International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cloud Cryptography: A Glance at Its Development

Shikhar Singh[1], Mahendra Sharma[2], Shreyansh Chaudhary[3], Parth Jain[4], Suraksha Shetty[5]

[1,2,3,4,5]Students, Jain University

Abstract
The use of encryption methods to safeguard data that is processed or stored in the cloud is known as cloud cryptography. As it helps to prevent unauthorized access, disclosure, modification, or destruction of data, it is a crucial security mechanism for cloud computing. The field of cloud cryptography is complicated and developing. It's critical to stay current with the most recent cryptographic methods and protocols as new threats and weaknesses appearCloud security includes cloud cryptography, which is crucial. Organizations can safeguard their data from unauthorized access, modification, and destruction by utilizing encryption techniques.

Keywords: AES, DES, 3DES, HOMORPHIC ENCRYPTION, FEDERATED LEARNING, HASHING

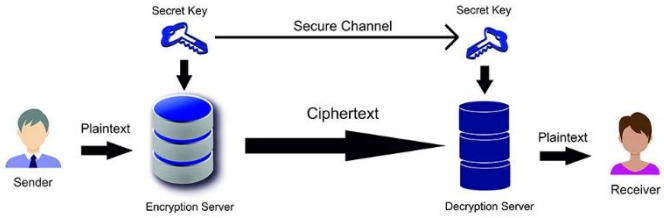
1. INTRODUCTION

Cloud cryptography refers to the use of cryptographic techniques to secure data and communications in cloud computing environments. As data is increasingly being stored and processed in the cloud, it is crucial to protect it from unauthorized access and potential breaches. With cloud cryptography, sensitive information is encrypted before it is stored in the cloud. This ensures that even if a breach occurs, the data remains secure and unreadable to unauthorized individuals. Encryption algorithms like AES (Advanced Encryption Standard) are commonly used to protect data at rest. There are different cryptographic algorithms :-

Symmetric Cryptography →The same key is used for both the encryption and decryption of data in symmetric cryptography, usually referred to as secret-key cryptography. This means that in order to encrypt and decrypt the information, both the sender and the recipient need to possess access to the same confidential key. A mathematical approach and a secret key are used to encrypt the initial plaintext in symmetric cryptography in order to create the ciphertext. The data is encrypted into ciphertext, which makes it difficult for people without authorization to access or decipher.
The immediateness as well as efficiency of symmetric cryptography is one of its primary advantages. In comparison to asymmetric cryptography, symmetric cryptography's algorithms are typically faster. This makes it perfect for real-time communications when speed is a necessity or for encrypting massive volumes of data.

Key management, however, is a serious drawback of symmetric cryptography. Sharing the secret key securely between the sender and recipient becomes challenging because the same secret key is used for both encryption and decryption. Unauthorized access to encrypted data may come from the jeopardizing of the key.

Secure key distribution techniques, which includes leveraging secure channels or asymmetric cryptography to securely share the secret key, are frequently used to address this issue of security.



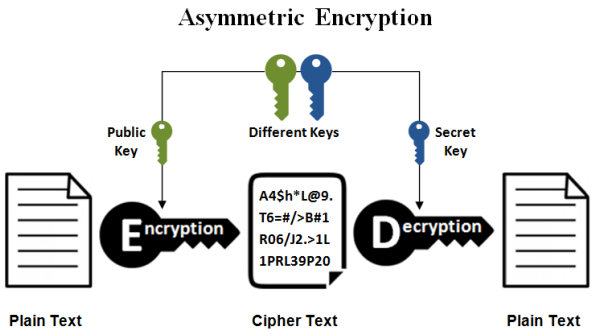
Symmetric Cryptography

Asymmetric Cryptography →Asymmetric cryptography, commonly referred to as public-key cryptography, is a cryptographic technique that encrypts data and communications using a set of two keys: a public key and a private key. Asymmetric cryptography uses two separate keys with a mathematical link between them, in contrast to symmetric cryptography, which uses the same key for both encryption and decryption.

