IJARESM
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING, SCIENCE & MANAGEMENT

# SECURE RSA INTERFACE IN CLOUD COMPUTING USING ENCRYPTED ONE TIME PASSWORD

**Jayesh Chauhan[1], Mr. Jayesh Mevada[2], Mitesh Patel[3], Kajal Isamaliya[4]**
M.Tech, Computer Engg., Merchant Engg.College, Basna , Mehsana, India[1]
M.Tech, Computer Engg., Merchant Engg.College, Basna , Mehsana, India[2]
Assistant Professor, Computer Engg., Merchant Engg.College, Basna Mehsana, India[3]
Assistant Professor, Computer Science Engg.., SNPIT&RC, Bardoli,Gujarat, India[4]

***Abstract:- Cloud computing is an On-demand self-service Internet infrastructure where a customer can pay and use only what is needed, managed by an API. The Service Provider plays an active role in transmitting information across the cloud. Privacy for the information through authentication is being considered important. The main objective of the proposed architecture is preserving the privacy of the information ensuring that this information cannot be misused. In this we have proposed secure cloud architecture to address the user privacy problem in a cloud. By using OTP and WTP in cloud computing system, our proposed architecture achieves better goal of preserving the privacy of a user.***

***Keywords:-*** **Cryptography, Cloud Computing, Public Key, Encrypted one time password**

## I. INTRODUCTION

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures. Security is one of the major issues which is hampering the growth of cloud computing. It is difficult, from a user perspective, to over-protect a service. If you make the login process too hard for a user, the user might grow tired of that service. It is also important for the cloud providers to have good security standards in order for the common users to trust the cloud, for future growth of the cloud technology. In a cloud system, company susceptible data and information will be stored on third-party servers, and user will possibly have very inadequate understanding or control regarding this information [3]. The four primary types of cloud models are:

1. Public
2. Private
3. Hybrid
4. Community

Each has its advantages and disadvantages with significant implications for any organization researching or actively considering a cloud deployment.

**Public Cloud**

*All rights reserved by www.ijaresm.net*

A public cloud is a cloud computing model in which services, such as applications and storage, are available for general use over the Internet. Public cloud services may be offered on a pay-per-usage mode or other purchasing models. An example of a public cloud is IBM's Blue Cloud.

**Private Cloud**

A private cloud is a virtualized data center that operates within a firewall. Private clouds are highly virtualized, joined together by mass quantities of IT infrastructure into resource pools, and privately owned and managed.

**Hybrid Cloud**

A hybrid cloud is a mix of public and private clouds. Community Cloud A community cloud is an infrastructure shared by several organizations which supports a specific community.

**Cloud Solutions**

These services are categorized into five prominent sections as follows:

1. Infrastructure as a Service (IaaS): Provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources, and allow the consumer to deploy and run arbitrary software, which can include operating systems and applications. The consumer has control over operating systems, storage, deployed applications, and possibly limited control of select networking components [3].
2. Software as a Service (SaaS): Provides the consumer with the capability to use the provide's applications running on a cloud infrastructure [3].
3. Platform as a Service (PaaS): Provides the consumer with the capability to deploy onto the cloud infrastructure, consumer created or acquired applications, produced using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations [3].

**Cryptography**

Cryptography is a process which is associated with scrambling plaint into cipher text (Encryption), then back again to plain text (Decryption). The key feature of asymmetric cryptography system is encryption and decryption procedure are done with two different keys - public key and private key. This is one main difference between symmetric and asymmetric cryptography, but that difference makes whole process different.

**RSA Algorithm**

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman introduced a cryptographic algorithm, which was essentially to replace the less secure National Bureau of Standards (NBS) algorithm. Most importantly, RSA implements a public-key cryptosystem, as well as digital signatures. RSA is motivated by the published works of Diffie and Hellman from several years before, who described the idea of such an algorithm, but never truly developed it. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors.

**Algorithm Steps:**

*All rights reserved by www.ijaresm.net*

1. Select two different prime numbers p and q for security aim, the integer's p and q must be large.

2. Calculate n=p*q, n will be used as the module for public key and private key.

3. Calculate f(n)=(q-1)(p-1) Where f is a function of Euler's

4. Select an integer e such that 1<e<f(n) and GCD (e, f(n)) =1, e and f(n) are co prime.

5. Determine d: d is multiplicative inverse of e mod (f(n)) (e * d) mod f (n) = 1 d is the private key.

**Encryption**:

M is plain text data.

