ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue IX, September 2016

An Approach towards Security in Heritage Cloud Using OTP System

Rishi kumar sharma[1], Dr. R.K.Kapoor[2]
Research Scholar, Computer Science, AISECT University, Bhopal, India[1]
Associate Professor, Computer Science, NITTTR, Bhopal, India[2]

***Abstract*— Cloud storage services is one of the most popular services in cloud computing technology. A crucial problem to be addressed in the cloud storage care the security mechanism of protecting the private data and shared data with other users. Since data are moved into cloud data centers, which run on virtual computing in the form of virtual machine, there are a number of security problems which are yet to be met. In this paper, we present a heritage technique to protect the security of owner's data and enforce the data access control. This technique forms amulti cloud system where child cloud is exist for multiple users for data storage offering lesser load on client systems there by using the cloud computing technique. This technique introduces a base cloud controlled by a single administrator which provides the data backup for child cloud after undergoing specific segmentation and encryption algorithms to ensure security and integrity of data. The generate one time password is then used by user to authenticate itself to the heritage cloud. The following paper aims to focus on the security, privacy and trust issues.**

***Keywords*- cloud computing, heritage key management System, One Time Password.**

I. INTRODUCTION

"Cloud computing is a model for a enabling suitable, on demand network access to a shared pool of configurable computing resources that can be soon provisioned and released with minimal management effort."

Cloud computing offers data storage system which enables the users to be less dependent on the client system and provides an architecture to upload data in a cloud that can be shared by multiple users and also provide security through authentication of the end user. The system proposed in this paper offers a robust and secure architecture which allows the data security of user as well as protects the system against other external agents. This system also offers an extensive usability model which helps the user to communicate with the cloud with the help of various devices having different OS platform. The proposed heritage cloud architecture of cloud computing offers an additional level of security in which data is uploaded in the base cloud after undergoing encryption followed by segmentation of data.

The concept of one time password (OTP) is that it is only valid for a single login session or transaction [1]. The use of encrypted static passwords are also not a immune from the attack by using a key logger [2] or sort of it, because if an attacker managed to get the original 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 [3]. If you make the login process too hard for a user, the user might grow tired of that service. It is also vital for the cloud providers to have good security standards in order for the common users to trust the cloud, for future rise of the cloud technology.

II. METHODOLOGY

There are different methods to implement one time password (OTP) technique, which are as follows [6] :

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

b) Event Synchronization – During this methodology, both the client and server can normally have an identical initial seed i.e. counter value. Whenever client wants to be login, it produce a one-time password from the initial seed and any other input (PIN) and updates the seed. User submits this one-time password produced to server. Server also produces the password for that example using the seed (counter) and other inputs. If both passwords match, the server authenticates the user and updates the seed.

c) Asynchronous Challenge-Response Technique – During this methodology, all time the application presents a dynamically generated peerless challenge to the user when it tries to login to server. User enters this challenge into the client software. Then client software use some crypto primitive technique to produce a unique password by the combination of challenge and any other information (PIN) provided. Every time server produce a new challenge for user

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue IX, September 2016

when it wants to login. This proposal good security because This proposal good security because the pusher has to start the brute-force search from scratch all time a new one-time password is generated.

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

1) The current time.
2) The 4-digit PIN code
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 PC 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. BENEFITS OF OTP IN CLOUD COMPUTING

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

IV . PROPOSED WORK

This architecture proposes a child cloud and abase cloud to incorporate a multi cloud system to ensure data integrity and security in cloud computing. The sub system of multi cloud architecture are as follows:

Child cloud:

The child cloud can be created using centrally built software which enables the child cloud to fall under the category of SaaS (software as a service) cloud computing model. The child cloud consists of a group of systems which are interconnected through LAN which in turn forms the child cloud. The internal users can access the child cloud through the same LAN where as the external users can access the child cloud through devices supporting a web browser using GPRS services. This model thus enables multiple users to access the child cloud simultaneously. The child cloud also maintains security of data by authentication of the user accessing cloud. A user can only access data after suitable authentication is met. This is done by administrator and hence a user is only permit to access his data in the child cloud.

Administrator:

The administrator is the most indiscernible part of this architecture as it is responsible for the efficient functioning of the child and the base clouds. The main functions of administrator are:

a. Data encryption: The data gathered from the child cloud is encrypted using the RSA data encryption algorithm to maintain the security of data.

b. Data segmentation: The encrypted data is then segmented using the data segmentation algorithm .This results in data to be divided into chunks which are stored in isolated systems in the base cloud. Each chunk is in an unreadable format to ensure data security of a high level.

c. Data decryption: Whenever the user requests for a file, the file is retrieved from the base cloud .The data so retrieved from the base cloud is in an unreadable encrypted format. For the file to be back in its original forms data decryption takes place. The data retrieved from the base cloud is uploaded to the administrator who in turn performs decryption code to get the data in its real form. This is then sent to the child cloud to user. The data sent is user specific and can only be sent to the authenticated users. The user authentication is done by the administrator & child cloud to maintain integrity of data.

