ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Cloud Computing Security and Trust Enhancement by Using OTP

Santosh Kumar Singh, Dr. P. K. Manjhi, Prof. (Dr.) Rajesh Kumar Tiwari

Research Scholar, Dept. of Computer Applications, Vinoba Bhave University, Hazaribag, Jharkhand, India

Assistant Professor, University Dept. of Mathematics, Vinoba Bhave University, Hazaribag, Jharkhand, India

Senior Prof., Dept. of Computer Science & Technology, R.V.S Coll. of Engg. & Tech, Jamshedpur, Jharkhand, India

ABSTRACT: Cloud computing provides the capability to use computing and storage resources on a rented basis and reduce the investments in an organization's computing infrastructure. With all its benefits, cloud computing also brings with it concerns about the security and privacy of information extant on the cloud as a result of its size, structure, and geographical dispersion. Secure communication in cloud environment is necessary to access remote resources in a controlled and efficient way, the security to access the cloud also need to be tightened, not just to rely on usernames and passwords but also to the dynamic code of the mobile token which is difficult to be cracked. Dynamic mobile token is an application which is planted in the mobile phone to generate a code that was formed by the method of one time password and can only be used for one login session or transaction. This technique is very much secured, robust and highly efficient. The produced mobile token which is valid for only a small session is used by client to authenticate itself. The purpose of this paper is focus on granting and authenticating data, while these data are transferred over cloud to gain the trust from the provider and aims to focus on the security, privacy and trust issues. Our work mainly deals with cloud computing security model.

KEYWORDS: Cloud Computing, One Time Password, Mobile Token, MD5, Security and Access Control.

I. INTRODUCTION

Cloud computing is an internet techniques that uses central remote servers to keep, stores data and applications. Cloud computing enables consumers and firms' employees to use applications without the needs to install special software's, this technology allows more efficient computing by centralizing storage, memory, processing and bandwidth [1]. Cloud computing allows delivering hosted services over the Internet by using software that is installed on computer based on client-side. Cloud computing can be summarized by three segments: applications, storages, and connectivity, Cloud computing is independent computing as it is totally different from grid and utility computing, an example of cloud computing is Google Apps, it enables to access services via the browser and deployed on millions of machines over the Internet [2]. The architecture of cloud computing can be classified to three types of models' services, namely Infrastructure as a service (IaaS), Software as a Service (SaaS) and Patform as A Service (PaaS) [3-5]. In cloud computing, the available service models are:

- 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.
- 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.
- Software as a Service (SaaS). Provides the consumer with the capability to use the provider's applications running on a cloud infrastructure.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

The concept of one time password (OTP) is that it is only valid for a single login session or transaction [6]. It is widely used as a password that is not static in the database, but only as a single use password. The use of encrypted static passwords are also not immune from the attack by using a key logger [7] or sort of it, because if an attacker managed to get the main password and OTP password still login and transactions will not be processed because the password is no longer valid. Code generation as encryption is using Message-Digest Algorithm 5 (MD5) which is widely used with 128-bit hash value. This algorithm has been widely used for security applications, password encryption, and integrity test of a file [8].

The application of Dynamic Mobile Token uses three codes consisting of epoch time as the key of one time password, the value of the "secret" variable in which each user has a different value so that when it degenerate at the same time, it will result in different value, and 4 digit random value between 1000 and 9999 resulting from the website. These three values are then combined and encrypted with md5 algorithm to generate the output of the value of 128 bits or 32 hexadecimal numbers. Only first 6 digits of the hexadecimal number are used from the result of the output.

Traditional hardware based appliances had no control over data once it is in cloud. Therefore it requires the use of virtual security appliance to protect and maintain the data. There are various security layers, some of them are:

(1) Authentication: Authentication identifies a user. More clearly, authentication is process of determining whether someone or something is, in fact, who or what it is declared to be. Authentication level description: (A). Single factor authentication: it requires only one factor which "something user knows" like username and password. (B). Multistep authentication: requires multi step authentication process which must be executed in consecutive order or sequence successfully. Example: Gmail, BOX. (C). two factor authentication: it is the subset of two steps. It requires the use of only two factors from the below list: Something you know (password, pin) something you have (token, key) Something you are (fingerprint, retina scan etc.) Example: PKI system (D). Multi factor authentication: it requires the use of three or more factors from below list: Something you know (password, pin) something you have (token, key) Something you are (fingerprint, retina scan etc.) Example: key card entry system

(2) Authorization: Authorization provides authenticated users with permissions to certain resources. These resources can be system objects like information, application programs etc.

