Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA2012-5, February 10, 2012

Two Factor Authentication on Cloud

Shanmugapriya S
AP/HOD
Dept of IT
M.I.ET college of Engg
Trichy
9443876946
E-mail:
shanmugapriyaraj@
yahoo.com

Gulzar Begam J
Dept of CSE
M.I.ET college of Engg,
Trichy
9843894352.
E-mail:
gulzarjani@gmail.com

Anitha M
Dept of CSE
M.I.ET college of Engg,
Trichy
9442108806
E-mail:
anitha_es07@yahoo.
com

Cynthia Napoleon
Dept of IT
M.I.ET college of
Engg Trichy

Abstract - Security is something which cannot be comprised with, especially in cloud computing. Data in the cloud are constantly under threat. But more companies will move to the cloud once they are satisfied that their data is safe on the cloud. So it's really important to device ways that will enable the authorized user to gain access to the cloud at the same time not making it too difficult for them to do so. In this article, we focus on authentication issues are overcome by using Two factor Authentication, ie Palm Print based identification system using the textural information employing different wavelet transforms. OTP (One Time Password) can be generating by the use of Trusted Computing Technology to develop more secure shared secret key tokens using mobile phones.

Keywords : *Authentication, Palm Print, OTP, Policy.*

I. INTRODUCTION

In cloud computing is the cloud data storage, in which subscribers do not have to store data on their own servers ,where instead their data will be stored on the cloud service provider's servers. In the cloud computing , subscribers have to pay the services providers for this storage service. This service does not only provides flexibility and scalability for the data storage , it also provide customers with the benefit of paying only for the amount of data they need to store for a particular period of time , without any concerns for efficient storage mechanisms and maintainability issues with large amounts of data storage . In addition to these benefits customers can easily access their data from any geographical region where the Cloud Service Provider's network are internet can be accessed. An example of the cloud computing is show in the Fig 1.Along with these unprecedented advantage, cloud data storage also redefines the security issues targeted on the customer's out sourced data (data that is not stored / retrieved from the customers own servers

Figure 1. Cloud Computing Architecture

II. AUTHENTICATION

Authentication is the first step in the user- connection process. Any organization deploying an information system needs a reliable connection to its system and applications. Creating a single and reliable identity source associated with rights managements, is the basis for good identity and access management. The user-connections process can be implemented. In four stages:

Initial process- common to all connections

1. Starting the work station and authenticating a user.
2. The workstation checks the user's rights and connects the user to his or her resources.

Connecting to application itself

1. The user runs a secure applications and authenticates to this applications
2. The applications checks the user's rights and connects the user to his or her transactions and data.

User authentication is one of the main points of this process. It enables the information system to verify the user's identity and associates the user with his or her rights.

III. RELETED WORKS

A Policy Base Authentication:

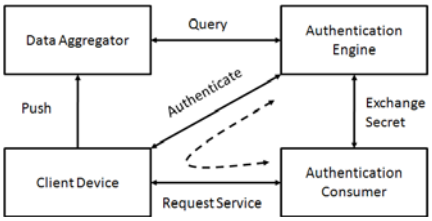


Figure 2 Policy – Flow of Data.

We consider an architecture with the following types of participants: client devices, data aggregators, an authentication engine, and authentication consumers. The client de-vices

generate observable context and actions as part of their regular use. The data aggregators collect data on context and actions from client devices, and from auxiliary sources(such as schedules provided by third parties). The authentication engine obtains data from data aggregators, and mayrequest data directly from client devices. It makes authentication decisions based on collected data and authentication policies. Authentication consumers provide policies to the authentication engine based on end user access requests(e.g., a webpage access request or a payment request). Finally, the authentication consumer responds to a client's re-quest based on the authentication result it receives. Fig.2 demonstrates the relationship between participants. The authentication flow is as follows: Before authentication starts, the authentication consumer lists the access re-quests (e.g., a webpage access request or a payment request)that require authentication. For each request, the authentication consumer will register a policy with the authentication engine. The policy includes at least three parts: the access request, the information to be collected from client devices or data aggregator for this access request, and a rule to generate the authentication result. During normal operation, client devices periodically report to the data aggregator. This data will be used to track user behavior and support authentication requests. The authentication flow starts when an access request is received by the authentication consumer. (This request may have been initiated by a client device that the system collects data from, or by another device, such as a credit card reader.) Upon receiving the request, the authentication consumer redirects the request to the authentication engine,along with request details. The authentication engine retrieves the policy for the access request, extracts the information that needs to be collected, and sends an inquiry to the client device and/or data aggregator. The client de-vice and/or data aggregator receives the inquiry, generates a report, and sends it back to the authentication engine.[1]The authentication engine then applies the authentication rule in the policy and determines the authentication result(whether or not the client device is authenticated for the access request) and sends this back to the authentication consumer. Based on the authentication result, the authentication consumer will either provide the service (e.g., return the webpage content or accept the payment request) or reject the request.

