**Data Security Model For Cloud Computing Using V –GRT Methodology**

**ABSTRACT:**

Cloud Computing becomes the next generation architecture of IT Enterprise. In contrast to traditional solutions, Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique feature, however, raises many new security challenges which have not been well understood. In cloud computing, both data and software are fully not contained on the user's computer; Data Security concerns arising because both user data and program are residing in Provider Premises. Clouds typically have single security architecture but have many customers with different demands. Every cloud provider solves this problem by encrypting the data by using encryption algorithms. But there are also chances that the cloud service is not trust worthy, to overcome this problem. This paper introduces a new model called V-CRT methodology which overcomes the basic problem of cloud computing data security. We present the data security model of cloud computing with security vendor that eliminates the fear of misuse of data by the cloud service provider thereby improving data security.

**EXISTING SYSTEM:**

* Huang and Tso proposed an asymmetric encryption mechanism for databases in the cloud. In the proposed mechanism, the commutative encryption is applied on data more than once and the order of public/private key used for encryption/decryption does not matter.
* Re encryption mechanism is also used in the proposed scheme which shows that the cipher-text data is encrypted once again for duality.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Data confidentiality occurs because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification, and fine grained authorization.
* One of the main drawbacks of cloud is that there are too much of possibility for the cloud service provider for the misuse of the data that is stored in their data center by the client. Due to this, whatever methods that are proposed don't have direct impact to reduce this problem. There will be issues continuing in the cloud computing until the cloud service provider knowledge about the data is prohibited. There is also repeated usage of OTP method in the cloud computing techniques which makes this system to an inefficient one.

**PROPOSED SYSTEM:**

1) Username and the Password provided by the client to the cloud service provider. The password is encrypted by Hybrid Encryption method such as RSA, Ceaser cipher and alphabetic encryption

2) Cloud Service Provider (CSP) authenticates the user by verifying username and password by decryption and sends with the login key for the Security Vendor.

3) User space in CSP and the memory address allocated for the user is given by the Cloud Service Provider to the Security Vendor.

4) Login key for Security vendor

5) User authenticated with key provided by Cloud Service Provider

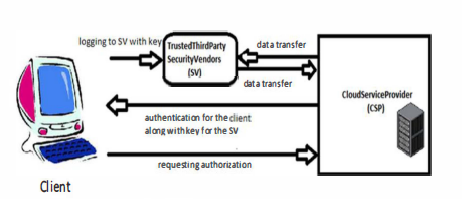
6) User selects the encryption method for various options that CSP does not aware of and stores the data

7) Security vendor sends the encrypted data to Cloud Service Provider

**ADVANTAGES OF PROPOSED SYSTEM:**

* More Secure System
* Results show better performance evaluation when compared with existing system

**SYSTEM ARCHITECTURE:**



**MODULES:**

* Cloud Service Provider
* Data Users Module
* Security Vendor's Module (Auditor)
* RSA, Ceaser Cipher, 3DES Algorithm

**MODULES DESCRIPTION:**

**Cloud Service Provider**

* In this module, we develop Cloud Service Provider module. This is an entity that provides a data storage service in public cloud. The S-CSP provides the data outsourcing service and stores data on behalf of the users. To reduce the storage cost, the S-CSP eliminates the storage of redundant data via deduplication and keeps only unique data.
* In this paper, we assume that S-CSP is always online and has abundant storage capacity and computation power.Java code to send the key to the Security vendor and the client by using Shishi.Receives the encrypted data forwarded by Vendor.Can view all users' database in the encrypted format.

**Data Users Module:**

* Design the Code for three encryption algorithms in Java. Design the Front End using Java. A user is an entity that wants to outsource data storage to the S-CSP and access the data later.
* In a storage system supporting deduplication, the user only uploads unique data but does not upload any duplicate data to save the upload bandwidth, which may be owned by the same user or different users.
* In the authorized deduplication system, each user is issued a set of privileges in the setup of the system. Each file is protected with the convergent encryption key and privilege keys to realize the authorized deduplication with differential privileges.

**Security Vendor's Module:**

* In this module, the Security Vendor select encryption algorithm that will be used to store data. Use keys received from cloud service provider for login. If authentication is succeeded, then services can be used.

**Triple DES, Ceaser Cipher, RSA Algorithm:**

* The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.
* In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1 GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Netbeans 7.2.1
* Database : MYSQL