ENERGY CONSERVATION IN CLOUD ENVIRONMENTS USING ALTERNATIVE EMAIL-ID APPROACH

[1]B.KrishnaPrasad
Asst.Professor in CSE
VignanUniversity,Guntur

[2]Dr.K.Tirupathirao
Professor in CSE
KL.University,Guntur

[3]G.C.N.Mahesh
M.Tech student
VignanUniversity

Abstract(100%) Cloud computing is a new Model for deliver and accessing the services over the Internet. So cloud provider responsibility to verify the user or client is Authorized or not.For this purpose cloud provider shall provide some Authencatation mechanism and satisfying that cloud provider concludes that the client is Authorized. During the verification of authorizatation mechanism,In . Traditional way cloud provider uses the password and Biometric authentication mechanism. During this process Cloud provider shall maintain the large database for storing the biometric parameters like finger print ,images etc..and need a Computational resources to verifying that. Here it's the problem for wastage the resources. To Eliminate the for maintaining the Large database and computational resources we proposed a technique called Alternative E-Mail-ID+UniqueIdentatification Number (UIN)+Person identity information approach for Authentication purpose for cloud providers.

Keywords—Cloud Computing, Alternative EMail-ID, PII, Unique Identification Number (UIN)

Introduction :(100%) As computing becomes increases, the energy consumption to computing is climbing. At the same time, the cost of energy is rising due to the scarcity of finite natural resources which are rapidly diminishing. As a result Energy management in commercial datacenters is an application area of rapidly growing interest from both the economic and ecological perspectives. Business organizations want to save Energy without forgoing performance. Data entries are integral parts of cloud computing. Recently Cloud computing has takes the promising approach for delivering Information and Communication Technologies (ICT) services. In the process of providing these services it is necessary to improve the utilization of data centre resources which are operating in most dynamic workload environments. In this context IT practitioners are focusing on energy efficient methods to reduce consumption. This result in making datacenters both environmentally and financially efficient particularly in the context of the world-wide financial crisis and Virtualization is the enabling technology for providing services through cloud computing, and is the most promising software solution for energy optimization. In cloud computing environment several virtual machines are run on top of the server hardware. This way the hardware can be shared in a more optimal way by many users

However Clients are set up the Service level agreement (SLA) with the cloud providers for required services done by the registration process online using internet. At this stage cloud providers are prepare the link for accessing the Virtual machine for the client ,In this link consists of IP-Address of the Virtual Machine(VM),Unique identification number and pdf file of the person identified information sent to the Client Alternative EMail-ID. Because from the cloud provider point of view, cloud provider responsibility for verifying the cloud services accessed by Authorized client or not. To achieve this cloud provider propose Authentication mechanism of Alternative email-id Approach

In this approach client should submit the job to the cloud providers, then cloud provider provides a unique identification number immediately and sent to the client alternative emailed. Generally the client should share the regular email-id for his knowing peoples like officials ,friends etc.but he should not share the Alternative email-id here its achieves the some evidence for Authencatation in addition to this provide the Link consists of the VM-IPAddress,userid ,password for login purpose which is sent through the alternative emailed so client should install and install and login the user id, password along with the Unique identification number.so this context cloud provider also concludes Client is authorizes. we organizes the this paper section1 consists of the Brief Introduction about the Biometric systems. Section 2 covers the describes Proposed method Section3: PersonalIdentificationinformation (PII) Section-4:- How to achieves the alternative email-id for security services

Section1: Brief Introduction about the Biometric Systems: Using the biometric system, in bio metric system includes several methods for verifying the Authencatation. All these listed below along with the Disadvantages and advantages.

1) Facial recognition: Facial recognition is the process to verifying the Authencatation based on the facial expressions of the images. however the facial features is quite sensitive to variations in the environment (camera position, lighting, etc.) at enrollment.

Disadvantages

When the light is imposed on the person, whose the person ware the glass, then the 2D image is affected at that it is not possible to detect the regular facial expression

2) Voice recognition:it is the process of determing the behavior patterns, physical attributes from differ from one person to person. In the voice recognition, the user speaks a specific word, the vibrations of the size of the jaw opening and by tongue and lip shape and position—factors that make each person's voice unique. we should be analyze these parameters and compare with the database. If both matches ok otherwise Authencatation fail.