C=m^e mod n

**Decryption**:

C is received cipher text.

M= C^d mod n

## II. ENCRYPTION STANDARD USED

### A. *AES (Advanced Encryption Standard)*

AES is relatively new and very complex that operates on discrete blocks of data using a fixed key. AES is publicly available and can be freely used without hitting any legal problem [1]. The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length [4].

Here a new approach such that where we go for AES to give security for the log files which contains log records. When a user access a data own by an owner, a log record id generated and kept in the log file which will be in an encrypted format. When the owner follow a log pull method to get his log file, he should enter the secret key by which that log file will be decrypted and accessible by that owner [4].

### B. *RC4*

RC4 is very old and is very simple. WEP and TKIP implement the RC4 cipher. RC4 is a stream cipher that does not have a discrete block size. Instead, it uses a key stream of pseudorandom bits that is combined to the data using an exclusive OR (XOR) operation. A good example of the weaknesses of RC4 is the implementation of WEP. The primary reason why RC4 is very popular is the fact that it is simple and it can be very fast [1].

Difference of AES and RC4

- AES is a block cipher while RC4 is a stream cipher.
- AES is extremely secure while RC4 is not so.
- RC4 is very fast compared to AES.
- RC4 is trademarked while AES is not.

### C. *Two - factor authentication with OTP*

Two factor authentications together with OTP is much safer than static passwords, when looked at from an access attack perspective, such as sniffing, password cracking and social engineering. However, it cannot protect against two common attacks [1].

- Man-in-the-middle attack

An attacker sets up a fake website, resembling a legitimate site that the user surfs to in order to log in. The user generates the OTP and sends it to the fake website controlled by the attacker, which can now use this password to login to the real website [1].

- Trojan attack

*All rights reserved by www.ijaresm.net*

A Trojan is installed on the user's computer, allowing a hacker to "piggyback" on the session established when the user logins to a website. These two attacks are best solved by educate users in how to spot web pages with false certificates and how to protect your computer and keep anti-virus software up to date [1].

## III. TYPES OF EXISTING SYSTEMS

There are several systems for dealing with two way mobile authentication. They may differ in delivering the password to the authorized user or a different entity based on the security constraints. Some of them are as follows

### *A. Tokens*

A token is a device used to authorize the user with the services. A token may be software or hardware. Software tokens are used to identify the person electronically, i.e. it may be used as a password to access something. Hardware tokens are small hand held devices which carry the information which stores cryptographic keys, digital signatures or even bio-metric data by which we can send generated key number to a client system. Mostly all the hardware tokens have a display capability. The hardware tokens include a USB, digital pass etc. Drawbacks A token shall be carried all the time. Special software is required to read the token. Anyone can access the information that has the token i.e. in case of theft.

### *B. Biometrics*

A biometric authentication is the advanced form of authentication. A biometric authentication is nothing but it scans the user's characteristics such as finger print and eye retina and stores in the form of a string. When the user tries to authenticate it matches with the stored data and then gives access when a commonality is achieved and when the user has gained access he can enter the password to view the required information.

Drawbacks Biometric authentication is convenient only for limited applications, since the system becomes very slow for a large number of users. Finger prints can be taken on a small tape and can be provided for the hardware Additional hardware is required to detect the fingerprints and eye retinas.

### *C. One time Password*

Dynamic password (One-Time-Password) technology is a sequence password system and basic idea is to add uncertain factor in authentication so that users need to provide different messages for authentication each time. By this way, the applications themselves can obtain higher security guarantee than those use static password technology. When login request from user is received, server system generates a one-time password and sends it through a SMS to a GSM cell phone registered for that specified user. The one-time password has a default timeout. In the second phase of the authentication, a request is sent with the user id and a hash of the one-time password. If both the onetime and user specified password is valid then the user will be authenticated.

Two way one time authentication works as follows:

- User send a login request server with its ID and pin(Static password)
- If ID and PIN match with the ID and PIN stored in database, server generate one time password (OTP) and send it through SMS or email to the user.
- Server request user for OTP
- User enters OTP and if it matches then user is authenticated.

