International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206639

A Review on Cryptography in Cloud Computing

A. Jsv Sai Bhargav[1], Advin Manhar[2]
[1]Research Scholar, Amity University Chhattisgarh, Raipur, Chhattisgarh, India
[2]Assistant Professor, Amity University Chhattisgarh, Raipur, Chhattisgarh, India

Article Info
Volume 6, Issue 6
Page Number: 225-230
Publication Issue :
November-December-2020

Article History
Accepted : 05 Dec 2020
Published : 12 Dec 2020

ABSTRACT

Cloud computing is the delivery of computing services over the web instead of keeping files on a proprietary disk drive or local memory device. Computing services can include servers, storage, databases, networking, software. The main reason and great advantage for using the cloud are that the user can store and access the stored data in the cloud from anywhere anytime and getting all its services for a low cost. Despite, Security has always been a big concern with cloud computing because the information stored in the cloud is not directly maintained by the customer. When the user uploaded or stored data during a cloud computing service, the info owners are unlikely to understand the path via which their data is being transmitted. The user is unknown to the fact whether the information is being collected, analyzed, and accessed by a third party or not. To overcome the security issues various cryptography algorithm is proposed. This paper focused on the basics of cloud computing and discussed various cryptography algorithms present in the existing work.

Keywords : Cloud Computing, Cryptography, Security, Data.

I. INTRODUCTION

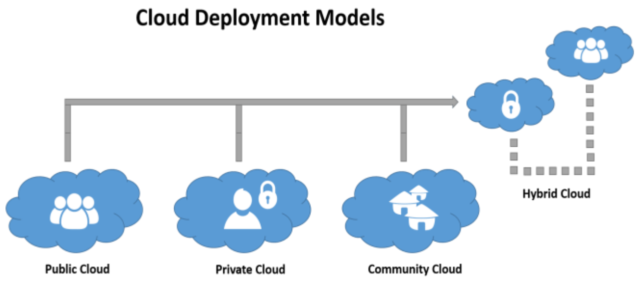
Cloud computing gives a brand new manner of offerings with the aid of using re-arranging diverse sources and supplying them to customers primarily based totally on their demands. Cloud act as a software program virtualized. It additionally performs an essential position withinside the subsequent technology of cellular networks and offerings. Storing information withinside the cloud significantly reduces the storage burden of customers and brings them to get the right of entry to convenience, hence it has emerged as one of the maximum essential cloud offerings. Cloud computing lets in the commercial enterprise person or character person to apply the utility through the net without putting in of their system. The most important gain of cloud computing is a low cost, improved storage, and flexibility.However, The foremost threat in cloud computing is safety and privateness and agree with emerging as an important difficulty that influences the fulfillment of cloud computing (i.e. With the aid of using placing the precious information on a person else's server in an unknown location. Cloud safety includes the practices and generation essential to protect cloud computing offerings from cybersecurity threats. For this, Cryptography is broadly carried out to make certain information safety, privateness, and agree with in cloud computing. But present answers are nevertheless imperfect and inefficient, hence impractical. Storing encrypted information withinside the cloud makes it tough to carry out auditing on information control even though the threat of privateness leakage is significantly reduced. This unique difficulty pursuits to convey collectively researchers and practitioners to talk about diverse factors of cryptography and information safety in cloud computing.

Cloud Computing:

Cloud computing is usually described in one of two ways. Either based on the deployment model, or on the service that the cloud is offering.

Based on a deployment model, we can classify cloud as:

- public,
- private,
- hybrid
- community cloud



Depending on the user or business need the different types of the cloud are available .

There are four types of clouds available .

Private Cloud : A private cloud can be accessed by a single group or a single organization It is managed by a third party or organization .

The private cloud is highly secure and flexibility so the private cloud is often used by larger organizations or the government sectors .

Public Cloud : A public cloud can be accessed by any user with an internet connection and want to pay as per their usage The files are hosted by a third party.