Draw Backs:

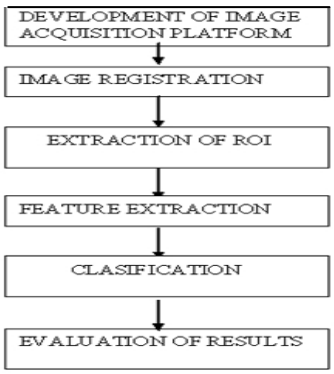
In the policy based authentication method , we need to store the lots of information about the clients .These information are used for the authentication purpose The authentication consumer can generate the quires based on the collected information. There is chance that client can forget the answer for that quires , what he stored at the first .so that client cannot access the data from the storage.

IV. PROPOSED SYSTEM

A Palm Print Authentication

Biometric based personal identification is getting wide acceptance in the networked society**.** Palm print based personal verification has quickly entered the biometric family due to its ease of acquisition, high user acceptance and reliability .The palm print based identification system using the textural information, employing different wavelet transforms The wavelets used for the analysis are Biorthogonal, Symlet and Discrete Meyer

Algorithm For Palm Print Based Authentication:



Development of Image Acquisition Platform:

In developing an image acquisition ,we using an enclosed black box which contain two plates . The upper plate holds the camera and the light source while the bottom plate is used to place individual's hands. The user is quest to place his hand maximally flat on the imaging surface and keep his finger apart. A line is drawn on the imaging surface and the user is asking to place his middle finger in line with it. The middle finger if kept aligned with a certain reference lines facilitates rotational and translational invariance.

Image Registration :

By using Image registration technique in [2] . The ac-quirked color (RGB) parameters of palm print are changes to HIS parameters. Gray level image retain all the useful discriminating information required for personal identification . By following equation we can convert the color image into gray level image using below equation

$$I = (0.2989*R)+(0.5870*G)+(0.1140*B)$$

The longest line in a palm passes through the middle finger and any rotation is consider with reference to this line The theta between the normal axis and the longest line passing through the middle finger is calculated by using below equation,

$$\theta = (1/2)\tan^{-1}(2c/a-b))$$

After determination of theta, we rotate the palm print accordingly for vertical alignment using affine transform. After the vertical alignment of the palm print , morphological operation of dilation is apply to remove holes in binary images. Finally distance transform is apply with the chessboard metric to calculate the centre of palm print . Max[x1-x2,y1-y2].

Feature Extraction And Classification:

We can obtain ten images of each individual of which five are using for training and the rest of them are using for validation .The obtaining registered palm print image is analyzed for its texture using different symmetrical wavelet. The palm print region 256*256 has been decomposed into three scales for each wavelet type.

B One time password

The motivation for using one-time passwords is that the compromise of one password should not affect the security of sessions involving another password. The one-time password serves to mutually authenticate the client and the server; there are no other long-term values like public keys or certificates. Authentication is based on knowledge of the shared password. Informally, a protocol will provide secure mutual authentication A accepts a session as being with party B unless B participated in the protocol, and vice versa. We want a one-time-password protocol to give secure mutual authentication for the current session even if other one-time passwords have been revealed. We are using the Trusted Computing Technology to develop more secure shared secret key tokens using mobile phones.

OTP generator consisting of two parts.

1. OTP Token Configuration.
2. OTP Generation

OTP Token Configuration:

The first part is to initialize and configure the OTP token by managing the secure exchange of the shared key between the user's mobile phone and SP, also store the shared secret key securely on mobile phone.