*All rights reserved by www.ijaresm.net*

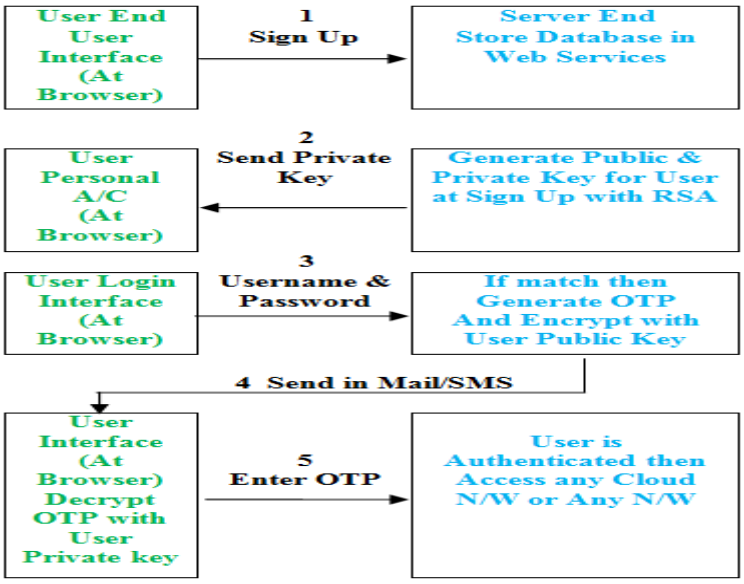
Major problem of existing system is it needs a third party such as GSM mobile number, email id etc.

## IV. PROPOSED SYSTEM

The Proposed system is based on the existing system. In the proposed, first user need to generate a key pairs, using any public key cryptography algorithm (e.g. RSA algorithm). In the proposed system user will request for login with ID and PIN (static password). If it matches with data stored in data based then server generate a random password (OTP) and encrypt it with the stored user's public key and send it to user. User will decrypt the encrypted one time password (EOTP) and send it to sever and if it match with original algorithm is used in the proposed system as public key cryptography algorithm. In the proposed system third party such as GSM mobile number or email id is not required. User will generate a key pairs using RSA algorithm and stores public key into the database during registration of users account.

Proposed system works as follows:

- User will register in application and get User Id and Password.
- User will request for login with User Id and Password.
- Server will verify User Id and Password and generate one time password and encrypt it with user's public key which is stored in database and send the encrypted OTP to user.
- User will decrypt the encrypted OTP with private key and send the result to server.
- Server will match it with generated OTP, if it matches then user is authenticated.




Advantage of proposed system over existing system:-

- Proposed system is independent of third party (e.g. email, GSM mobile number).
- Proposed system is highly secure based on key size.
- Proposed system is more efficient.

Application Area:-

- All the social networking sites: The proposed system will provide more secure authentication system compared to existing systems used by social networking sites.
- All the electronic-commerce sites: The proposed system will provide more secure authentication system compared to existing systems used by electronic-commerce sites.
- In the e-banking sectors also proposed system is very useful.

*All rights reserved by www.ijaresm.net*

## CONCLUSIONS

According to research we conclude that the encrypted OTP gives better security instead of plain OTP. The proposed system is designed to improve security, efficiency and to remove dependency on third party.

## REFERENCES

[01] Akhil Kaushik; Hari Om Awashti; Kirtika Goel; Sakshi Goel "Secure Authentication with Encryption Technique for Mobile on Cloud Computing", 2012 International Journal of Scientific Research Engineering & Technology

[02] Dr.Sandeep Sharma; Navdeep Kaur Khiva "Secure Cloud Architecture for Preserving Privacy in Cloud Computing using OTP/WTP", 2013 Global Journals Inc. USA.

[03] Vishal Paranjape; Vimmi Pandey"An Approach towards security in Private Cloud Using OTP", 2013 International Journal of Emerging Technology and Advanced Engineering.

[04] K Rintumol Joseph; Fabeela Ali Rawther" Information Accountability on Cloud for Data Sharing in a Distributed Environment", 2013 International Journal of Latest Trends in Engineering and Technology

[05] Sagar Acharya; Apoorva Polawar; P.Y.Pawar" Two Factor Authentication Using Smartphone Generated One Time Password", 2013 IOSR Journal of Computer Engineering.

[06] K.Marimuthu; D Ganesh Gopal; Harshita Mehta; Aditya Rajan; P Bhuminathan"A Novel Way of Integrating Voice Recognization And One Time Password To Prevent Password Phishing Attacks", 2014 International Journal of Distributed and Parallel Systems.

[07] Atul Kahate , Cryptography and Network Security , Tata McGraw- Hill Publishing Company Limited.

[08] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, New Delhi.

[09] http://en.wikipedia.org/wiki/One-time_password

[10] http://en.wikipedia.org/wiki/Cloud_computing

*All rights reserved by www.ijaresm.net* 