Disadvantages:

Suppose a person suffers some illness such as a cold, then change the person voice, at this time its difficult to .recognition

[Signature recognition:

Signature is the process to enrolls into the system by signing his or her name a number of times. The software analyzes the dynamic motions produced by the signer during each signature.

Disadvantages:

a. Signature verification is designed to verify subjects based on the traits of their unique signature. As a result, individuals who do not sign their names in a consistent manner may have difficulty enrolling and verifying in signature verification.]

DNA:

Disadvantages:

a. Extremely intrusive.

b. Very expensive.

Retinal scanning:

A retinal scan, is the process to identify the retina of the persons. Inthis scanning we determining the blood vessels in the retina. Suppose The retina absorb light energy more than the tissue of the surroundings are easily identified

Disadvantages:

a. it is potentially harmful to the eye

b. .its take more time for comparison depending on the size of the database

c. Very expensive

Iris recognition:is the process of determine the part of the eye between the sclera and the pupil

Once scanning the retina and recording the patterns of capillary blood vessels at the back of the eye then software creates the unique pattern for the blood vessels

Disadvantages:

a. A lot of memory for the data to be stored.

b. Very expensive

Fingerprint:

Fingerprinting is the process to determine the patterns like lines, arches, loops, and whorls.

An image of a fingerprint is captured by optical scanning ,or capacitance sensing.

Disadvantages:

If the skin of the finger changes while growing the age and some times the finger print alsonot working due to humidity with the hand

Hand Geometry:

Disadvantages:

a. Very expensive

b. Considerable size.

c. It is not valid for arthritic person, since they cannot put the hand on the scanner properly.

Proposed method : Registration process contain the 3 phases

General information phase(Client Perspective)+Personal identifiable information(PII)(Client perspective) +Generating the Unique identity number(Cloud provider perspective (generate))

At registration point of view Client context (Registration form contains General information + PERSONALLY IDENTIFIABLE INFORMATION (PII))

1) Client shall provide the requirements in Registration form provided by the cloud provider through the internet
2) Provide the Regular email id and Alternative Email –ID(here the alternative email has password)in the registration form
3) Fill the PERSONALLY IDENTIFIABLE INFORMATION (PII)
4) Note down the Unique identity number and maintain confidentially

Suppose Unique identity number forget ,then go for PERSONALLY IDENTIFIABLE INFORMATION (PII)

5) If PII is ok then cloud provider concludes Client is Authorized again generate another Identification number

Cloud provider context:

1)Cloud providers shall provide the registration form and based on the registration details cloud providers generate the application form for PERSONALLY IDENTIFIABLE INFORMATION (PII)

2)Verifying the Registration process complete, if Registration process complete then

3)Cloud provider shall prepare the VM based on the Service level agreement(SLA)

1) Cloud providers ask the Personal identification Information (PII)
2) Client should provide alternative email id at that time cloud provider shall provide the Unique identity number for the client authorization .here Unique identity number purpose is if two clients are have the same alternative email id ,at that time cloud providers resolve this issue based on the unique identity number

About PII: Identifying PII

PII is ―Any information about an individual maintained by the cloud provider, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

To Distinguish an individual is to identify an individual. Some examples of information that could identify an individual include, but are not limited to, name, passport number, social security number, or biometric data

In contrast, a list containing only credit scores without any additional information concerning the individuals to whom they relate does not provide sufficient information to distinguish a specific individual.

To trace an individual is to process sufficient information to make a determination about a specific aspect of an individual‘s activities or status. For example, an audit log containing records of user actions could be used to trace an individual‘s activities.

Linked information is information about or related to an individual that is logically associated with other information about the individual. In contrast, linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable[3]

Generation of unique identification Number When the client submitted the job to the cloud provider through internet ,then cloud provider provide the unique identification number with help **of Interfac**e the mechanism involves The role of the jobs submitted to the through via Interface can take time to execute. So, after submitting the job unique id is allotted to every job for user's reference. This id can be used to monitor the status of jobs at any point of time. The job details which are provided includes status of the job (whether it's running or its over), time taken to complete the job, errors if any, and the output. The job details and status of the job is gathered by querying

Algorithm1:

INPUT : From Client to Cloud provider

OUTPUT: Client accessing services from the Cloud

```
    1]  Submitting the Job
    2]  Note down the Unique Identity Number and kept in Confidentially. Enter both Regular and alternative EMail-ID(both have passwords )
    3]  Install the VM and login with the User-ID(Alternative EMail-ID),Password and Enter the Unique Identity Number
    4]  If (Unique Identity Number =True)
    5]  Permitting the accessing the services from the cloud
    6]  Else
    7]  Will Answer the Questions based on PII
    8]  If(PII =True)
    9]  Generate the another Unique Identity Number
   10]  Go To Step 4
   11]  Else Stop.
```

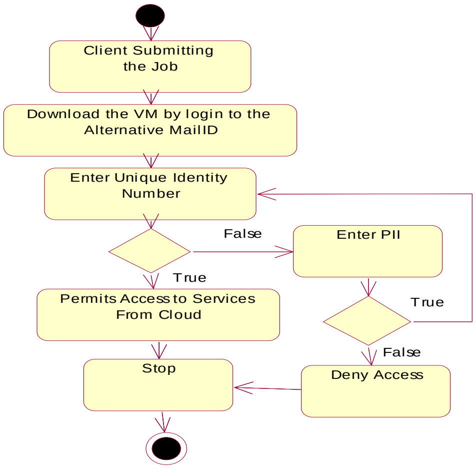
Algorithm:2

INPUT: From Cloud provider to Client

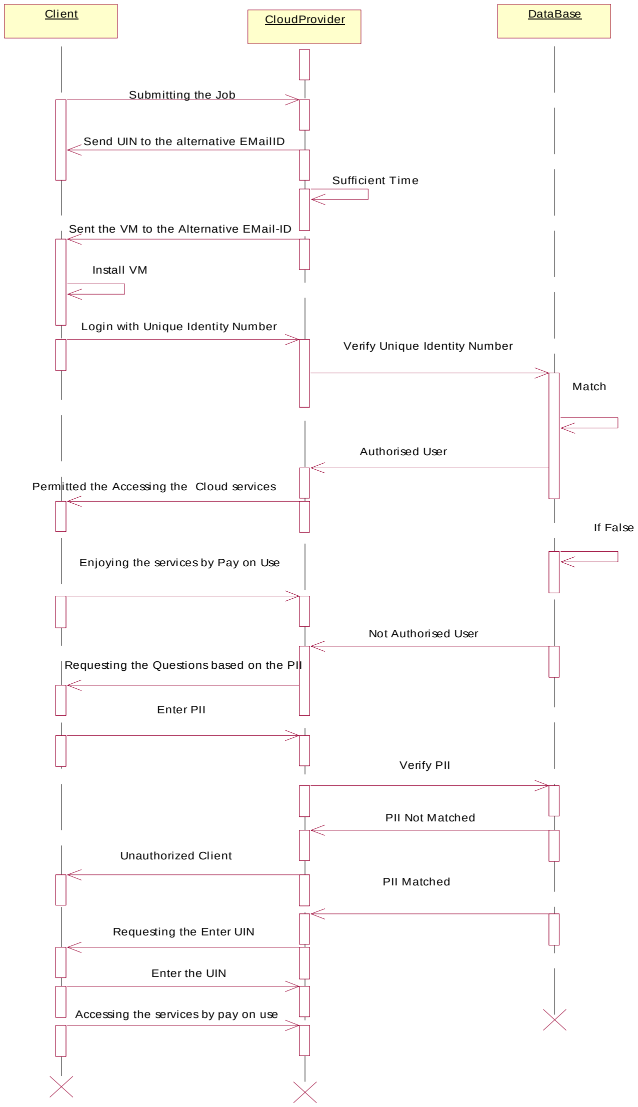
OUTPUT: Cloud provider shall give the assurance, Authorized Client only accessing the Cloud services from the Cloud.

```
   1]  Processing the Client Job and Generate the Unique Identity number based on the Cloud Sci Interface Clients
   2]  Accepts the Requests From Clients
   3] Sending VM to the Client Alternative EMail-ID. Requests Clients Unique Identity Number
   4] Verifies the Alternative EMail-ID,Password and Unique Identity Number
   5] If (Unique Identity Number = True)
   6] Permits the Access
   7] Else
   8] Will Generate Question the Client based on PII
   9] If(PII =True)
  10] Again Requests Unique Identity Number From Client
  11] Go To Step 5
  12] Else Stop
```