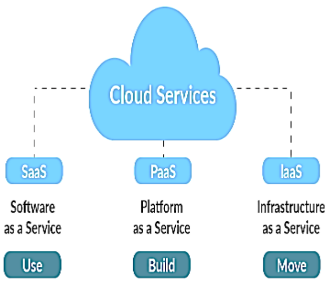
Example Amazon , window Azure Service Platform and sales force .

Community Cloud : A community cloud will be accessed by two or more organization that has similar cloud requirements

Hybrid Cloud : A hybrid is the combination of two or more cloud (public , private , and community)

Based on a service the cloud model is offering, we are speaking of either:

- IaaS (Infrastructure-as-a-Service)
- PaaS (Platform-as-a-Service)
- SaaS (Software-as-a-Service)
- or, Storage, Database, Information, Process, Application, Integration, Security, Management, Testing-as-a-service



Depending on the want of the buyer on the thanks to use the gap and sources associated with the cloud, the cloud provider issuer will provide the buyer greater or much less manipulate over their cloud. For instance: if it'll be for commercial enterprise use or non-public domestic use, the cloud want is also of assorted types. There are 3 forms of cloud that provide software program as a Service (SaaS), Infrastructure as a provider (IaaS), platform as a provider (PaaS).

1. **Software as a provider**: – SaaS, additionally called cloud software services. SaaS is controlled with the

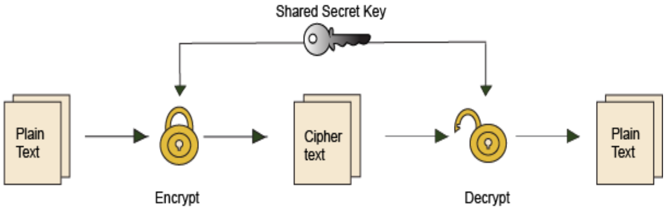
help of employing a third-party. Saas is used maximum generally utilized in commercial enterprise because of the very fact does now now not require to the founded of the software at once withinside the patron machine, the software is immediately run through the net browser . Some common examples of Saas are GoToMeeting, Google Apps

2. **Infrastructure as a provider**: – 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.

3.**Platform as a service:**– A PaaS machine goes grade better than the code as a Service setup. A PaaS provider gives subscriber's get right of entry to the weather that they require to extend and perform programs over the software. A number of the instance for PaaS is J2EE, Ruby, and LAMP.

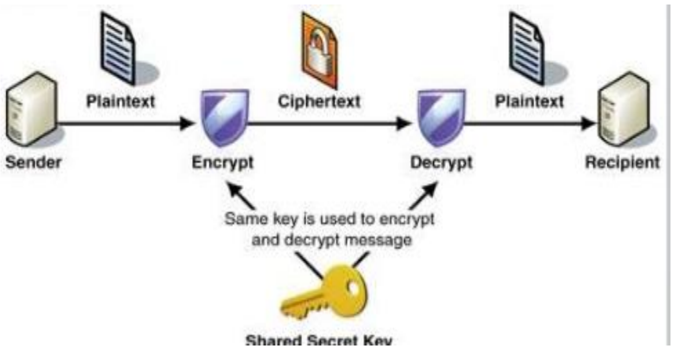
Cryptography:

Cryptography is the protective approach of information from the unauthorized party with the aid of using changing into the non-readable form. The most important reason for cryptography is preserving the safety of the information from the third party.For achieving Security in three categories: confidentiality, integrity, and availability. Cryptography mainly focusing on the confidentiality of information withinside the cloud. There are the following sorts of algorithms such as (i) symmetric key based algorithm, (ii)asymmetric key based algorithm, also called as public-key set of rules.Data cryptography is encoding the content material of the information like textual content and media to make it now no longer understandable, meaningless, and invisible all through transmission and storage, this process is called as encryption. The contrary method of retrieving the authentic records from encrypted records called decryption. To encrypt records on cloud storage each symmetric key and asymmetric key may be used, however in keeping with the bulk of the database and information saved in cloud storage the usage of symmetric key based algorithm is quicker than asymmetric key.