(3) Encryption of data: encryption is core basis in cryptography. It is the process of transforming information in an unreadable format or we can say it convert plain text into cipher-text and hence become unreadable. Data stored on PC, tablet, smart phones can be encrypted based on type of data. One of the biggest issue in cloud computing is that of security. As organizations and individuals moving their data to cloud, the safety of their data is a crucial factor. The main objective of this paper is to enhance data security for cloud computing. For authentication security purpose instead of only rely on username and password, an additional multi-auth-app has introduced which is based on two factor authentication with multi steps for creating mobile token which is valid for one login session or for short period. The generated mobile token is then used by client to authenticate itself for using cloud services. The data storage security is implemented by using AES encryption technique. It is a symmetric encryption technique and is very reliable and faster algorithm. This paper resulted in authentication and registration method that is both secure. Permissions for access rights like grant or deny on data are also get implemented. MD5 technique is used for hashing client registration and login details. Hashing is for verifying the contents of message. Hence, our approach also maintains data integrity. In this paper we are going to present work and its implementation details using Eucalyptus.

This paper organized in following manner: In Section II, we are introducing the concept and the necessity to adopt one time password (OTP) for granting and authenticating data hosted by the Cloud provider. Detailed proposed work presented in section III. In section IV, we will present proposed work implementation. Section V concludes the paper.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

II. OTP (ONE TIME PASSWORD)

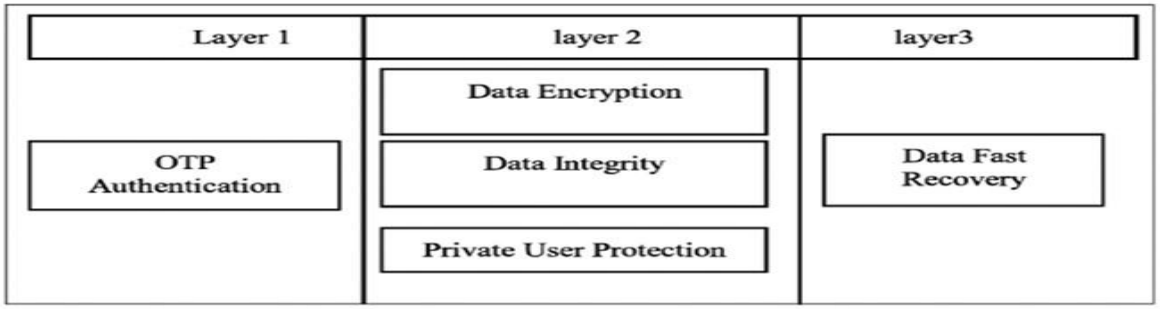

Fig.1. Model of the three-tire data protection

In Fig. 1 Layer (1): is Class authenticate users accessing the cloud, the solution often applied is to use one-time password (OTP). The system requires high security authentication, which requests from both sides: users and vendors, but vendors with cloud-free. Layer (2): This layer ensures Data Encryption, integrity of data (Data Integrity) and protects user privacy (Private User Protection) through an encryption algorithm for value. Layer (3): Class user data recovery serves for fast data decoding speed.

