WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Cloud Cryptography

Gayatri Chandrakant Jadhav, Komal Ishwara Awale, Ankita Annaso Patil,Kalpana N. Rode.

Department Of Electronics and Telecommunication , Sharad Institute of Technology College of Engineering (Yadrav),India
jadhavgayatri201@gmail.com,awalekomal63@gmail.com,ankitaapatil1008@gmail.com

ABSTRACT

Cloud computing is the delivery of computing services over the web instead of keeping files on a proprietary disc drive or local memory device. Computer services can include servers, storage, database, 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 services, 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 basis of cloud computing and discussed various cryptography algorithms present in the existing work.

INTRODUCTION

Cloud computing gives a brand new manner offering 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 with inside the subsequent technology of cellular networks and offerings. Storing information with inside 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.

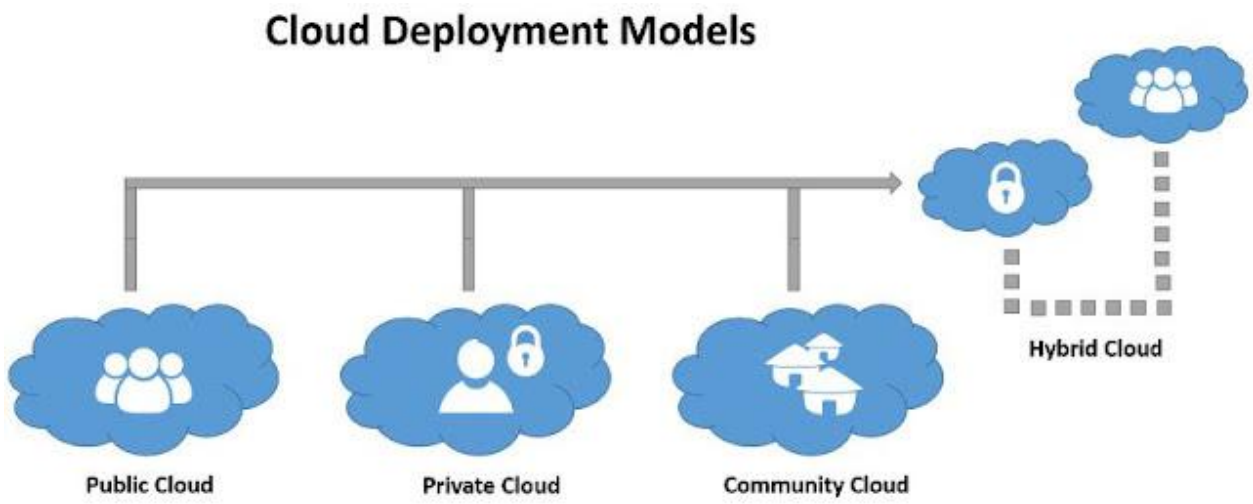
Cloud computing- an upcoming trend in computing world, when compared with traditional computing process has many advantages. We need to have all our computing resources in the premises where we are going to work. But it is not the case with cloud computing. Similarly, setup an environment with all the needed resources, not all the resources will be used all the time. But in cloud, we hire and use what we need and pay only for what we have used. Thus, Cloud has many advantages when compare to other computing techniques. So one way to secure data on the cloud environment is using cryptographic techniques.
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. Cryptography is broadly carried out to make certain information safety.

Cloud Computing:

Cloud computing is usually described in one of two ways. Either based on 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 are available:

- Private Cloud: A private cloud is a model of Cloud Computing where the infrastructure is dedicated to a single user organization.
- Public Cloud: It is an IT model where on demand computing services and infrastructure are managed by a third party provider and shared with multiple organizations with public internet.
- Hybrid Cloud: Is a computing environment that combines an on-premises datacenter (also called a private cloud) with a public cloud, allowing data and applications to be shared between them.
- Community Cloud: This cloud is used for large infrastructure, such as government organizations that connect to one cloud to upload data with unified information or a campus server that connects one cloud computing community.

CLOUD COMPUTING AND CRYPTOGRAPHIC :

Cryptography involves the conversion of clear text into an unreadable form. Cryptography is a technique frequently used to transfer contents safely by ensuring that only the intended recipient can read them. This domain spotlight provides an
overview of the history of cryptography and the many complex, imaginative approaches used in contemporary enterprise encryption.

Cloud Computing Encryption :

Encryption for cloud computing world is an important issue that needs to investigate in several studies. One major focuses of encryption in cloud computing is identification based on encryption. Cloud encryption is the process of transforming data from its original plain text format to an unreadable format, such as cipher text, before it is transferred to and stored in the cloud. The three major encryption types are DES, AES, and RSA.

Cloud Computing Decryption :

The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

Cloud storage providers encrypt data and pass encryption keys to the users. These keys are used to safely decrypt data when needed. Decryption transforms the concealed data back into readable data. Basically, the data that's encrypted has three types: in transit, at rest and in use.

CONCLUSION:

The distribution of information is one of the main health issues for the cloud infrastructure platform. The advent in cloud infrastructure transforms the computer technology landscape significantly and eventually renders computation a reality. Nonetheless, this offers a broad variety of benefits, but the research community is only drawn to certain problems in this area, including the management of services, the regulation of electricity, storage of knowledge. So many things need to be studied. Opportunities in this sector are appropriate for a pioneering contribution and lead to substantial market development. In our paper we have discussed the basic definition of cloud and types of cloud and then gave brief description about cloud computing and its types then cryptography and some of the algorithms used in cloud cryptography and their working.

REFERENCES:

[1] Joseph Selvanayagam1, Akash Singh2, Joans Michael ,Jaya Jeswani,Secure File Storage on cloud using cryptography: (IRJET),2018 [2].

[2] 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.

[3] S. Lei, Wang Ze-wu, "Research and Design of Cryptography Cloud Framework," IEEE. 2018

[4] 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