Cloud cryptography Literature review

A significant distributed computing approach that is fueled by economies of scale is cloud computing. It brought together a variety of resources, including computing power, storage, There are several risks connected to the cloud network, such as the possibility of unlawful data hacking. When data is being transferred, a third party may intercept it and alter it.{6} Data integrity, data availability, data confidentiality, privacy, transparency of data, and control over where data sits are the primary concerns in terms of cloud data security. cryptography method is the process to encrypt and decrypt data to overcome security issues.

{3} Cryptography is the process of converting ordinary plain text into unreadable text and vice-versa. It is a way of storing and sending data in a way that only the intended recipients can access it. Cryptography can be used for end user authentication in addition to data protection from modification. Cryptography before the modern age was synonymous with encryption, the conversion of information from a readable state to something unreadable (SSC) Based upon mathematical concepts and calculations data may secure. Cryptography security divided into 4 types as per paper (SSC).

{2} Cloud cryptography can be classified into two types one is symmetric and second one is asymmetric encryption algorithm. {1} Symmetric key cryptography is a type of encryption technique where messages are encrypted and decrypted using the same secret. Such a method of information encoding has been frequently utilized in the past for a very long time to enable covert communication. In order to improve data security, symmetric key methods are now widely used in many laptop designs. For both encryption and decryption, only one key will be utilized. {5}IN Asymmetric key, a wide public key cryptography method Two keys may be used in cryptography: a backup key for decoding and a primary key for encryption (the public key) (private key). the final public key, which has a private key that is only known to the owner and is accessible to all users. Asymmetric encryption uses a lot of energy during its operation, therefore while it does not have key distribution issues, it is slower than symmetric encryption.

Symmetric and asymmetric key further subdivided according to encryption types.

**Symmetric Encryption Algorithm (Secret Key Cryptography) can be classified into further steps.** Symmetric encryption methods are built on the concept of a separate key shared by two or more parties. The same key is used to encrypt and decrypt the so-called "plaintext" (which represents the message or piece of information that is being encoded). Data is encrypted using a technique known as a cipher, which produces an output after passing a plaintext (input) through it.

**Advanced Encryption Standard (AES)** It is a National Institute of Standards and Technology specification for electronic data encryption (NIST). It also helps to encrypt digital information, such as financial, governmental, and telecommunications data. US federal agencies use the delicate, unclassified materials. The AES symmetric key technique employs a single key that can be used for both encryption and decryption. Encryption follows as the block size is 128 bits, and the key sizes for AES-128, AES-192, and AES-256 are 128, 192, and 256 bits, respectively. A symmetric algorithm called blowfish is intended to take the place of the DES or IDEA algorithm. Data encryption and decryption are accomplished using the same secret key.

Further Asymmetric Algorithm can be classified into as follows. Rivest Shamir Adleman (RSA) Algorithm as The term "RSA" refers to a public-key cryptosystem for Internet-based encryption and authentication. Modular arithmetic and fundamental number theories are used by RSA to do calculations involving two enormous prime numbers. A variety of products, platforms, and businesses use the RSA system extensively. This encryption standard is one of the de facto ones. A few companies that use RSA in their operating systems include Novell, Apple, and Microsoft. Elliptic Curve Cryptography (ECC), ECC is a modern public-key cryptographic technique developed to avoid the abuse of cryptographic keys. The asymmetric cryptosystem makes use of number theory and elliptic curves in mathematics to produce a short, quick, and reliable cryptographic key (algebraic structure). It has been proposed that the ECC method should replace the RSA technique due to the small key size of the ECC.

{4}Cloud cryptography can be used by some users they are Alibaba Cloud Security Eco system, The infrastructure and platform for cloud services are secured by Alibaba Cloud. The security model used by shared security responsibility differs slightly from the standard security paradigm used by on-premises data centers. Customers can take advantage of the capabilities and underlying security assurance that Alibaba Cloud offers, resulting in a higher total security return.,

Microsoft: With every new version of the Windows operating system, Microsoft offers certificates for the underlying cryptographic modules used in our cloud services. {7}Google: With the help of Google Drive, we can save our private files in the cloud. The TLS (Transport Layer Security) standard is used by Google Drive to encrypt data even before it leaves the device. After that, it is uploaded to the drive.

The data is first decrypted and then re encrypted with 256-bit AES when it reaches Google (Advanced Encryption Standard).

, {7}G-Suite: Whether it is moving within Google as it switches from one data center to another, or when it is going over the Internet between the client and Google, Google encrypts core G Suite data while it is still "in transit." Between Google and the consumers, they use HTTPS to encrypt this data with security and forward secrecy., IBM: To protect data and operate, BM employs Hyper Protect Crypto Services. A complete range of encryption and key management services are available through IBM Cloud Hyper Protect Crypto Services for security-related needs., Amazon will be classified into some more categories like encryption, decryption and permission checker.

Conclusion: In this paper we got to know that what is cloud computing and how it be classified and also mentioned about different types of deployment models. Based upon issues how cryptography is used to enhance cloud data security and how it is classified. Paper mentioned how cloud cryptography used by users in real time.

Anyhow data privacy is the concern for provider and user, as to enhance system to overcome data lost

Reference:

1. <https://www.researchgate.net/publication/261201256_Use_of_cryptography_in_cloud_computing>
2. <https://www.researchgate.net/publication/351991473_Cloud_Cryptography_-A_Security_Aspect>
3. <https://www.researchgate.net/publication/332014709_CLOUD_CRYPTOGRAPHY_TECHNIQUES_USED_BY_COMPANIES>
4. <https://www.researchgate.net/publication/354968072_SECURING_CLOUD_WITH_CRYPTOGRAPHY>
5. <https://www.researchgate.net/publication/348460397_A_Review_on_Cryptography_in_Cloud_Computing>
6. <https://www.researchgate.net/publication/348548524_CRYPTOGRAPHY_IN_CLOUD_COMPUTING_FOR_DATA_SECURITY_AND_NETWORK_SECURITY>
7. <https://www.researchgate.net/publication/348674997_A_study_on_Role_and_Applications_of_Cryptography_Techniques_in_Cloud_Computing_Cloud_Cryptography>

.