There are various methods to implement one time password (OTP) technique, which are as follows [9]

a) Time Synchronization - In this technique, both the client and server will have synchronous time clocks and it use an algorithm that generates one-time password from that synchronous time and any other inputs (PIN). In this time is used as the changing factor, which changes every 60 seconds. The token time must be synchronized with the authentication server time. That is, if the authentication server and the user token don't keep the same time, then the expected OTP value won't be produced and the user authentication will fail.

b) Event Synchronization – In this method, both the client and server will typically have an identical initial seed i.e. counter value. Whenever client wants to login, it generates a one-time password from the initial seed and any other input (PIN) and updates the seed (increment/ decrement the counter). User submits this one-time password generated to server. Server also generates the password for that instance using the seed (counter) and other inputs. If both passwords match, the server authenticates the user and updates the seed (increment/ decrement the counter).

c) Asynchronous Challenge-Response Technique –In this technique, every time the application presents a dynamically generated unique challenge to the user when it tries to login to server. User enters this challenge into the client software. Then the client software use some crypto primitive technique to generate a unique password by the combination of challenge and any other information (PIN) provided. Each time server generates a new challenge for user when it wants to login. This offers good security because this offers good security because the intruder has to start the brute-force search from scratch every time a new one-time password is generated.

PASSWORD MODE

Dynamic Mobile Token there are two modes used [10, 11]:

1. Challenge/Response Mode (C/R) [12]
   This mode is most often used when doing transaction. In this mode the server provides a challenge in the form of a series of numbers. That number must be entered into the Mobile Token to get an answer (response). Then the user enters the number that appears on its own Mobile Token into text box on the website. Mobile Token will issue a different code though with the same code challenge. Periodically depending on the time when we answer the challenge in a token.
2. Self Generated Mode (Response Only) in this mode the server does not give any kind of value (challenge). Mobile Token users can directly issue a series of combination of numbers and letters without having to enter the challenge. As the mode C/R, Mobile Token also issued different codes periodically depending on the time when the token is ordered to produce self- generated code.

One time passwords (OTP) are generated based on three parameters-

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

1) The current time.
2) The 4-digit PIN code

Strong authentication system along with virtual private network: A secure cloud solution for cloud computing

3) Init-secret

These three parameters are then hashed together with MD-5 and will generate an OTP, which will then used by user to login. At the server side, server knows 4-digit PIN code and Init-secret, for proving authentication it will also calculate OTP by using current time of the server. As, it is based on time synchronization technique so mobile time and server time must be properly synchronized If calculated OTP and received OTP are same, then user will allowed to access the cloud. Since time is part of the hash, so OTP is valid only for three minutes. During the registration process and at the time of login and even when user accesses the services from the cloud lots of important information is transmitted through the network. For securely transmitting all the information between the client and server secure socket layer has been used. HTTPS protocol has been used for that purpose. It is responsible for transmitting all the information in secure manner. The main concept of HTTPS is to create a secure channel over an insecure network. This ensures reasonable protection against eavesdroppers attack and man in the middle attack, provided that adequate cipher for data is used. For securely transferring all the information AES-256 encryption technique has been used. It will encrypt all the information by using this encryption technique so that sensitive information doesn't disclosed to anyone.

III. PROPOSED SYSTEM

This section describes a proposed data security model and focuses on enhancing security by using two factor authentications, encryption, hashing, and access rights policy. The security framework will take care of authorization and authentication, confidentiality and integrity of user while accessing any cloud server.

The Fig. 2 below shows that how authentication will be carried out. Steps which will going to involve during authentication is listed below

- A client wishes to log in will surfs to the login page.
- The client then starts an application on a mobile phone, and enters a PIN code.
- After entering the PIN code, OTP is generated and displayed on the phone.
- The client enters his username and the OTP at the login page, and sends the information to the authentication server.
- The server either permits or denies the client to access the cloud.

