IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 3, June 2022

Impact Factor: 6.252

A Review on Cryptography: Solution using Cloud

Farsana Hussain[1] and Reghunath[2]

Santhigiri College of Computer Science, Vazhithala, Thodupuzha[1]

Assistant. Professor, Santhigiri College of Computer Science, Vazhithala, Thodupuzha[2]

Abstract:*Cloud cryptography is an encryption which is used to safeguard the data that is stored in the cloud. In Cloud Cryptography there is a tendency for using public and personal keys for the Encryption and Decryption of data for keep up the integrity of knowledge. Some measures are held in cloud cryptography like hacking, infringement, and infected by malware, for preventing such problems cloud cryptography secure data by adding a strong layer of protection. Cloud providers uses encryption for securing the data which is hosted, and gives permission the users to shared cloud services securely and conveniently. And also cloud cryptography assures confidential information without set back the delivery of data.*

Keywords: Cloud Computing, Cryptography, Encryption, Decryption, Cloud Security, etc.

I. INTRODUCTION

Cloud Computing is a network service which is used to connect over the internet, it used for share information, and resources. Computing services derived over the web instead of keep the files under any disk drive or local memory devices [5]. Computing services included software, networking, storage, servers and databases. The major goal and merit of using cloud by a user is that to access and store the required data which is in the cloud, and can be accessed from anytime anywhere and provide the services for low cost [1]. In cloud computing, resources unit preoccupied and virtualized from the cloud provider's IT framework and created accessibility towards client.

Cloud infrastructure provides several advantages to different core participant and cloud clients, these number of advantages the research unit access to knowledge hold on the cloud despite the flexibility, pay-on-demand basis and location and economic edges by saving the corporate from shopping for different IT infrastructure and hardware. Cloud cryptography is nothing moreover its technique for protecting confidential information and secure from the mediator [4].

II. LITERATURE REVIEW

1. Asmita A. Jagtap, Pratibha A. Tambewagh, Survey on Cloud Cryptography, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 10, Issue 5, May 2021.
2. Pawandeep Kaur, Devi Sowjanya, Jagadeesh, Indramani Sharma, CLOUD CRYPTOGRAPHY, International Advanced Research Journal in Science, Engineering and Technology, Vol. 8, Issue 4, April 2021.
3. A. JsvSai Bhargav, AdvinManhar, A Review on Cryptography in Cloud Computing, “International Journal of Scientific Research in Computer Science, Engineering and Information Technology”, Volume 6, Issue 6, November-December-2020.
4. Miss Ruchira Gajanan Mankar, Prof. Prashant P. Patil, Cloud Computing - Cryptography, Journal of Emerging Technologies and Innovative Research”, Volume 8, Issue 7, July 2021.

III. CLOUD COMPUTING

Cloud computing is mostly telling as in two different manners, one is on the basis of services and other is on the basis of cloud models.

DOI: 10.48175/IJARSCT-4918

The cloud models classify into

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud

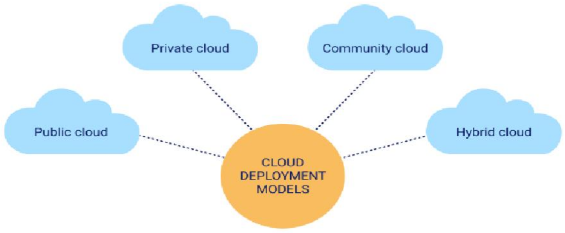


Figure 1: Cloud Models

These clouds are used on the dependency of user and business requirements.
The mostly available clouds are:

A. Private Cloud

A private cloud can be accessed by individual organization or group. It is a model which is exactly the opposite of public cloud. It preforms one to one environment for individual users. In private cloud we not want to share our hardware with any other ones. The other name of private cloud is internal cloud and have the ability to access system and services within the organization. This cloud was highly flexible and secure so that we can use this cloud over a large organization or the government sectors [5].

B. Public Cloud

A public cloud is a cloud that anyone can be very easily to access system and services. These clouds provide less secure because it is open sources for everyone. It is a shared, on-demand infrastructure and resource which is shared by the third-party provider [2].

C. Hybrid Cloud

Hybrid cloud is the combination of more than two cloud that is public cloud, community cloud, and private cloud. Organization has the ability to move application and data in between different clouds by using the combination of more than two cloud deployment techniques as their need [2].

D. Community Cloud

Community cloud can access more than two organization which contain similar cloud requriments.it is very cost-effective, shared infrastructure, flexible and scalable [2].

