WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cloud Cryptography

Alfiya Javed Jamadar[1], Shraddha Appasaheb Kadage[2], Shubhashri Prakash Kumbhar[3], Akshata Suresh Chougule[4], kallyani Narayan Rode[5]

Electronics and Telecommunication Department, Sharad Institute of Technology College of Engineering Yadrav, Maharashtra, India. Email: shubhakumbhar1439@gmail.com

ABSTRACT

With the net having reached a level that merges with our lives, growing explosively during the last several decades, data security has become a main concern for anyone connected to the net.. Data security ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of information. So as to realize this level of security, various algorithms and methods have been developed. Cryptography can be defined as techniques that cipher data, reckoning on specific algorithms that make the information. Unreadable to the human eye unless decrypted by algorithms that are predefined by the sender.

Keywords: Public cloud, Private cloud, Community cloud and hybrid cloud.

INTRODUCTION

Cloud computing is attracting a lot of coverage from individuals reception to the united states both in publications and among consumers. And it isn't always established specifically. Cloud computing could be a membership-a contract obsessed with which you'll get networked disk space and device services. This paper includes the fundamental concept of cloud computing technique and therefore the sorts of cloud and therefore the techniques of cloud computing, the concept of cloud cryptography and the way it's useful to us and the way it might save our data from breaches and ensures security. The paper also includes some algorithms employed in cloud cryptography and its application. It also includes the benefits and disadvantage of cloud cryptography and the way it's used beneficial to us in our future. The most aim of the research paper is to relinquish a broad way description of cloud cryptography and its benefits.

CLOUD

When you are employed within the software sector, you hear companies claiming their data is processed within the cloud more frequently than not. It may be misleading because the corporate itself wants to use terms that have little to try and do with the products themselves. The cloud relates to the info and knowledge management mechanism over the net. Simply placed, it allows you to preserve and consider data without the requirement for a tough drive on your device. In the days, the word "cloud" was seen as symbolizing the abstract wont to describe the layout of the net. If you're thinking about it, the net looks like a world web that links all people from across the world, exchanging knowledge and viewing it through a variety of networks. So, if you utilize this conceptual representation to explain the cloud, it implies exchanging and accessing knowledge over a network medium, particularly the web. Save the files on your magnetic disk will, though, have little to do with the cloud. The activity already applies to local storage and computational processes. Which implies your machine disc drive is physically next to you so as to produce access to all or any your valuable tools and records. That's how the electronics sector worked for many years. So although several companies are setting out to utilize the cloud, others also contend that the standard thanks to store data is additionally much superior.

Types of cloud: There are varieties of cloud.
They are:
1) Private
2) Public
3) Community
4) Hybrid

"Public cloud: hosted, operated and managed by the third party system owned by organization selling cloud services.

Private cloud: The private cloud infrastructure is operated for the exclusive use of a corporation. The cloud also be managed by that organization or a 3rd party. Private cloud is also on or off-premises.

Hybrid cloud: A hybrid cloud combines multiple clouds (private, public) where those clouds retain their unique identities but they're bound together as a unit.

Community cloud: Community cloud means an network built between organizations, typically with the problems of mutual storage and data protection. A gaggle cloud may belong to a single-country government, as an example. Group clouds could also be found on moreover as off premises.

CLOUD COMPUTING

Cloud storage could also be thanks to exploit the web and access on demand applications or other online services. Users share computing resources, bandwidth, disk capacity, memory, and applications. The services are shared with cloud storage, then are the cost. Users pays as they travel and use just what they have at any moment, bringing the customer down on prices. Cloud infrastructure is additionally considerably a market concept. Cloud infrastructure service vendors, whether they're applications, equipment, network, or provi ders data, distribute their offerings over the web.

CRYPTOGRAPHY

Cryptography is that the study of securing communications from outside observers. Encryption algorithms take the initial message, or plaintext, and converts it into cipher text, which is not understandable. The key allows the user to decrypt the message, thus ensuring on they'll read the message. The strength of the randomness of an encryption is also studied, which makes it harder for anyone to guess the key or input of the algorithm. Cryptography is how we will achieve more safer and robust connections to elevate our privacy. Advancements in cryptography makes it harder to interrupt encryptions in order that encrypted files, folders, or network connections are only accessible to authorized users.

