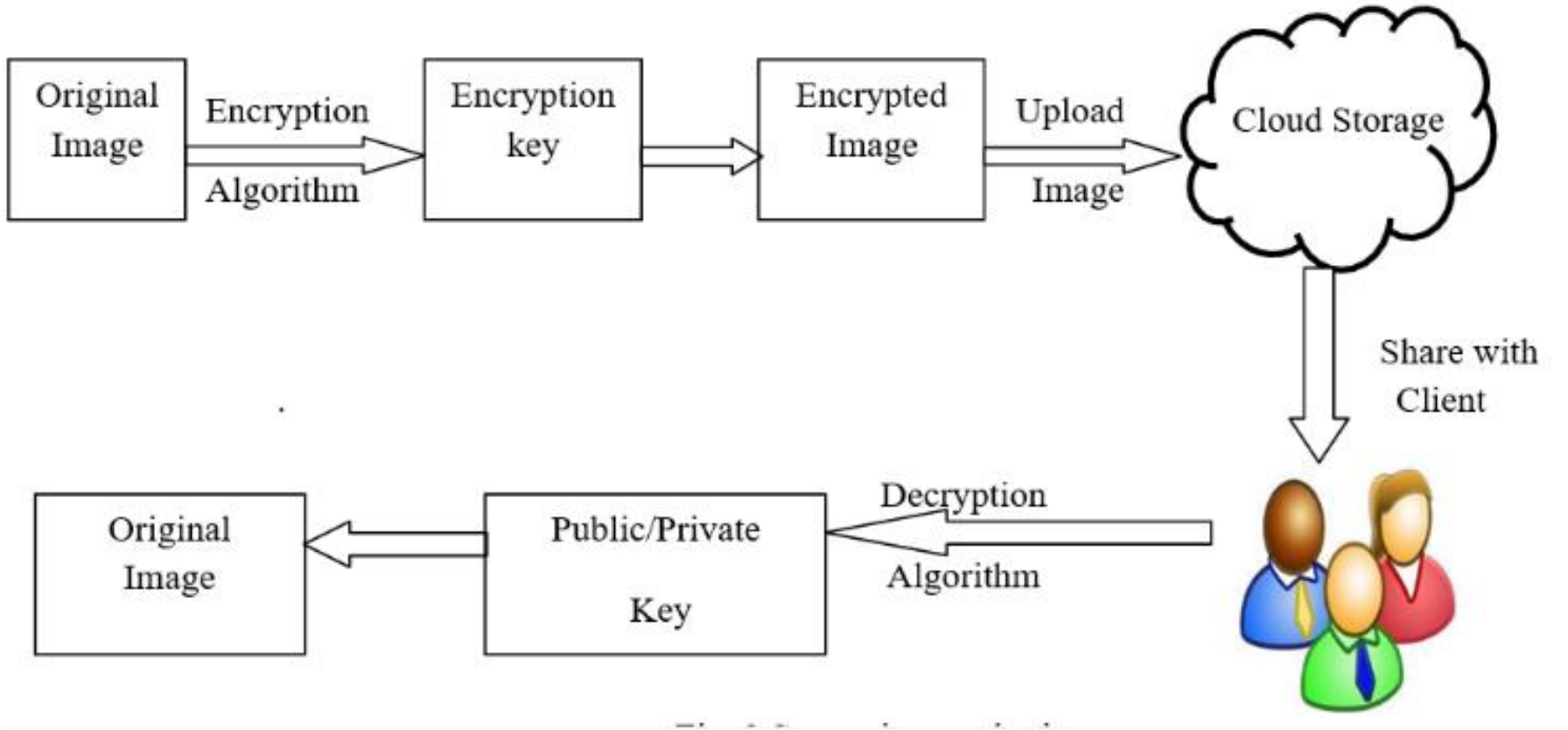

Figure 2 Secure image sharing

thank you for your listening