Symmetric key:

Symmetric key cryptography is a form of encryption scheme in which the equal secret's used each to encrypt and decrypt messages. Such a way of encoding information has been largely used within the past a long time to facilitate secret communication .These days, symmetric key algorithms are broadly implemented in different types of laptop structures to enhance data security. Symmetric encryption schemes rely on an isolated key this is shared among two or more people. The same key is used to encrypt and decrypt the so-referred to as plaintext (which represents the message or piece of information that is being encoded). The technique of encryption includes strolling a plaintext (input) through an encryption algorithm known as a cipher, which in turn generates a ciphertext (output). If the encryption scheme is powerful sufficient, the best manner for someone to examine or get entry to the statistics contained in the ciphertext is with the aid of the use of the corresponding key to decrypt it. The process of decryption is essentially changing the ciphertext back to plaintext. Symmetric encryption is also called private-key encryption and secure key encryption. It uses a private key that may both be various, a phrase, or a string of random letters. it is blended with the obvious textual content of a message to regulate the content material in a sure way. The sender and the recipient ought to understand the personal key that is used to cipher and decipher all the messages. Symmetric Key systems are faster and less complicated but the problem is that sender and receiver should interchange key in a secure way. The most popular symmetric-key cryptography structure is the data Encryption device(DES).



Encryption and decryption using the DES algorithm.

Data Encryption standard:

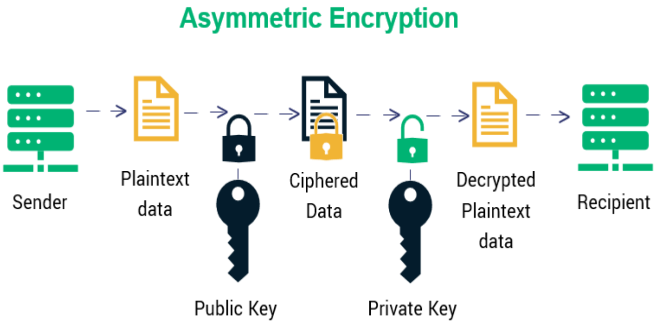
DES is that the archetypal block cipher-an algorithm that takes a fixed-duration string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the identical period. In case of DES, the block length is 64 bits. DES also uses a key to customize the transformation, so as that decryption can supposedly simplest be finished by means of who recognize the actual key used to encrypt. the important thing ostensibly includes sixty-four bits; but, the most convenient 56 of these are in point of fact utilized by the algorithm. eight bits are used totally for checking parity and are thereafter discarded. therefore the effective key period is fifty-six bits. The key's nominally stored or transmitted as 8 bytes, each with unusual parity. previous the principle rounds, the block is split into two 32-bit halves and processed alternately; this crisscrossing is noted because the Feistel scheme. The Feistel structure ensures that decryption and encryption are very similar tactics-the only difference is that the subkeys are applied within the other order when decrypting.

Diffie Hellman:

Diffie Hellman set of rules designed to generate a shared secret key for exchanging data confidentially.DH is one of the earliest, practical examples of public key exchange carried out in the area of cryptography and gives the basis for a ramification of authenticated protocols. for example DH is used to offer best forward secrecy in shipping Layer safety's ephemeral modes (referred to as EDH or DHE relying at the cipher suite) .The algorithm make used of exponentials module calculation to generate a key, which make key secured .

Asymmetric key:

The general public key cryptography could be a cryptography method that used two different keys, the primary one for encryption (public key) and also the alternative one for decryption (private key). the final public key recognized by everyone and also the private key only known by the owner. the general public key cryptography most known for system of verification, specified even one character change will cause verification to fail. The asymmetric encryption do not have key distribution trouble but slow evaluate to the symmetric encryption ,since they use an enormous amount of energy for their process.