The services provide by the cloud computing is that are:

- IaaS (Infrastructure-as-a-Service)
- PaaS (Platform-as-a-Service)
- SaaS (Software-as-a-Service)

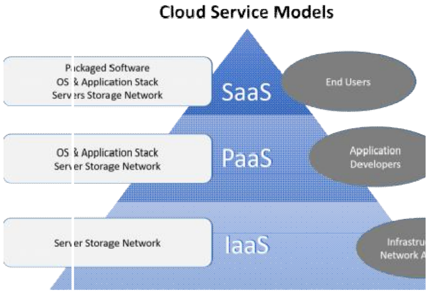


Figure 2: Cloud Service Models

A. Software-as-a-Service

SaaS, additionally called cloud software services. SaaS is controlled with the help of employing a third-party. Saas is used maximum generally utilized in commercial enterprise because of the very fact does now not require to the founded of the software at once within side the patron machine, the software is immediately run through the net browser. Some common examples of SaaS are GoToMeeting, Google Apastron machine, the software is immediately run through the net browser. Some common examples of SaaS are GoToMeeting, Google Apps [5].

B. Infrastructure-as-a-Service

IaaS presents many laptop sources, hardware, software program, and garage tool on consumer demand. IaaS customers can get the correct of entry to the provider through the utilization of the net. Some common examples of IaaS is Amazon, three Tera, GoGrid [5].

C. Platform-as-a-Service

PaaS is cloud service model which provide cloud-based platform for managing, running and developing an application. The cloud provider manages, hosts and maintain all the software and hardware included in the platform-servers, frameworks, storage, and operating system (OS), development tools as well as related services for software updates, backups and more. Some common examples of PaaS are Microsoft Windows Azure, Google App Engine etc. [5].

IV. CRYPTOGRAPHY

Cloud Cryptography is the method which is used to store the data that is stored under the cloud. The major aim of using such technique for authentication. Society moving forward with technological advancements, so the companies must secure their data from infringement, hacking and other unsecured layers. The objective of using cloud cryptography is to encrypt algorithms with mixed codes, such technique known as ciphertext [6]. The term cryptography derives from a Greek word “Kryptos,” meaning secret and “draphikos,” meaning printing. It is known as cryptography.

The cryptography can be in interactive codes, in letters, in pictures, in numerical words, or in any types of information. An example for cryptography supposes we use a plaintext for transmit a message by the sender which is decoded and that text is transmitted to the corresponding receiver after decrypted, such data transmission is refer as cipher code. These applied to the very important string of data or obscure information so that on one can easily understand but the recipient can understand. Often uses algae for transforming the plaintext into cipher text with the proper network [8]. Such mechanism is known as encryption, it is a process of translating legible and readable data into meaningless data. This algorithm is used to transforms plaintext to cipher text. It uses a key to entry in the coding algorithm and the values must be independent towards the plaintext, such entry is used to transmit the plaintext into cipher text. Different keys can be provided numerous coding text, but the opposite key can be used within the coding algorithm instead of decipherer side. There are three different kinds of cryptography methods are used to keep our data secured and protected from mediator i.e.

1. Asymmetric Key Algorithm,
2. Symmetric Key Algorithm,
3. Hash Functions [7].

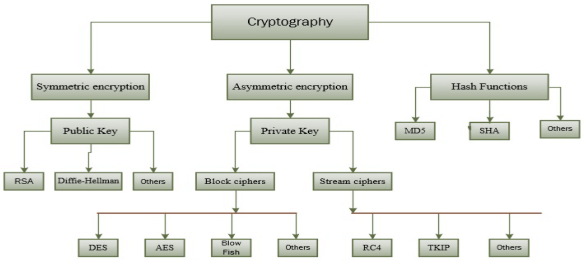


Figure 3: Diagram of Categorization of Different Cryptographic Techniques.

