International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Data Security In Cloud using Stenography

Aman Gupta[1], Aditya Mehrotra[2], Rishabh Arora[3]

[1]*Aman Gupta, I.M.S Engineering College, Uttar Pradesh, India*
[2] *Aditya Mehrotra, I.M.S Engineering College, Uttar Pradesh, India*
[3]*Rishabh Arora, I.M.S Engineering College, Uttar Pradesh, India*

Abstract: Cloud Computing is an Internet-Based computing that provides shared computer, processing resources and data to computers and other devices. Basically, cloud computing means storing and accessing data to get the relevant data and programs over the Internet instead of your computer's hard drive. It has modified the method associations IT, empowering them to land up a lot of deft, gift new plans of actions, offer a lot of administrations.

The Cloud computing scene keeps on acknowledging dangerous development. Keeping up management over the data is key to cloud action ten years previous, business sector info normally dwelled within the association's physical base. Cloud Computing allows companies to avoid upfront infrastructure costs. Cloud computing also allows enterprises to get their applications up and running faster. Cloud computing is the result of adoption of existing technologies and paradigms.

The main Goal of cloud computing is to allow users to take benefit from these technologies without the need for deep knowledge about or expertise with each of them. The Cloud aims to cut costs of the hardware. Automatic computing Automates the process through which the user can provision resources on Demand. Cloud Computing adopts concepts from Service.

1)Introduction:

Cloud computing is that the developing field within the current time. Cloud computing is characterized because the arrangement of assets offered through the online to the purchasers on their interest by cloud suppliers. It passes on everything as an administration over the online in light-weight of consumer interest, for occasion operating framework, system instrumentality, storage, assets, and programming.

To secure the Cloud suggests that secure the medications (estimations) and capability. Security objectives of knowledge is dependent on the 3 basic aspects such as: Availability, Confidentiality and Integrity. The privacy which is provided to the various knowledges and data within the cloud is adopt by cryptography.

Cryptography further divides into three algorithms: -

*Symmetric-key Algorithm

*Asymmetric-key Algorithm

*Hashing. Integrity of information is ensured by hashing algorithms.

Mainly Cloud has three Components such as: -

*Client Computers- Client are the device that the end user interacts with cloud.

*Datacenter- It is collection of servers where application is placed and is accessed via internet.

*Distributed Servers- Servers are in geographically different places, but server acts as if they are working next to each other.

Cryptography is the scrambling of the substance of the knowledge as an example: content picture, sound, options to form the knowledge unintelligible. The main purpose of cryptography is to extract data securely from the intruders. The inverse procedure of obtaining back the primary info from encoded info is cryptography, that restores the primary info. For secured info at Cloud Storage each symmetric-key and uneven key calculations are often used.

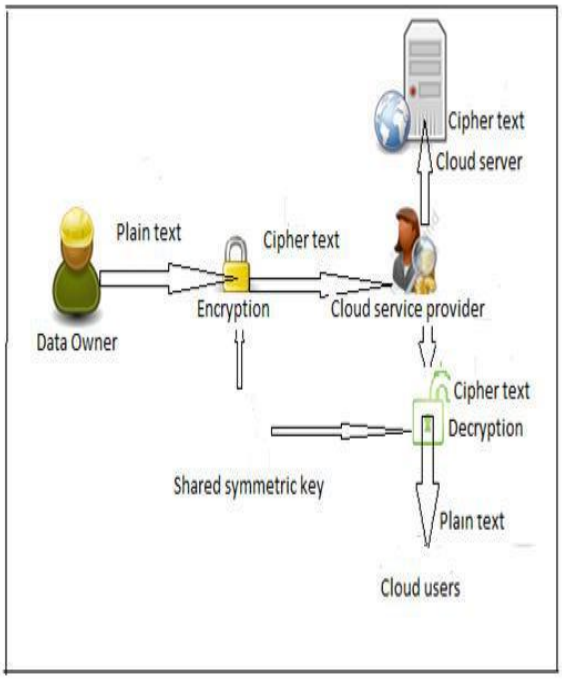
2)Related Work:

Jing-Jang Hwang et al has projected an inspiration of action for cloud computing for info security utilizing info cryptography. Cloud administration provider will be responsible for information of knowledge storage and data encryption , that takes additional procedure overhead for procedure of knowledge in cloud server. The inconvenience is caused due to this technique because there is no management for stored information. Attribute primarily based cryptography and evident info decipherment technique to provide info security in cloud based framework.