In asymmetric cryptography, the private key is kept private and only the owner is aware of it; in contrast, the public key is freely disseminated and widely dispersed. While the private key is required for decryption, the public key is utilized for encryption.

The recipient's public key is used to encrypt the message when someone wishes to send them a secure message. The only way to decrypt a message once it has been encrypted is with the recipient's private key. Asymmetric cryptography has numerous potential benefits. One significant benefit is that anyone can freely share and use the public key, enabling secure communication with numerous parties without the requirement for a prior key exchange. As the private key is kept private and is not shared, it also does away with the necessity for a secure key distribution mechanism.

Asymmetric cryptography is slower and less effective than symmetric cryptography since it requires more calculation. It is frequently used in conjunction with symmetric cryptography because of this. For instance, symmetric keys are frequently transferred safely via asymmetric cryptography so as to encrypt huge volumes of data.

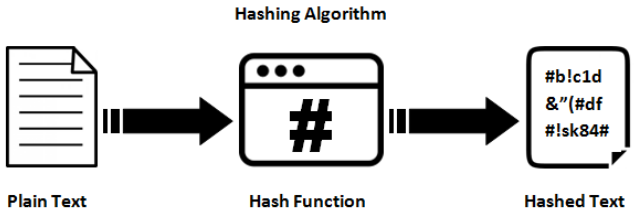


Hashing Cryptography→ Cryptographic hashing, sometimes referred to as hashing, is a technique for converting data into a fixed-size output known as a hash value or digest. It is computationally impossible to recover the original data from the hash value because this process is irreversible. Hash functions are intended to be quick and effective, generating distinct hash values for various inputs.
In hashing cryptography, the output hash value is always a defined length, regardless of the amount of the input data. The hash value is produced by the hash function using the input data as input and performing intricate mathematical calculations. The hash value will be entirely different if the input data is even slightly altered.

Digital signatures, password storage, and data integrity checking are all common uses for hash cryptography. Following are a few typical applications:

1. Data Integrity: Data integrity can be checked via hashing. You may verify that the data has not been altered by comparing a file's or message's hash value before and after transmission.
2. Password Storage: In many systems, hash values rather than the passwords' original form are used to store passwords. The user's password is hashed and compared against the hash value that has been previously stored. This adds an extra layer of security because the original passwords cannot be easily acquired, even if the hash values that are saved are hacked.
3. Digital Signatures: Digital signatures depend heavily on hashing. Data that has to be signed is hashed, and the hash value is encrypted using the signer's private key to establish a digital signature. After decrypting the hash value with the signer's public key and comparing it to the hash value of the received data, the recipient can then confirm the digital signature.

While hashing cryptography offers integrity and verification, it does not offer confidentiality, and this is a crucial distinction to make. Since hash values are often regarded as public knowledge, the actual data is not shielded from access or reading.



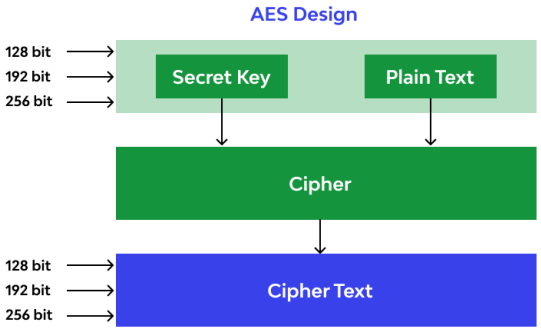
2. DIFFERENT ENCRYPTION ALGORITHMS

Advanced Encryption Standard → Widely used symmetric encryption technique The Advanced Encryption Standard (AES) offers high security for safeguarding sensitive data. The Data Encryption Standard (DES) was chosen as its replacement by the National Institute of Standards and Technology (NIST) of the United States in 2001.