DOI: 10.48175/IJARSCT-4918

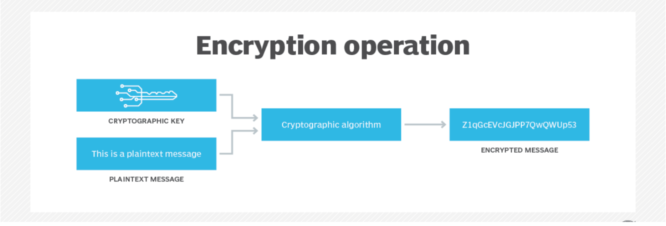
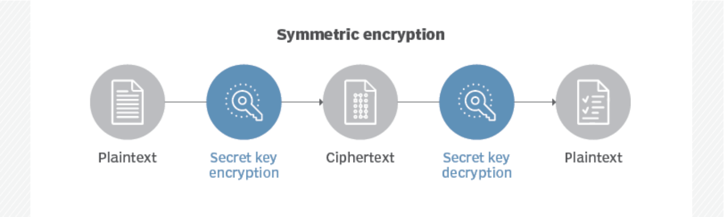


Figure 4: Diagram of Cryptography Encryption Operation

A. Symmetric Encryption Algorithm (Secret Key Cryptography)

In symmetric encryption, is a type of cryptography that refers as a private key which can perform in both encryption and decryption [8]. If anyone have the copy of the key then that person can easily decrypt and encrypt information [7]. Suppose the private key is need to transport the encrypted message in between two people, then a backup for that hidden key must be used to accessible to both the sender and receiver [8].



Figures 5: Symmetric Encryption

- **DES (Data Encryption Standard):**
  DES is an algorithm which is used for the data encryption that can generate secret key for both the encryption and decryption [4]. It was established during 1970s under the IBM team then after it accepted by the National Institute of Standards and Technology (NIST). These algorithms have the ability to take plain text in 64-bits of block and changes them into cipher-text by using 48-bits [8].

- **Blowfish:**
  Blowfish is an algorithm that designed to restore IDEA and DES algorithm, it is a symmetric algorithm. It also uses secret key for decrypt and encrypt data. This algorithm is used to divide data into large block of 64-bits and generate a key range from 32-bits to 448-bits. Due to the high speed and overall efficiency, it provides password protection tools in e-commerce for the securing payments [4].

B. Asymmetric Encryption Algorithm (Public-Key Cryptography)

In Asymmetric algorithm, process dual-key which means it uses both the private key and public key. The person who had the public key then easily sent information safely and by using private key we can decrypt it. Suppose we have only public key then it should be a one-way function because it doesn't provide same security issues as like symmetric encryption and comfortably distribute a public key [7].

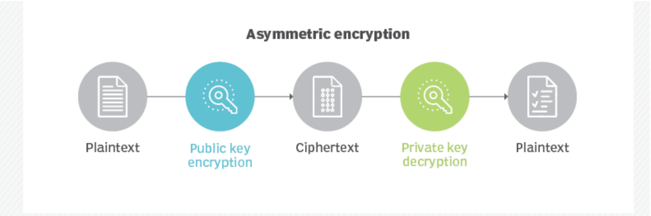


Figure 6: Asymmetric Encryption

- **Diffie Hellman Algorithm:**
  Diffie Hellman set of rules designed to generate a shared secret key for exchanging data confidentially. Diffie Hellman algorithm is used to maintain the shared secret which is used in the secret communications during the exchanging data under the public network that uses the elliptic curve for generate points and gain the secret key that used in the parameters [5]. Diffie Hellman is one of the too soon, practical examples of public key exchange conveyed out in the area of cryptography and gives the basis for a branch of authenticated protocols. For example, Diffie Hellman is used to give better confidentiality in shipping Layer safety's ephemeral modes. The algorithm make used of exponentials module calculation to generate a key, which make key secured.
- **RSA(Rivest-Shamir-Adleman):**
  RSA is the famous Asymmetric cryptographic block encryption or digital signatures or key-exchange encryption schemes. This algorithm contains both the public key and private key. It basically follow the principle of numbers, usage of public and non-public key operation of two prime numbers. For the data encryption and decryption this algorithm uses both the public and non-public keys. RSA processed into three different steps: First step for the key production, second step for encryption process and the last step for decryption process [8].
  This algorithm widely used in variety of industries, products and platforms. Many companies like Novell, Microsoft and Apple were use RSA algorithm for their operation systems. Easy to multiply two prime numbers but in the case of RSA is focus on the complexity of calculating the original number from product [4].

Step 1: Generate the RSA modulus:

The first step starts with the collection and estimation of two primary numbers, p and q and the element N, as indicated. N=p*q.

Step 2: Derived Number (e):

Find a number e to be more than one and less than (p-1) and (q-1) dependent number. The prime condition is that (p-1) and (q-1) are not normal except 1.

Step 3: Public Key

The pair of numbers n and e listed type the public RSA key and are publicly accessible.