Encryption- In this process plain text is converted into Cipher test.

Decryption process

Cloud administration provider has additional machine and storage overhead for check of consumer properties with the outsourced dis-organized data.



3) Security Problems In Cloud:

The Security requirements of a cloud and non-cloud server are quite similar. The Cloud Security Alliance's considers that scientific classification in lightweight of various security areas and procedures that should be followed and provides huge cloud arrangement. Some protection and security-related problems for Cloud computing are as follows: -

I. Governance:

Administration suggests administrations and approaches for application advancement and for knowledge innovation. Design, Usage, testing , utilize and observance of sent are connected with administrations.

II. Malicious Insiders:

The associations understand this danger. Malicious insider's measures danger that has been linked to the confidential data or the association personal data.

III. Service Hijacking:

Sometimes due to phishing risk also exists. With the help of phishing the hacker will become able to access all the relevant data of the user and also can steal the data which can be confidential to the user and also misuse that data , what is more privacy to the administrations.

IV. Hypervisor Vulnerabilities:

The Hypervisor is that the principle programming which is a part of virtualization. There are noted security vulnerabilities for hypervisors and arrangements.

4) Objective:

Main Objectives are as follows: -

- To overcome Cloud Computing Security Challenges.
- Provides Techniques to protect information within the Cloud.
- Provides Strategies for Secure Transition over Cloud.

4.1) Cloud Computing Security Challenges:

Data Protection is the top priority in the list of cloud issues nowadays. As Cloud Computing is trending among the technologies.

There Cloud service suppliers periodically recycles disc space and erase all the existing information.

4.2) To Protect Information Within the Cloud:

Protection using Traditional Models for the protection of information, often with devices like Firewalls and Intrusion Detection System. All mention techniques and software does not provide adequate protection against privileged users and other types of security attacks. It is crucial to audit the whole secret writing and key management answer to produce a comprehensive multilayered approach to protect all the sensitive information.

4.3) Strategies for secure transition over cloud:

Data Security solves the problem of cloud security for the enterprises within the operational settings through a centralized management interface. The major key factor that works with cloud suppliers and enterprises to guard information whether it is physical, virtual or cloud environments.

5) SPLIT Formula:

This Formula comprises that file is splitted into as many parts the user requires. As many parts the file is divided, the more security will be provided to the file.

In this Split formula, the file is compressed and encrypts at the client site and shares it to the Cloud server.

At the receiver end the file will be downloaded, decrypted and decompressed and finally merge to get the whole file which client sends.

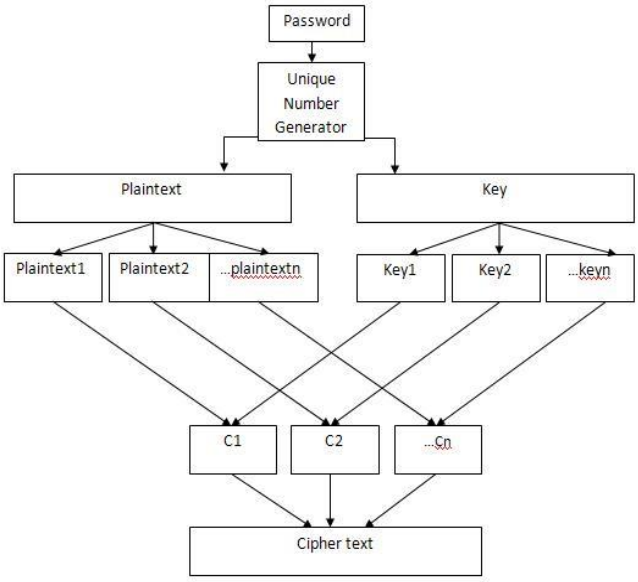
The benefits of using this that due to OTP feature, only authorized user will be able to access the data through Cloud server. This provides maximum security over Cloud. Folder Lock in folder lock approach, whereas lockup a folder we be inclined to supply xml file inside the locked folder and then our program checks whether the folder consists of xml file or not.