AES encrypts and decrypts data using a symmetric key and works with fixed-size blocks of data, usually 128 bits. It works with keys that are 128, 192, and 256 bits long, providing greater security. The key is used to conduct a number of mathematical operations on the input data, such as substitutions, permutations, and bitwise operations.

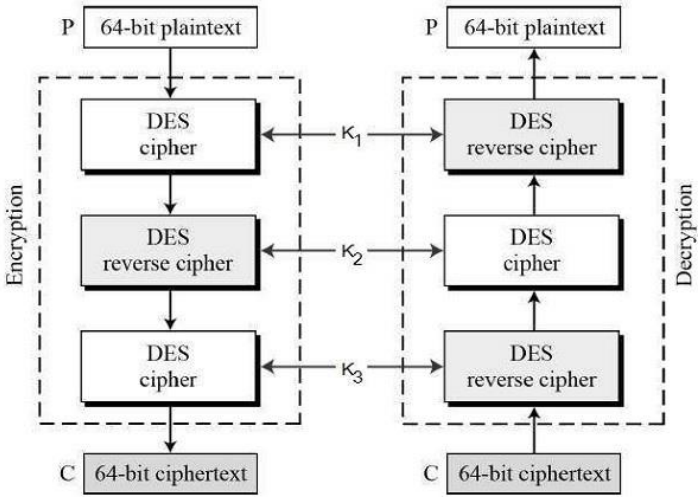
The robustness of AES to different cryptographic assaults is one of its main advantages. The cryptography community has examined it thoroughly, and it has turned out to be extremely secure when used properly. AES is widely used in many applications, including secure communications, data storage, and financial transactions. It has been accepted as the encryption standard by numerous organisations.

AES is thought to be computationally effective, making it appropriate for hardware as well as software applications. It provides strong encryption while using the least amount of processing power and system resources, striking a fair balance between security and performance.



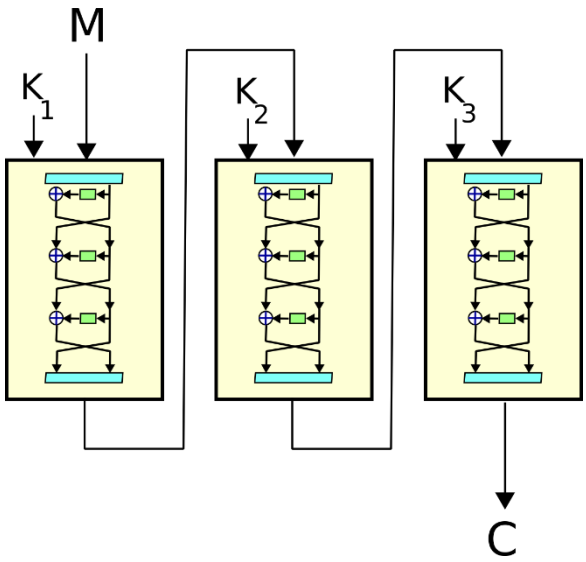
Data Encryption Standard :- An encryption method that has been around since the 1970s is called the Data Encryption Standard (DES). It was initially created by the National Bureau of Standards in the United States, which is now known as the National Institute of Standards and Technology, to protect sensitive data from unauthorised access

The symmetric key algorithm utilised by DES makes use of the same key for both encryption and decryption. In order to scramble the data into an unreadable form, it operates on blocks of data that are typically 64 bits in size. Because of the amount of its keys and the complexity of its encryption algorithm, DES is able to offer a high level of security. As processing power increased over time, DES became more vulnerable to brute-force attacks. The Advanced Encryption Standard (AES), which was created in reaction to this, replaced DES. AES is the favoured option for the majority of applications nowadays since it provides a greater level of security and efficiency.



