ISSN:0975-9646

Modified Secure Two Way Authentication System in Cloud Computing Using Encrypted One Time Password

Geetanjali Choudhury
B-Tech student,
Department of Computer Science Engineering,
Regional Institute of Science & Technology,
Meghalaya.India.

Jainul Abudin
Assistant Professor,
Department of Computer Science Engineering,
Regional Institute of Science & Technology,
Meghalaya.India.

Abstract:-Cloud Computing is a concept that has many computers interconnected through a real time network like internet. Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Cloud computing provides facility to share distributed resources and services that belong to different organizations or sites. In private cloud system, information is shared among the persons who are in that cloud. In this paper we have proposed new authentication system for cloud computing platform. The Proposed technique based on encrypted one time password (EOTP). In the proposed technique one time password is encrypted by public key of user to obtain Encrypted one time password (EOTP). In the proposed system third party is not required.

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

I. INTRODUCTION

Cloud computing involve distributed computing over a network, where a program or application may run on many connected computers at the same time. It specifically refers to a computing hardware machine or group of hardware machines commonly refers as a server connected through a communication network such as the network, an intranet, a local area network (LAN) or wide area network (WAN). Any individual user who has permission to access the server can use the server's processing power to run an application, store data, or perform any other computing task. Therefore, instead of using a personal computer every-time to run the application, the individual can now run the application from anywhere in the world, as the server provides the processing power to the application and the server is also connected to a network via internet or other connection platforms to be accessed from anywhere. All this has become possible due to increasing computer processing power available to humankind with decrease in cost as stated in Moore's law.

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

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:

i. Infrastructure as a Service (IaaS): This provides a platform virtualization environment as a service rather than purchasing servers, software, data centers etc.
ii. Software as a Service (SaaS): This service deploys software over the Internet which is deployed to run behind firewall in your LAN or PC.
iii. Platform as a Service (PaaS): This kind of cloud computing provide development environment as a service. You can use the middleman's (broker) equipment to develop your own program and deliver it to the user through the Internet and Servers.
iv. Storage as a Service (StaaS): This is database like services billed on utility computing services basis; e.g gigabyte per month
v. Desktop as a Service (DaaS): This is the provisioning of the desktop environment either within a browser or as a terminal server

Cryptography

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or clear text) into cipher text (a process called encryption), then back again to plain text (known as decryption). The key feature of asymmetric cryptography system is encryption and decryption procedure are done with two different keys - public key and private key. Private Key cannot be derived

with help of public key that provides much strength to security of cryptography.

This is one main difference between symmetric and asymmetric cryptography, but that difference makes whole process different. This difference is small but it is enough that it has implications throughout the security.

How public key cryptography works?

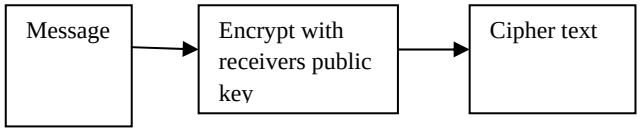


Figure 1:- At sender end

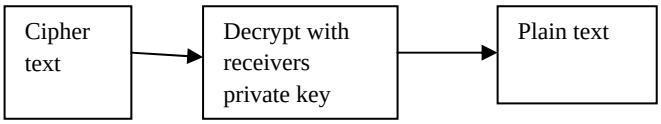


Figure 2:- At receivers end

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[2]. 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.

RSA algorithm:

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.

$C=m^e \bmod n$

Decryption:

C is received cipher text.

$M= C^d \bmod n$

EXISTING SYSTEMS

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

1. 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.

2. 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[5].

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.

3. One time Password:

Dynamic password (namely, One-Time-Password) technology is a sequence password system and is the only password system proved non-decrypted in theory[8] . Its 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 one-time and user specified password is valid then the user will be authenticated.

Two way one time authentication works as follows:

Step 1. User send a login request server with its ID and pin(Static password)

Step 2. If ID and PIN match with the ID and PIN stored in database, server generate a one time password (OTP) and send it through SMS or email to the user.

Step 3. Server request user for OTP.

Step 4. User enters OTP and if it match then user is authenticated.

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

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 users 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 one time password (OTP) user is authenticated. RSA 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:

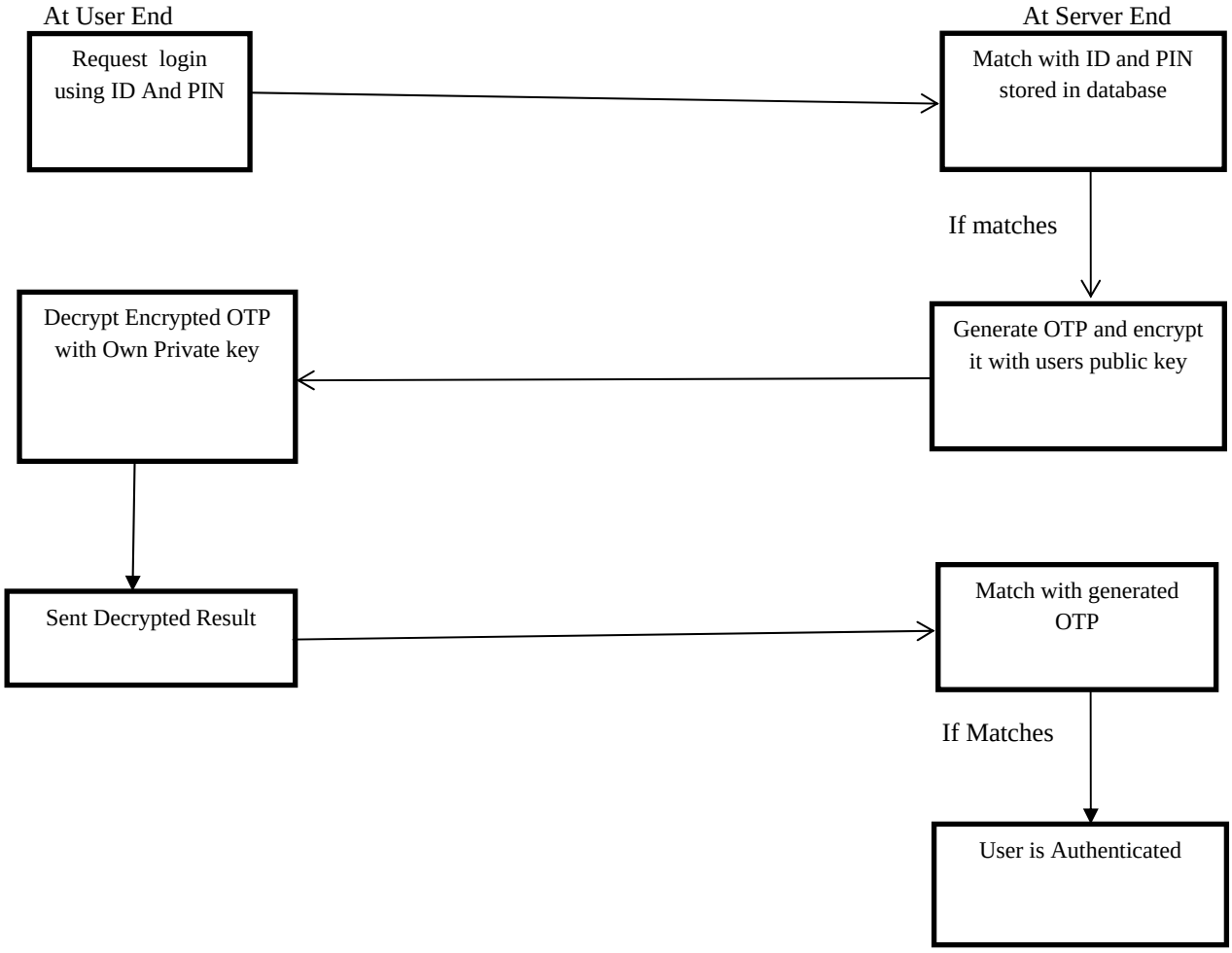
Step1. User will request for login with ID and PIN.

Step2. Server will verify ID and PIN and generate a one time password and encrypt it with users public key which is stored in database and send the encrypted OTP to user.

Step3. User will decrypt the encrypted OTP with private key and send the result to server.

Step4. Server will match it with generated OTP , if it matches then user is authenticated.

How it works?



Advantage of proposed system over existing system:-

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

APPLICATION AREA:-

Although this proposed system is designed for cloud authentication it can also used in other area which are describe bellow:

1. All the social networking sites:

The proposed system will provide more secure authentication system compared to existing systems used by social networking sites.

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

FUTURE WORK:

Future developments include a user friendly GUI and extending the encrypted OTP algorithm so that system become more secure.

CONCLUSION:-

In this paper we used public key cryptography (RSA algorithm) for encrypting and decrypting one time password. In the proposed system encrypted one time password is directly send to user through the network. In the proposed system third party such as GSM mobile number or email is not required. The proposed system is designed to improve security, efficiency and to remove dependency on third party. Proposed system is highly secure and is dependent on the key size. The key pairs are generated with the help of public key cryptography algorithm.

REFERENCES:-

1. http://en.wikipedia.org/wiki/Cloud_computing
2. Atul Kahate , Cryptography and Network Security , Tata McGraw-Hill Publishing Company Limited.
3. William Stallings, “Cryptography and Network Security Principles and Practices”, Prentice Hall, New Delhi.
4. http://en.wikipedia.org/wiki/One-time_password
5. H:B Kekre,V.A Bharadi , International Journal of Intelligent Information Technology Application,2009,2(6):279-285.