Types of Cryptography

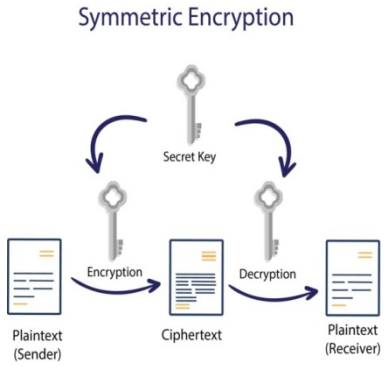
Cryptography can be broken down into three different types:

- Secret Key Cryptography
- Public Key Cryptography
- Hash Functions

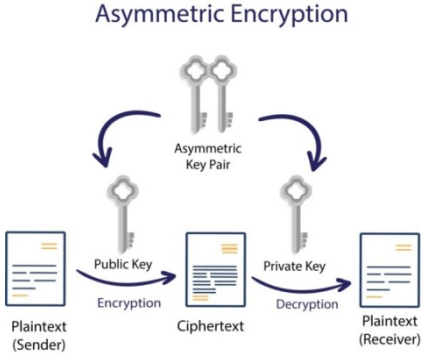
Secret Key Cryptography, or symmetric cryptography, uses one key to encrypt data. Both encryption and decryption in symmetric cryptography use the identical key, making this the simplest style of cryptography. The cryptographic algorithm utilizes the key in a very cipher to encrypt the info, and when the information must be accessed again, someone entrusted with the key can decrypt the info. Secret Key Cryptography is used on both in-transit and at-rest data, but is usually only used on at-rest data, as sending the secret to the recipient of the message can cause compromise.

Examples:

- AES
- DES
- Caesar Cipher



Public Key Cryptography, or asymmetric cryptography, uses two keys to encrypt data. One is used for encryption, while the other key can decrypts the message. Unlike symmetric cryptography, if one key is used to encrypt, that same key cannot decrypt the message, rather the other key shall be used.



One key is kept private, and is called the “private key”, while the other is shared publicly and can be used by anyone, hence it is known as the “public key”. The mathematical relation of the keys is such that the private key cannot be derived from the public key, but the public key can be derived from the private. The private key should not be distributed and should remain with the owner only. The public key can be given to any other entity.

Examples:

- ECC
- Diffie-Hellman
- DSS

Hash functions are irreversible, one-way functions which protect the data, at the cost of not being able to recover the original message. Hashing is a way to transform a given string into a fixed length string. A good hashing algorithm will produce unique outputs for each input given. The only way to crack a hash is by trying every input possible, until you get the exact same hash. A hash can be used for hashing data (such as passwords) and in certificates.

Some of the most famous hashing algorithms are:

- MD5
- SHA-1
- SHA-2 family which includes SHA-224, SHA-256, SHA-384, and SHA-512
- SHA-3
- Whirlpool
- Blake 2
- Blake 3

CRYPTOGRAPHY IN CLOUD COMPUTING

Cryptography in the cloud employs encryption techniques to secure data that will be used or stored in the cloud. It allows users to conveniently and securely access shared cloud services, as any data that is hosted by cloud providers is protected with encryption.

FUTURE SCOPE

Cloud storage protection concerns are an ongoing study and experimental area. Several issues, one of which is user data and software health, have been found. Protection of various approaches and strategies is possible via cloud providers. A framework for evaluation is introduced to tackle the problem of choosing a cloud provider dependent on customer protection criteria. Cloud cryptography will be a major issue in future because now a day’s everything like databases software’s hardware’s runs using cloud since it takes less space time and less cost to build and easy to manage.

CONCLUSION

Companies and enterprises need to take a data-centric approach to protect their sensitive information from advanced threats in this complex and emerging environment of virtualization, cloud services, and mobility.

Companies must implement security solutions that provide consistent protection for sensitive data, including the protection of cloud information through encryption and cryptographic key management. A comprehensive cloud security and encryption platform should provide strong access controls and key management capabilities, enabling enterprises to make extensive use of encryption, so that they can meet their security objectives.

REFERENCE

1. https://www.cloudmanagementinsider.com/cloud-cryptography/
2. https://medium.com/?source=post_page-----c8263668f86c
3. https://www.geeksforgeeks.org/an-overview-of-cloud-cryptography/
4. Joseph Selvanayagam1, Akash Singh2, Joans Michael ,Jaya Jeswani,Secure File Storage on cloud using cryptography: (IRJET),2018
5. 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.