5.1) Algorithm:

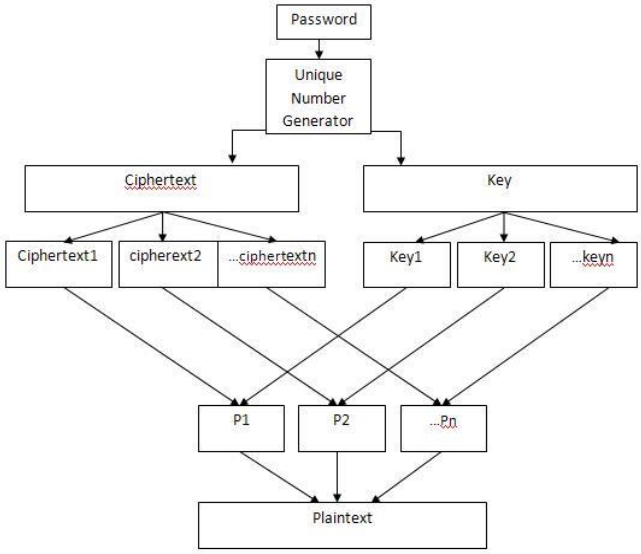
The encryption is done through the following steps

Step 1: Start.
Step 2: Accept file name and password.
Step 3: Generate unique random number from the password, which serves as the key. Step 4: Split the file and the key into n splits.
Step 5: Encrypt the first split of the file with the first split of the key, second split of file with second split of key and so on.

5.2) Encryption:



5.3) Decryption:



6.) Proposed Technique

The unique technique is proposed for providing the advanced encryption and decryption knowledge supports parallel programming such that new approaches can make uses of multiple-core processor to attain the high security with high speed. Here AES Encryption is used.

The sections that introduce the keys for encoding and decoding.

- Symmetric-key encoding
- Public-key encoding
- Key-Length and encoding Strength

Symmetric-key encoding:

In Symmetric -key encoding the encoding key may be calculated from the decoding key. Symmetric -key cryptography is economical while implementing. Symmetric-key cryptography plays a vital role within the SSL protocol, that is wide used for authentication, tamper detection, and cryptography over TCP/IP networks.

Public-key encoding:

It is a cryptographic system that uses pairs of keys which are: public keys are spreaded all over widely and private keys which are only owner have. In public key encryption, any person can encrypt a message using the public key of the receiver but such a message can be decrypted.

Key length and encoding strength:
The key strength of Associate is decided by finding the quickest methodology to interrupt the algorithmic rule.

Sender:
*Start with registration if already a member then login, the user only will be able to login when it will enter the OTP received on registered email.
*Then the file will be splitted into as many parts we want and placed it in a separate folder.

Receiver:
*The receiver will download the file if and only if it will be validated user.
*Then the file will be de-compressed and decrypt to get the merged file.

7). Conclusion
In today's world among technologies Cloud computing is a replacement and organizations also accepting this with open hands because of security reasons. Due to all security reasons organizations accepting Cloud computing.
DES, Triple-DES. AES and Blowfish etc. measure some rhombohedral formula. DES and AES measure largely used rhombohedral algorithms. DES is sort of straight forward to implement than AES.
Cloud computing is likely to have the same impact on software so that foundries have had on the hardware industry. They recommend the developers should be wise to design their next generation of systems to be deployed into Cloud computing. I believe the new IT procurement model offered by cloud computing is here to stay. Whether adoption become as prevalent and deep as some forecast will depend largely on overcoming fears of the cloud over security of the text documents.
Cloud computing is dynamical method which IT departments using constantly. Security may be a major demand in cloud computing because the confidential data should not be shared with other competitors which will be harmful to other company. Business have a variety of documents or data such as infrastructure, platform and applications which are very useful to the companies. Our future is going to be considering some issues associated with existing security formulas and implement a better version of Split algorithm.

8.) Future Scope:
As mentioned above several security algorithms that provides security to our confidential data. Due to increasing number of hacking in such a way our data should be secured such that there will be no misuse of our data. It also includes several areas that need enhancement like a lot of economical algorithms may be developed which may increase the security level. In future we will keep increasing the advancement of the security.

9.) Reference:

- http://datasecurityincloudcomputing.wikispaces.asu.edu/Conclusion
- https://www.safaribooksonline.com/library/view/cloud-security-and/9780596806453/ch12.html
- https://en.wikipedia.org/wiki/Cloud_computing_security
- http://www.slideshare.net/princechandu1441/data-security-in-cloud-computing
- http://journals.sagepub.com/doi/full/10.1155/2014/190903
- http://enterprise-encryption.vormetric.com/rs/vormetric/images/wp-cso-vormetric-data-security-in-the-cloud-updated.pdf