Activity Diagram



Client Submitting the Job
Download the VM by login to the Alternative MailID
Enter Unique Identity Number
False
Enter PII
True
Permits Access to Services From Cloud
True
False
Stop
Deny Access


Client
CloudProvider
DataBase
Submitting the Job
Send UIN to the alternative EMailID
Sufficient Time
Sent the VM to the Alternative EMail-ID
Install VM
Login with Unique Identity Number
Verify Unique Identity Number
Match
Authorised User
Permitted the Accessing the Cloud services
If False
Enjoying the services by Pay on Use
Not Authorised User
Requesting the Questions based on the PII
Enter PII
Verify PII
PII Not Matched
Unauthorized Client
PII Matched
Requesting the Enter UIN
Enter the UIN
Accessing the services by pay on use

Authentication : cloud provider provide the VM-IP-Address based on the SLA sent to the client alternative e mail id .here one question arises from researcher point of view why we are choosing the alternative email-id instead of regular email id -- because the regular emailed should share almost all knowing people .so attacker point view analyzing the regular emailed and guessing the password based on the some parameters like one can often make an educated guess about a person’s technical ability, employment, and social savvy based on an email address — and those guesses (whether correct or not) may be unfavourable. For example, here are some stereotypes:

- At the very bottom of the email address hierarchy are addresses from an ISP — that is, addresses ending in @att.net, @comcast.net, @cox.net, @earthlink.net, @anything.rr.com, @verizon.net, and so on. These betray perhaps the worst misconception, which is that you must accept what your ISP offers or that there are no better alternatives (there are always better alternatives to an ISP’s email). And they suggest that you’re stuck with your provider, because switching ISPs would mean giving up that email address.
- Addresses from Hotmail, Yahoo, Excite, Juno, and similar free email providers imply that you don’t take email very seriously, and may suggest a holdover from student days. And it’s distinctly worse if you have a computer-suggested name like

- jsmith487@hotmail.com rather than, say, johnsmith@hotmail.com (which at least tells me you're an early adopter). A Gmail address suggests you're more sophisticated than the average email user, but not sophisticated enough to set up Gmail with your own domain name (or perhaps too poor — custom domain names used to be free but now require a paid Google Apps subscription, at $50 per user per year). In particular, when I get business email from someone using a gmail.com address, I have to wonder what kind of employer can't spring for a professional-looking domain name or why the sender is choosing to send from a personal address instead of a work address.

personal details ,business details etc so trace out the password. so this method is not secure. That's why introduce the concept of alternative email-id. Because of the Attackers point of view he/she should not expected about the alternative Email-id. At cloud provider context also Client login the VM-IP-Address with the user id (Alternative Email-id)and password, at that time Cloud Provider shall give the assurance. in addition to this client should enter the Unique identity number provided by the Cloud provider. Again its verifies with the help database and if true then cloud provider concludes the client is authorized. So cloud provider will gives the access to services from the cloud. This achieves the **Authorization, Confidentiality AND Integrity** .

Access Control: Cloud environment pay per use. So cloud provider should doubtful for accessing the services. At that time he resolve the issue by displaying the warning message and imposing the questions based on the PII. Client Shall give the answers correctly then again generate the Unique Identification number and sent to the alternative email id of the client. Then client verifies his alternative email id and enter the unique identification number .if yes then client authorized. in this way cloud provider achieves the access controls .

Non-Repudiation: Cloud providers shall provides the Service level agreement with the client so no concept of Non-Repudiation

Refrences:

[1] K. Thirupathi Rao, L.S.S.Reddy, P. Sai Kiran, V. Krishna Reddy, B. Thirumala Rao--GENETIC ALGORITHM FOR ENERGY EFFICIENT PLACEMENT OF VIRTUAL MACHINES IN CLOUD ENVIRONMENT--2010 International Conference on Future Information Technology(ICFIT 2010))

[2] Rohitash Kumar Banyal, Pragya Jain, Vijendra Kumar Jain Multi-factor Authentication Framework for Cloud Computing 2013 Fifth International Conference on Computational Intelligence, Modeling and Simulation

[3] Erika McCallister ,Tim Grance ,Karen Scarfone Recommendations of the National Institute of Standards and Technology (GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII))

[4] Cloud Computing principal By RajKumar Buyya