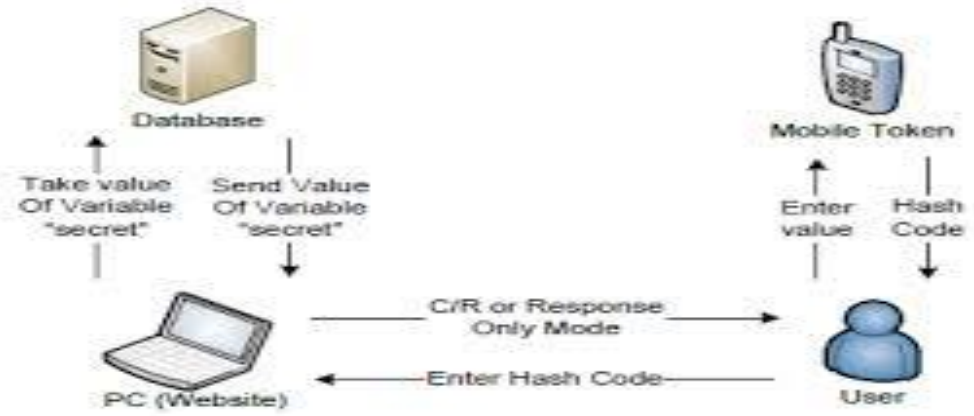

Fig.2. Steps for Authentication

Enrollment: A new device enrollment is a critical step because Cloud should be sure that this device is authenticated and not a source of malicious activity. A device enrollment should be performed with two factor authentication. The second factor could be an OTP (one time password) sent as an SMS to the phone number associated with the account,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

or an OTP preset on any other device, which was already enrolled. For each new device the account owner should be notified by email.
How it works step by step:

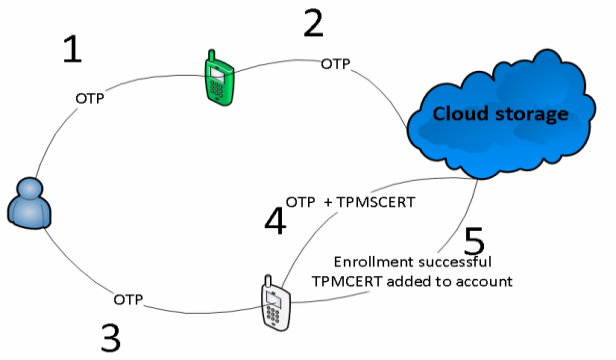

Fig.3. Device Enrollment

1. As shown in Fig. 3 User generates an OTP on a device enrolled previously;
2. Generated OTP goes to cloud;
3. User enters the OTP on a new device;
4. Device generates a TPM (trusted platform module) signe Certificate request (TPMCRT);
5. If OTPs from steps 2 and 4 are equal, the enrollment is successful.

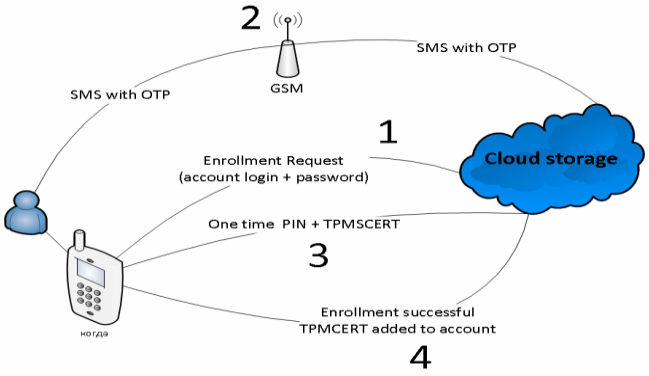

Fig.4. New Device Enrollment

In the case of a new device:

1. As shown in Fig. 4 New device performs an enrollment request with a login and a password;
2. Cloud sends SMS with an OTP to an associated phone number;
3. New device sends TPMCRT + OTP;
4. If OTPs from steps 2 and 3 are equal, the enrollment is successful.

TPMCRT is

1. Client device generates a private key and a certificate request for each enrollment;
2. TPM signs Certificate request (TPMCRT), so we get a unique device certificate.

Benefits:

- In a case of credentials leak, an attacker can't enroll a new device, and get user's data;
- If an attacker has an access to an enrolled device and can generate an OTP for a malicious device, the victim will get a notification.

Proposed Work:

Registration: Firstly users who want to access the cloud services have to register themselves as shown in Fig. 5 in which using flow chart showing process of authentication. A registration form has to be filled by them which include client information. All the user information now gets stored in cloud database. As registration mechanism includes

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

crucial information, this must be protected from others. For the security purpose MD-5 hashing is used by the authors on registration information. User information now gets stored in cloud where password and all the other details are stored in hash format using MD-5 hashing so that any attack by malicious users would be ineffective and hence also maintains integrity. Md-5 hashing is a one way system and is unbreakable [8].