3DES → The Triple Data Encryption Standard algorithm is an improved version of the Data Encryption Standard (DES) algorithm. It was created to offer a higher level of security and fix the flaws in the first DES. Three consecutive applications of the DES method utilizing different encryption keys are known as 3DES. The length and complexity of the key are greatly increased throughout this procedure, making it more resilient to brute-force attacks. A stronger and more secure encryption procedure is offered by the three encryption iterations.

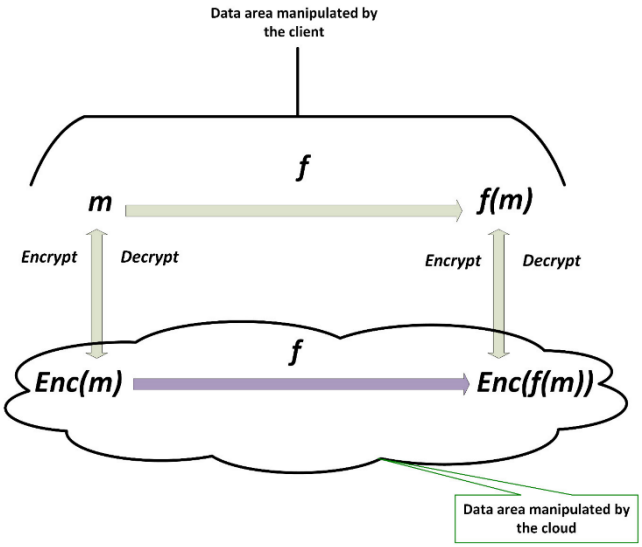
A separate encryption key, typically 56 bits long, is used for each cycle of 3DES. As a result, 3DES has an effective key length of 168 bits, giving it a substantially wider key space than DES. 3DES is backward compatible with DES, it can be used with systems and program that currently employ the earlier encryption standard. For businesses looking to improve security without totally replacing their current infrastructure, it offers a workable upgrade path. It's important to keep in mind, too, that 3DES is thought of as being somewhat slow in comparison to more recent encryption algorithms, such the Advanced Encryption Standard (AES). AES has consequently emerged as the top option for many applications that demand quick and reliable encryption.



What are the future technologies being built for Cloud Cryptography?

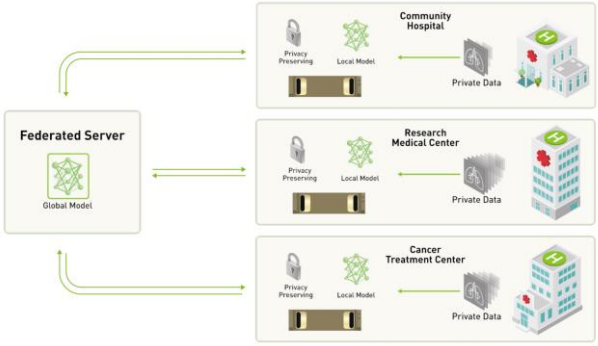
HOMOMORPHIC ENCRYPTION→ A sophisticated encryption method called homomorphic encryption enables computations to be done on encrypted data without the requirement for decryption. In other words, it makes it possible to manipulate and analyze encrypted data without revealing the plaintext underneath. Due to this characteristic, homomorphic encryption is a potent instrument for preserving the secrecy of sensitive data and safeguarding individual privacy.

Data exposed to potential security issues by traditional encryption techniques that demand decryption of the data before computation or analysis. On the other hand, homomorphic encryption enables operations like addition, multiplication, and comparison to be carried out directly on encrypted data.



FEDERATED LEARNING→ Federated learning is a decentralised method of developing machine learning models that enables a number of devices or entities to work together to extract knowledge from local data without sharing it centrally. Data is frequently gathered from numerous sources and centralised in classical machine learning in order to train a model. However, by keeping the data local, federated learning hopes to overcome issues with data security and privacy.

In a federated learning environment, each device or entity, such as smartphones, edge devices, or distributed servers, conducts training locally using their own data. Only the model parameters or updates are sent back and forth between the devices and a central coordinating server, as opposed to data. In this manner, the unprocessed data stays on the devices, guaranteeing privacy and data confidentiality.



