Secure and Trustworhty Data Storage in Cloud Computing

T. Saravanan, G. Saritha and R. Udayakumar

1Department of ETC, Bharath University, India
2Department of EEE, Sathyabama University, Chennai, India
3School of Computing Sciences, Bharath University, Chennai, India

Abstract: Cloud Computing is emerging technology which consist of existing techniques combined with new technology paradigms. In this new technology shared resources like software's, hardware's and information is provided to its users and other peoples on internet whenever demanded. Cloud computing enables users to remotely store their data and have the benefit of on-demand high quality cloud applications without the burden of local hardware and software management. The current solutions used today to login to cloud services have been investigated and concluded that they don't satisfy the needs for cloud services. They are insecure, complex or costly. So, data integrity is comes to on big issue. In order to maintain data integrity, proposed design consist of efficient encryption algorithm to use in a cloud background is RC4, which is safe and at the same time a speedy algorithm. It also provides two factor authentications with one time passwords which are really useful for login and access the cloud services in a safe manner. This concept focuses on authentication and transmission encryption in cloud services.

Key words: Cloud Computing · Data integrity · Dependable storage · RC4 Encryption algorithm · Two factor authentication with one time password

INTRODUCTION

Cloud computing is a universal word for anything that involves distributing hosted services over the web [1]. It can be an internet related computing environment that allows users to access different level of IT resources remotely through internet based client-side software as if it were installed locally in users own computer [2]. Where the IT resources include server, storage, service, application, network and so on. These resources are associated in a large computer network which is owned by a corporation (Both privately and publicly) [3]. Cloud computing also provides services to others devices (such as smart-phones) on demand over the Internet Companies, business organizations, academic or commercial researchers and any individual can be user of cloud computing. Cloud computing is a practical approach to experience direct cost benefits and it has potential to transform a data center from a capital intensive set up to a variable priced environment [4]. Nearly every cloud computing infrastructures be made of services distributed through common centres and built on servers [5]. The main cloud Service providers like Amazon, Sales force an Google examples of large and well reputed IT firms that are dynamically involved in cloud computing are Microsoft, Fujitsu, Hewlett Packard (HP), IBM, Dell and VMware. According to service model, cloud computing can be categorized into three main categories Infrastructure-as-a-Service (IaaS),Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [6].Apart from this another cloud service is Storage as a Service (StaaS) which allows user to store their data and access these anytime via internet [7].

Since cloud computing is a quite new subject, most of the cloud providers have not yet tighten up their security and still use insecure or complicated login methods [8]. The authentication part of cloud computing must be easy and flexible for the millions of user that it has, but at the same time be very secure to protect the data that it stored in the cloud [9]. At the same time the encryption method used during transmissions must also be very secure and, since the cloud's vast amount of users, a fast algorithm that doesn't require much computer power and processing.
Problem Description

System Model: Representative network architecture for cloud storage service architecture is illustrated in Figure 1. Three different network entities can be identified as follows:

- User: an entity, who has data to be stored in the cloud and relies on the cloud for data storage and computation, it can be either enterprise or individual customers.
- Cloud Server (CS): an entity, which is managed by cloud service provider (CSP)

To provide data storage service and has Significant storage space and computation resources.

Challenges in Cloud Computing: Although virtualization and cloud computing can help companies accomplish more by breaking the physical bonds between an IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing paradigm [10]. This is particularly true for the SaaS provider. Some security concerns are worth more discussion with the cloud model, you lose control over physical security. In a public cloud, you are sharing computing resources with other companies. In a shared pool outside the enterprise, you don’t have any knowledge or control of where the resources run [11].

Data integrity is assurance that the data is consistent and correct [12]. Ensuring the integrity of the data really means that it changes only in response to authorized transactions. Following are the major challenges in the cloud computing:

- Data Protection
- Data Recovery and Availability
- Security and Trust Issues

Ensuring Secure Transfer: The RC4 encryption techniques and OTP has provide solution for Secure Transfer to the cloud.

RC4 Encryption: RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence [13]. The key stream is completely independent of the plaintext used [14]. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text [15].

The algorithm can be broken into two stages: initialization and operation. In the initialization stage the 256-bit state table, $S$ is populated, using the key, $K$ as a seed. Once the state table is setup, it continues to be modified in a regular pattern as data is encrypted. The initialization process can be summarized by the pseudo-code

$$I := 0 \quad j := 0$$

while Generating Output:

$$i := (i + 1) \text{ mod } 256$$

$$j := (j + S[i]) \text{ mod } 256 \quad \text{swap}(S[i], S[j])$$

output $S[(S[i] + S[j]) \text{ mod } 256]$ end while

Two-Factor Authentication with OTP: Since the problems with static passwords, many have now started to use two-factor authentication with one time passwords as the login procedure for different services. One time passwords and Two-factor authentication is two separate solutions but is most often used together for a better security solution.

In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it’s very important to develop a secure OTP.

Endorsement with OTP: The authentication method used is two-factor authentication with a one-time password, The user's mobile phone will work as the authentication device, in which the user have to enter a 4-digit PIN code to generate an OTP that can be used for login.

The OTP that is generated based on three components,

- The 4-digit PIN code that the user enter.
- A secret random number that was created during device-initialization (Init-secret) that only exists on the user's mobile device.
- The current time

After hashing, the mobile phone will display the first six numbers of the hash that will be used as the OTP for login. Since time is part of the hash, the OTP is only valid
for three minutes. The OTP will then be sent to the server during login. The server knows the Init-secret and the pin-code, which is stored in a database and also the current time. Therefore the password can be verified by the server.

**Existing System:** Cloud System has the computation assigned in a great number of distributed computers, rather than local computer or remote server. Though cloud services are entirely based on distributed computing, broad range of both internal and external threats for data integrity still exist. On the other hand, since users may not retain a local copy of data from the cloud service.

Providers (CSP), to behave unfaithfully towards the cloud users regarding the status of their outsourced data. Similarly CSP may even attempt to hide data loss incidents so as to maintain a reputation. Finally, virtual machine attacks and Web service vulnerabilities existed long before cloud computing became fashionable.

**Proposed System:** To ensure the security and dependability for cloud data storage, the efficient mechanisms for dynamic data verification and operation and achieve the following goals: Data protection which is achieved by using RC4 encryption technique and transmission policy and secure access done by two factor authentication with one time password which is really helpful for highly reliable transmission and the Storage correctness is to ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud. Next thing is to achieve the availability of data in the cloud through cryptographic protocols supporting computation on cipher text. So the proposed design guarantees that the all technique has resilient against intruders and data modification issues.

**Test and Implementation of Solution:** The solution of using mobile OTP and RC4 encryption to provide a safe connection to the cloud service, when using a cloud service, the user usually connect through a web browser to a server running somewhere which is probably unknown to the user. Based on this assumption, the experiment will consist of two computers that connect to each other over the Internet. The server-computer will run VMware to create a virtual machine (VM) with Hadoop Server 12.

![Fig: (a) represents data loss without encryption (b) Data protected using encryption](image-url)
CONCLUSION

In this paper, we investigate the problem of data security in cloud data storage. To achieve the assurances of data in the cloud the client files has been encrypted. In order to avoid the problem of data security let propose an Effective and flexible distributed storage supports one Time password with strong two factor authentication scheme to ensure the availability of users’ data in the cloud. Through detailed security and extensive results show that our scheme is highly efficient and resilient to different problems.

REFERENCES