RSA Algorithm:

The RSA algorithm is a cipher wherein the plaintext and ciphertext are integers between 0 and n-1 for some n. It makes use of exponentials, plaintext encrypted in blocks through C = Me mod n where C is the ciphertext and M the plaintext. In the same way, the plaintext is attained by using M = Cd mod n, where d is the private key.

The Main factors of RSA lie in that algorithm can be relevant for encryption/decryption, digital signature, and for the key exchange. It is the most widely used asymmetric encryption algorithm. When you encrypt with a private key, the cipher textual content can simplest be decrypted with the public key. It used for SSL/TLS (secure sockets layer/transport layer security), for protecting information, you transmit and get hold of over the internet, for example, while you do your online banking or actually log in into a website. The biggest obstacle RSA algorithm is once d is determined the cipher textual content can decrypted easily.

II. 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 give up servers. those customer/server communications take place over networks that can not be depended on. communication takes place over open, public networks including the net, or non-public networks which may be compromised via external attackers or malicious insiders.

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). energetic assaults contain an attacker impersonating a purchaser or server, intercepting communications in transit, and viewing and/or modifying the contents before passing them directly to their meant vacation spot (or dropping them absolutely).This paper has given a clear view on cloud computing and its security issues using cryptography methods.

III. REFERENCES

[1]. M. A. Vouk, "Cloud computing - Issues, research and implementations," Proc. Int. Conf. Inf. Technol. Interfaces, ITI, pp. 31–40, 2008.

[2]. P. S. Wooley, "Identifying Cloud Computing Security Risks," Contin. Educ., vol. 1277, no. February, 2011.

[3]. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.

[4]. Cloud Performance Evaluation: Hybrid Load Balancing Model Based on Modified Particle Swarm Optimization and Improved Metaheuristic Firefly AlgorithmsJune 2020International Journal of Advanced Science and Technology 29(5):12315-12331, Advin Manhar.

[5]. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[6]. V. J. Winkler, "Securing the Cloud," Cloud Comput. Secur. Tech. tactics. Elsevier., 2011.

[7]. A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, "Security risks and their management in cloud computing," 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc., pp. 121–128, 2012.

[8]. T. Mather, S. Kumaraswamy, and S. Latif, "Cloud Security and Privacy," p. 299, 2009.

[9]. F. Yahya, V. Chang, J. Walters, and B. Wills, "Security Challenges in Cloud Storage," pp. 1–6, 2014.

[10]. VijayaPinjarkar, Neeraj Raja, KrunalJha,AnkeetDalvi, "Single Cloud Security Enhancement using key Sharing Algorithm, "Recent and Innovation Trends in Computing and 2016Communication, 2016.

[11]. V. Vankireddy, N. Sudheer, R. Lakshmi Tulasi, “Enhancing Security and Privacy in Multi Cloud Computing Environment,” International Journal of Computer Science and Information Technologies, 2015.

[12]. Swapnila S Mirajkar, Santoshkumar Biradar, “Enhance Security in Cloud Computing,” International Journal of Advanced Research in Computer Science and Software Engineering,2014. 13Ashalatha R, “A survey on security as a challenge in cloud computing,”International Journal of Advanced Technology & Engineering Research (IJATER) National Conference on Emerging Trends in Technology,2012.

[13]. 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

[14]. S Mahim, “secure file storage on cloud using cryptography”, Mumbai, 03 | Mar-2018

[15]. Ahmed Albugmi Madini ,O. Alassafi Robert Walters, ” Data Security in Cloud Computing”, 2016.

Cite this article as :

A. Jsv Sai Bhargav, Advin Manhar, "A Review on Cryptography in Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 6, pp. 225-230, November-December 2020. Available at doi : https://doi.org/10.32628/CSEIT206639
Journal URL : http://ijsrcseit.com/CSEIT206639