Login and Data Authentication: The authentication method used in our scheme is based on two factor authentication that add an extra layer of security to the existing schemes [13] and make it stronger.

This solution offers greater benefits when compared to other types of authentication solutions:

- Username and the OTP are the only crucial information, sent over the network. Since the OTP is only valid for very short time it will be of no value for an attacker.
- PIN code is only known to the user which is used to generate the OTP on mobile phones.
- The cost will be absolutely free for both user and provider, since this is an open source solution.
- The user only have to carry his mobile phone with him and there is no need to carry any extra authentication device
- Easy registration process where everything can be done from home, no need to order an external authentication device or get the device from a local office.

As a result only authorized users can gain access to the cloud system.

Secure storing and accessing of data: After successful authentication, a user can now connect with the system. User can now have access to file storage system. For Encryption during file upload AES-256 has implemented in this application for secure data storage on server. AES as compare to RSA, DSA, and RC4 is much better encryption technique because its algorithm fast and reliable. AES-256 is symmetric key encryption technique. For other information transmission including registration and login details MD-5 hashing is used.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

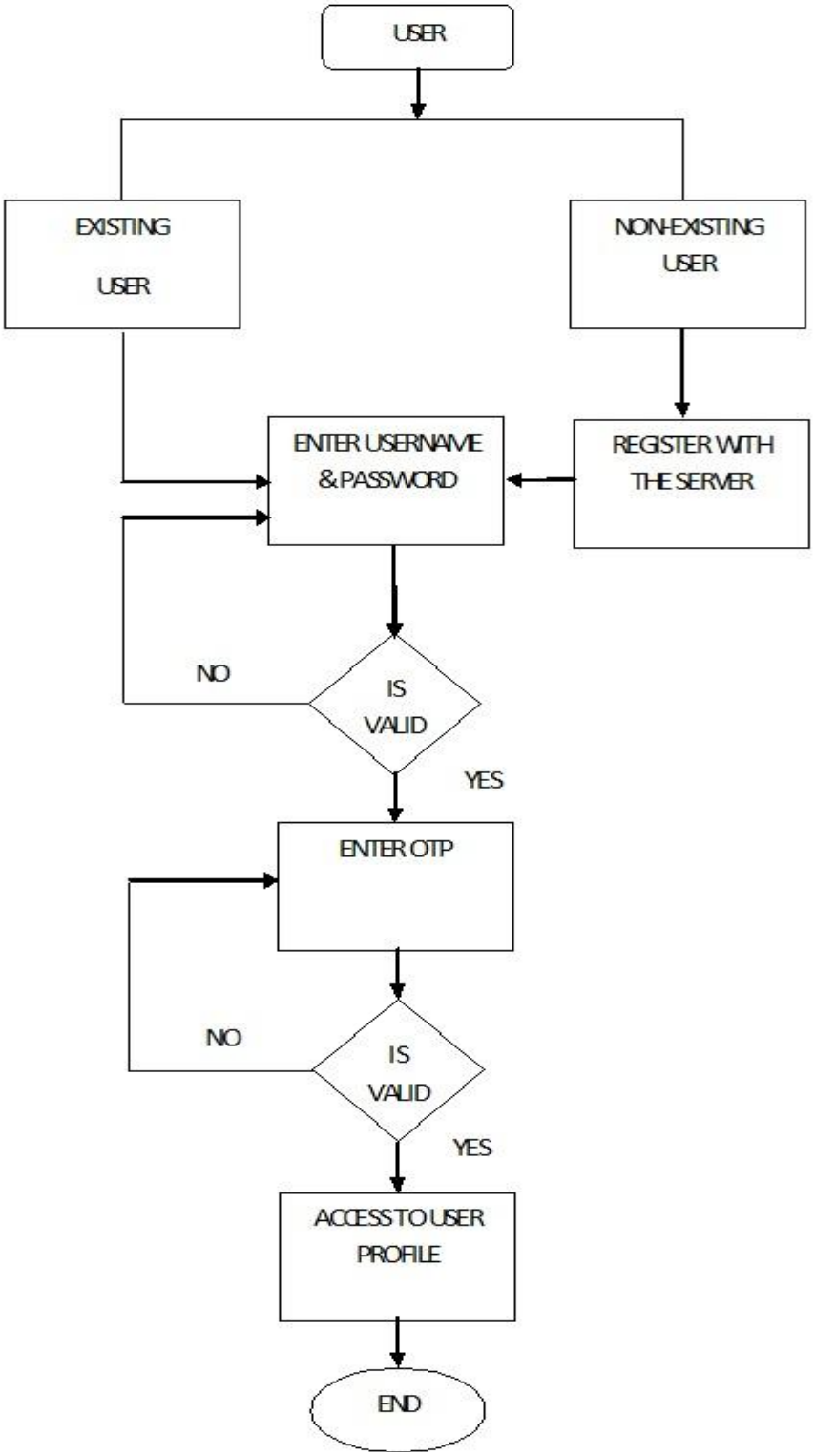

Fig.5.Flow chart showing AUTHENTICATION

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

IV. IMPLEMENTATION OF PROPOSED WORK

To securely manage our applications on our own cloud infrastructure provided by Eucalyptus as shown in Fig. 6, using IMOD (Infrastructure and Middleware on Demand), we need to perform the following 3 tasks: (1) Register Your Cloud, (2) Setup Your Eucalyptus Account, (3) Create SSH Keys (Creation of SSH keys is similar to AWS Account's SSH Key)

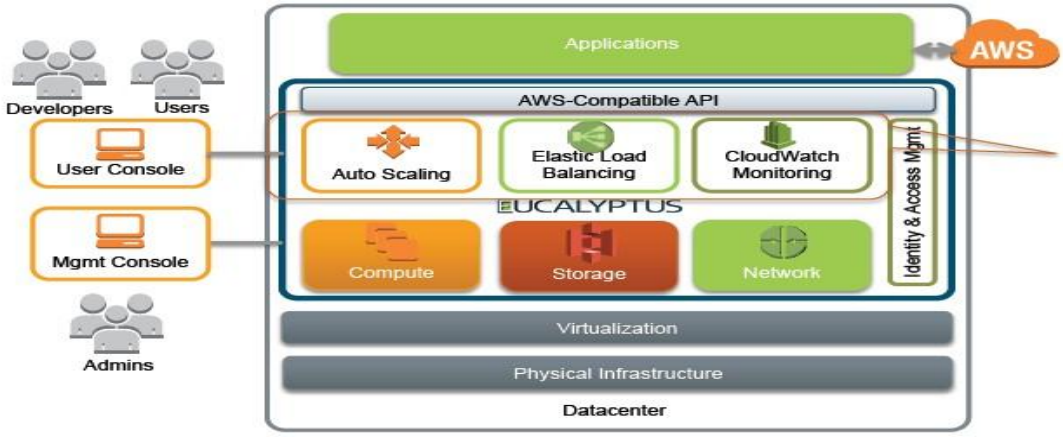

Fig.6. Eucalyptus block diagram

Register Eucalyptus Private Cloud: After logging in IMOD we need to go to the Kaavo's IMOD's account profile page, click on 'Register Your Private Provider' and fill the required information, as showing in Fig. 7, (1) Give a unique name to your Cloud (2) Provide the IP/DNS of your host running the Eucalyptus Cloud Controller. For testing we can also use the public instance of the eucalyptus cloud (mayhem9.cs.ucsb.edu) running at University of Santa Barbara, it is down quite often so it is best to setup our own private cloud and configure it in IMOD for management. (3) Provide the Port (default value is 8773) of the Web Services running on your Cloud Controller. (4) Finally provide the Time Zone (for mayhem9.cs.ucsb.edu, the Time Zone is GMT) of our Cloud Server. Once we click on 'Create' button our Cloud will be registered with IMOD and a hyperlink, with the name of our Cloud, will be added to the Providers tab.