Figure 4 show the steps.

1. User-A, known by SP_{-i} requests a shared secret key SK_i-A.
2. A nonce N_a is generated by the SP_{-i}'s server.
3. SP_{-i} sends N_a as an SMS to User-A.

4. The OTP Generator uses the MLTM to generate a non-migratable binding RSA key pair (K_{pu}-A, Kpr-A).
5. The public key K_{pu}-A is certified by the MLTM under an AIK. The OTP Generator sends the public key certificate (including K_{pu}-A) to the SP-i's server. Also, the OTP Generator generates a hash of K_{pu}-A and Na and sends the hash value to the SP-i's server.
6. The SP-i's server:
   (a) generates a hash value of N_a and the received $_{Kpu\text{-}A,}$
   (b) verifies that the received hash and the generated hash are equal in order to authenticate the user,
   (c) validates that the MLTM is genuine using the received certificate and
   (d) generates the shared secret key SK_i-A.
7. The server sends SK_i-A encrypted with Kpu-A, $Count_i$-A and a hash of both values and Na to the user mobile phone.
8. The OTP Generator stores $Count_i$-A and the value $E_K(SK_i\text{-}A)$ in the mobile phone securely and uses the MLTM to decrypt it when need.

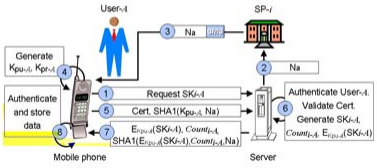


Figure 4: OTP Token Configuration

OTP Generation:

In OTP generation function we are using the SHA-1 algorithm for generating the OTP. In transaction based system the user sends OTP to SP every time. In order to generate OTP we are using counter and shared secret key. Fig.5 representing the flow.

Figure 5 Input parameters to the OTP generation function

V. CONCLUSION

Cloud computing has brought new challenges and opportunities for authentication. There is increasing demand for authentication to access services and data. At the same time, the cloud provides abilities such as centralized analysis and monitoring, and potential for new

and more accurate authentication techniques. Thus even though the risks of data exposure is high the cloud service providers are trying their best to provide a strong shield for the data stored in the cloud without slowing down their service. As per the proposed idea ;the implementation of Two factor Authentication in cloud computing will not only ensure that the data will be more secure but also give an edge to the security levels in cloud computing.

REFERENCES

1. Authentication in the cloud :a frame work and its application to the mobile users.
2. W.Li.D.Zhang,and Z.Xu,"Palm print identification by Fourier trans forms"Int.Journal of pattern Recogination and Artifical Intelligence.,vol 16,no.4,pp.417-432,2002.
3. New Palm Print Authentication System By using Wavelet Based Method
4. Towards Secure and Dependable Storage Services in Cloud Computing
5. C. Wang Q.Wang "Privacy preserving public auditing for storage security in cloud".
6. Zaigham Mahmood " Distributed and Intelligent Systems (DISYS) Research Group" Data Location and Security Issues in Cloud Computing" z.mahmood@derby.ac.uk.
7. Mohammed Alzomal "The Mobile phone as a Multi OTP using Trused Computing."

BIOGRAPHY

S.Shanmugapriya is received her B. Tech (IT) from Bharathidasan University Trichy and M.Tech (IT) from Sathyabama University Chennai. Her areas of interest are Java, Networking and Cloud Computing. She worked at Sathyabama University, Vellore Inst of Technology .She is having good experience in various IT projects and have attended in-plant training at BSNL, attended many work shops and seminars conducted by other colleges/universities. She is working as AP/HOD in the department of IT at MIET college of Engineering.

J.Gulzar Begam, is received her BE(CSE) from Anna university Chennai. Pursing ME at MIET college of engineering Trichy, Anna university. I worked for a software concern as Software Test Engineer.

M.Anitha: as done M.Tech at Bharathidasan University and B. Tech (IT) at Periyar University Salem. She was working with Angalamman college of Engineering Trichy. She had a role as ISO coordinator. She has attended work shops and Seminars in various colleges and universities.

Cynthia Napoleon Doing B.Tech (IT) at MIET College of Engineering, Anna university Trichy.