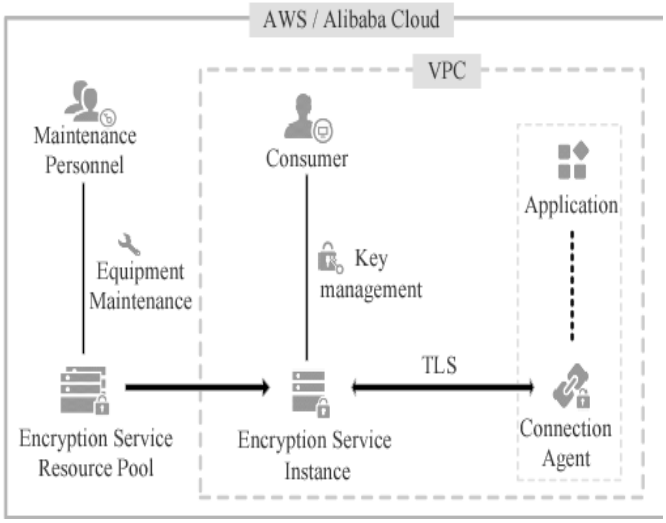
The updated global model is created by the central server by combining the model updates from the participating devices. The approach iterates until the intended model performance is attained before delivering the global model back to the devices to undergo further local training. The model may take into account the integrated understanding of all the devices thanks to this collaborative learning while likewise preserving data privacy.

Federated education provides plenty of benefits. The first benefit is improved privacy because there is less chance of data breaches or unauthorised access because the data never leaves the devices. Second, it

permits training on a variety of data sources, which can result in models that are more reliable and representative. Additionally, federated learning can reduce bandwidth utilisation and increase efficiency.

CONCLUSION→ In conclusion, cloud cryptography is essential for protecting data and communications in contexts that use cloud computing. Sensitive data can be protected from unauthorised access and potential breaches by using cryptographic techniques like symmetric cryptography, asymmetric cryptography, and hashing cryptography. The frequently used symmetric encryption methods Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple Data Encryption Standard (3DES) provide varied degrees of security and effectiveness.

The continued development of cutting-edge cloud cryptography solutions will be essential in assuring data privacy, secrecy,and integrity in the digital era as cloud data storage and processing grow more widespread. These developments will be crucial in solving new security concerns and making cloud-based services efficient and safe for people and businesses all around the world.



REFERENCES

1. K. Stanoevska-Slabeva, T. Wozniak Grid and Cloud Computing-A Business Perspective on Technology and Applications Springer-Verlag, Berlin, Heidelberg (2010)
2. National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.
3. E. Naone, Technology overview, conjuring clouds, MIT Technology Review, July–August, 2009.
4. Zhang Y, Qin RW, Shen YC. The application of cryptography resource system in cloud computing [J]. Journal of Information Security Research. 2016;2(6):558-61..
5. Cyber Chief Magazine, Cybersecurity 2020 Top Trends Shaping Management Priorities, Ed 8.
6. Douglas R. Stinson, Cryptography: Theory & Practice, Chapman and Hall Publications.
7. Joseph Selvanayagam1, Akash Singh2, Joans Michael ,Jaya Jeswani,Secure File Storage on cloud using cryptography: (IRJET),2018 [2].
8. Sarojini, G. & A, VIJAYAKUMAR &Selvamani, K.. (2017). Trusted and Reputed Services Using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud. Procedia Computer Science. 92. 506-512. Mezzovico, Switzerland.

9. S. Lei, Wang Ze-wu, “Research and Design of Cryptography Cloud Framework,” IEEE. 2018
10. G. L. Prakash, M. Prateek and I. Singh, ’Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System’, International Journal Of Engineering And Computer Science vol. 3, issue 4, pp. 5215- 5223, April 2014