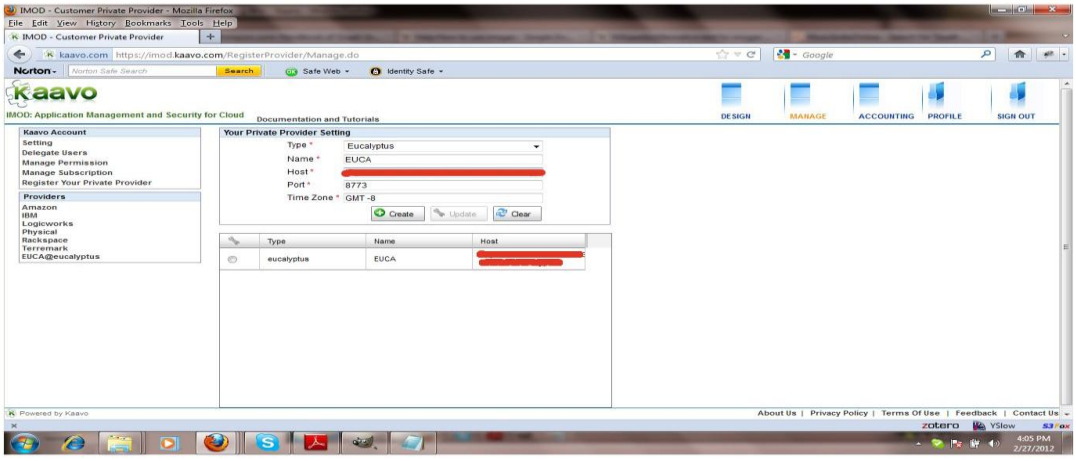

Fig.7. Eucalyptus Cloud Register

The model which we propose in the present scenario works like this:

- The user logs in to the system using Mobile OTP.
- Server I is the cloud controller which is used to access various installed applications on Server II.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

The proposed model as shown in Fig. 8 can be built using an Ubuntu Enterprise Cloud using three machines in which we use two servers, Mobile phone is used to authenticate server I and access the private cloud. Now sever I comprise of cloud controller which is used to control server II .For creating this entire Model we use Eucalyptus cloud. Eucalyptus is software available under GPL that helps in creating and managing this private cloud. It provides an EC2-compatible cloud computing platform and S3-compatible cloud storage platform.
Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems) has become very popular and is seen as one of the key open source cloud platforms. Since Eucalyptus makes its services available through EC2/S3 compatible APIs, the client tools written for AWS can be used with Eucalyptus as well. Cluster Controller manages one or more Node Controllers and deploys/manages instances on them. CC also manages the networking for the instances running on the Nodes under certain types of networking modes of Eucalyptus.

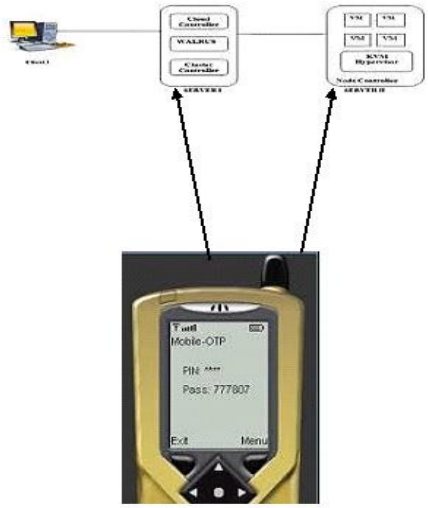

Fig.8. Working System

Benefits of OPT in cloud computing:

- OTP offers strong two-factor authentication.
- The OTP is unique to this session and cannot be used again
- OTP offers strong security because they cannot be guessed or hacked
- Provides protection from unauthorized access Easier to use for the employee than complex frequently changing passwords
- Easy to deploy for the administrator Good first step to strong authentication in an organization
- Low cost way to deploy strong authentication

V. CONCLUSION

Cloud computing is a promising technology with profound implications not only for Internet services but also for the IT sector as a whole. Unfortunate, several obstacles issues are exist; particularly these issues are related to service-level agreements (SLA), security and privacy, and power efficiency. One time password authenticates users and MD5 hashing for hiding information. This model ensures security for whole cloud computing structure. In this paper we have identified generic design principles of a cloud environment which stem from the necessity to control relevant vulnerabilities and threats so, in this paper we have proposed to make use of Dynamic one time password with two factor authentication as a strong authentication technique which requires mobile phone as an authentication device. In this technique mobile phones are responsible to produce OTP which is valid only for 3 minutes. A combination of

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Mobile OTP and SSO can address most of the identified threats in cloud computing dealing with the integrity, confidentiality, authenticity and availability of data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh through federations, within which essential trust is maintained.