Step 4: Private Key

Personal key d from p, q and e is determined. It is the statistical association between the numbers− ed = 1 mod (p-1) (q-1)

Encryption Formula:

Find a transmitter transmitting the basic text message to an individual with a public key (n, e). In the specified case, using the following syntax to encrypt a plain text file.
C = Pe mod n

Decryption Formula:

The method of decryption is rather straightforward and integrates measurement modelling into a structured strategy. In view of the private key d of recipient C, the outcome module is measured as − Plaintext = Cd mod n [8].

C. Hashing

In Hash function, is a type block-chain which is used to secure most critical facets. Both the separate keys are used for encrypt and decrypt the messages. It shows much faster recuperate of result [3].

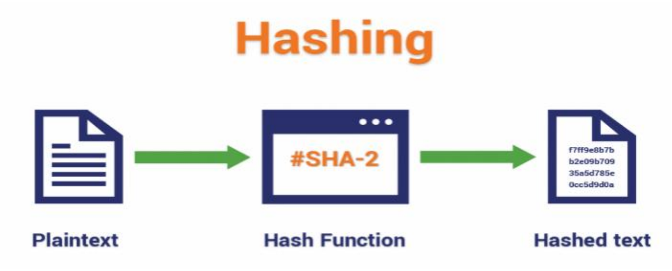


Figure 7: Hash Function

V. FINDING AND SOLUTIONS

Problem

1. **Increasing cloud threats due to improper encryption**
2. Multiple cloud threats such as unauthorized data exposure and leaks, weak access controls.
3. Susceptibility to attacks, insecure interface, account hijacking etc. adversely affects the security of the company record and details.
4. Security and compliance risk are major consideration for the company.

Recommendation

1. Implement data encryption techniques to eliminate risk of information.
2. The company can implement various data encryption methods such as AES, triple DES etc. in order to securely protect both personal and professional hackers.
3. The files and folders must be VPN encrypted keeping in need the requirements and utility of the data.

VI. CONCLUSION

The vital goal is to store firmly and access information in cloud that's not controlled by owner of info. Software structures often have a couple of endpoints, typically more than one client, and one or more are given up servers. Those customer/server communications take place over networks that cannot be depended on. Cryptography can defend communications that traverse untrusted networks. There are principal kinds of assaults that an adversary may try and perform on a community. Passive attacks contain an attacker actually listening on a community phase and attempting to examine touchy records as it travels. Passive attacks may be on-line (wherein an attacker reads traffic in actual-time) or offline (wherein an attacker without a doubt captures site visitors in real-time and perspectives it later possibly after spending a while decrypting it).

In this paper, it shows the different types of cryptographic algorithms which is used under the cloud computing. This different algorithm used for encrypt data in transition from the cloud user to the cloud provider's platform.

ACKNOWLEDGMENT

I have taken efforts in this paper. However, it would not have been possible without the kind support and help of many individuals. I would like to extend my sincere thanks to all of them. I am highly indebted to Dr. Reghunath K for their guidance and constant supervision as well as for providing necessary information regarding the paper & also for their support in completing the seminar. I would like to express my gratitude towards my parents & friends for their kind cooperation and encouragement which help me in completion of this paper.

REFERENCES

[1] Survey on Cloud Cryptography, Vol. 10, Issue 5, May 2021.

[2] https://www.geeksforgeeks.org/cloud-deployment-models/

[3] https://www.thesslstore.com/blog/what-is-a-hash-function-in-cryptography-a-beginners-guide/

[4] Cloud Computing – Cryptography, Volume 8, Issue 7, July 2021.

DOI: 10.48175/IJARSCT-4918

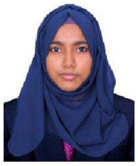
[5] A Review on Cryptography in Cloud Computing, Volume 6, Issue 6, November-December-2020.

[6] https://www.arpatech.com/blog/what-is-cloud-cryptography/

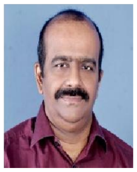
[7] https://www.techtarget.com/searchcloudcomputing/tip/Where-cloud-cryptography-fits-in-a-security-strategy/

[8] Cloud Cryptography, Vol. 8, Issue 4, April 2021.

BIOGRAPHY



Farsana Hussain, student of Santhigiri College of Computer Sciences, Vazhithala, has pursing in Master of Computer Applications. Interesting area is Cloud Computing, Cryptography, Java Technologies etc.



Dr. Reghunath K, Assistant Professor, Department of Computer Science, Santhigiri College, Vazhithala. He has got Ph.D. in Big Data securities and presented 10 more research papers in national and international seminars. Interesting area is Cloud Computing, Big Data, Networking etc.