BIOGRAPHY

Santosh Kumar Singh is a Research Scholar in the Department of Computer Applications, Vinoba Bhave University, Hazaribag, Jharkhand. He received M. Phil (Computer Science) degree in 2011 from MBU, Solan, H.P, India. His research interests are Cloud Computing, Parallel and Distributed Computing etc.

Dr. P.K.Manjhi is Assistant professor in the University Department of mathematics, Vinoba Bhave University, Hazaribag, Jharkhand, India.

Prof. (Dr.) Rajesh Kumar Tiwari is HOD of Department of Computer Science & Technology R.V.S College of Engg. & Tech.Mango, Jamshedpur, Jharkhand

REFERENCES

[1] Karwasra, N., & Sharma, M. "Cloud computing: security risks and its future". International Journal of Computer Science and Computer Engineering, Special Issues on Emerging Trends in Engineering, pp.5-9, 2012.
[2] Shaikh, F. B., & Haider, S., "Security threats in cloud computing". Proceedings of 6th International Conference on Internet Technology and Security Transaction, Abu Dhabi, United Arab Emirates (UAE), pp. 214-219, 2011.
[3] Subashini, S., & Kavitha," A Survey on security issues in service delivery models of cloud computing". Journal of network and computer application ,elsevier pub, vol.34(1) ,pp.1-11, 2011
[4] Mell, P., & Grance, T., The NIST definition of cloud computing. NIST U.S.Department of commerce. Special Publication ,.800-145, Gaithersburg, MD, 2011.
[5] Zhang, Q., Cheng, L., & Boutaba, R., "Cloud computing: State-of-the-art and research challenges". Journal of Internet Services Applications(2010), 1:7-18, doi:10.1007/513174-010-0007-6.
[6] Dr. Mark D. Bedworth PhD BSc FSS. "A Theory of Probabilistic One-Time Password". Computer Science Computer Engineering and Applied Computing, Security and Management. Vol-1,Issue-4, pp.38-43, 2013.
[7] Jeyachandran, A., & Poongodi, M. (2018). Securing Cloud information with the use of Bastion Algorithm to enhance Confidentiality and Protection. International Journal of Pure and Applied Mathematics, 118(24).
[8] Kiddo. 2010. Hacking Website: Menemukan Celah Keamanan & Melindungi Website dari Serangan Hacker. Mediakita, ISBN-9797942686.
[9] Ronald Rivest, "MD5 Message-Digest Algorithm", rfc 1321, April 1992.
[10] "Privacy and consumer risks in cloud computing", Dan Svantesson, Roger Clarke, computer law & security review 26 (2010) 391e97, @ 2010 Svantesson & Clarke. Published by Elsevier Ltd. doi:10.1016/j.clsr.2010.05.005.
[11] N.Haller,Bellcore,and C. Metz. " A One-Time Password System. Kaman Sciences Corporation". https//tools.ietf.org/html/rfc1938. Year 1996.
[12] Fadi Aloul, Syed Zahidi, Wassim El-Hajj. "Two Factor Authentication Using Mobile Phones". Digital Library Telkom Institute of Technology (IEEE), AICCSA pp.641-644, 2009.
[13] Arya Sapoetra Y. Rancang Bangun Arsitektur Library Sistem Autentikasi One Time Password Menggunakan Prosedur Challenge-Response. Informatics Engineering, Pembangunan Nasional "Veteran" University, East Java, 2010.
[14] S.Zhang & X. Chen,"The Comparison Between Cloud Computing and Grid Computing", Computer Application and System Modeling (ICCASM), International Conference. 22- 24 Oct . 2010. pp: V11-72, 2010.