Base cloud:

The Base cloud falls under the same SaaS(software as a service) cloud model similar to the child cloud. Base cloud is consumed for storing a backup of the data & information stored in the child cloud in an encrypted form. This is done after the administrator performs the data encryption and segmentation on the data taken from the child cloud. The base cloud can only be controlled by the administrator to ensure integrity of data. Each segmented data known as chunks are stored in separate systems in the base cloud. In case data is being retrieved from base cloud, the encrypted and segmented data is sent to the administrator for the data decryption and de-segmentation before sending it to the user. Thus, the proposed system technique ensures security and integrity to the data saved in the cloud and also provides an architecture

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue IX, September 2016

which is secure and reliable through use of Linux as the Operating system.

PROPOPOSED SYSTEM FOR AUTHENTICATION

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

i) A client desire to log in will surfs to the login page.
ii) The client then starts an application on a pc , and enters a PIN code.
iii) After entering the PIN code, OTP is generated and displayed on the pc with system id.
iv) The client enters his username and the OTP at the login page, and sends the information to the authentication server.
v) The server either permits or denies the client to access the cloud.

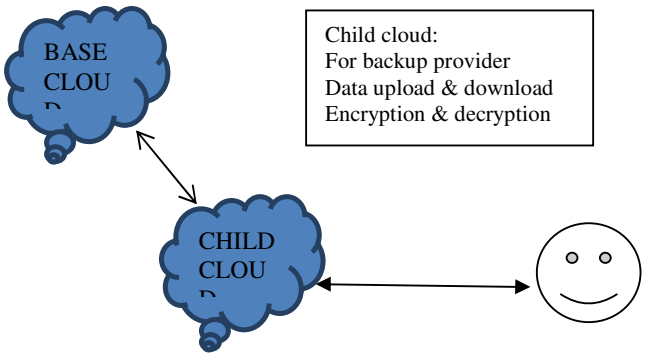

Fig 1.1 Heritage key management System

Algorithm

1. Start
2. Client enter user id and password to access child clouds services
3. User enter OTP
4. User enter option upload data or download data
5. If data upload
   i. Upload data to child cloud
   ii. Cloud take data and
      i. Perform encryption using a unique key.
      ii. Perform data segmentation
      iii. Send data to base cloud with RSA
      iv. Base cloud save each data in separate system
6. If download
   i. If downloading encrypted secure file .
      i. Cloud take data from base cloud with RSA
      ii. Perform de-segmentation on the data
      iii. Perform decryption on data
      iv. Send data to client
7. End

V.PROPOSED RESULTS & COMPARISION CHART

PROPOSED RESULTS

1. Efficient and reliable technique.
2. Maintaining multi high level data security.
3. Use of data encryption to insure data integrity for services.
4. Use of Linux to avoid virus interference and safety of the system.

COMPARISION CHART

REGULAR	PROPOSED
Data is available publically but security is not maintained.	Data is availablepublically with data security and integrity.
Encryption with OTP is not available.	Encryption of datatakes place to provide dataWITH OTP security.
Virus attacks are notmonitored.	Virus attack is filtereddue to Linux being used in the back end.
Less reliable	High level ofreliability is ensured.
No backup provided	Multi cloud backupsystem present.

VI.CONCLUSION

As we have represented in this paper security and integrity of data is maintained by a unique and robust technique in already booming technology of cloud computing system. This new heritage cloud technique provides an extensive support to maintain the integrity and endow security to user's data. This new system incorporates multi cloud technique which offers data security in cloud computing. The introduced technique can find its application in all systems where data integrity and security is vital, such as defense, private and Public sector undertakings, etc.

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 or pc as an authentication device. In this technique mobile phones or pc are responsible to making OTP which is valid only for 2 minutes. A combination of Mobile OTP and SSO can address most of identified threats in cloud computing dealing with integrity, confidentiality, authenticity and availability of the data and communications. The solution, presents a hierarchical level of service, available to all involved entities, that realizes a security mesh through federations, with in which essential trust is maintained.

REFERENCES

[1] Dr. Mark D. Bedworth PhD BSc FSS. February 2008. A Theory of probabilistic One time Password . Computer science computer engiuneering and Applied computing , Security and Managenment ..
[2] Kiddo. 2010. Hacking Website: Menemukan Celah Keamanan & melinduring website dari serangan haker .mediakita.
[3] Rivest, Ronald L. 1992.The MD5 Message Digest Algorithm.
[4] Privacy and consumer risks in cloud computing", Dan Svantesson, Roger Clarke, computer law & security review 26 (2010) 391e97, @

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue IX, September 2016

2010 Svantesson & Clarke. Published by Elsevier Ltd. doi:10.1016/j.clsr.2010.05.005.

[5] Amir M. Talib , Azmi Murad, Rusli Abdullah "CloudZone: Towards an integrity layer of coud data storage based on multi agent system architecture " IEEE cnference 2011.

[6] Arya Sapoetra Y. June 2010. Rancang Bangun Arsitektur Library Sistem Autentikasi One Time Password Menggunakan Prosedur Challenge-Response. Informatics Engineering, Pembangunan Nasional "Veteran" University, East Java.

[7] "Dynamic Authentication: Need than a Choice", A. Saxena, Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference, 10 (1) (2008), 214, IEEE conference.

[8] Amir M. Talib , Azmi Murad, Rusli Abdullah "CloudZone: Towards an integrity layer of cloud data storage based on multi agent system architecture". IEEE conference 2011.

[9] Cong Wang and Kui Ren, Wenjing Lou and Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services" ,IEEE Network July/August 2010

[10] Daniel Nurmi, Rich Wolski, Chris Grzegorczyk, Graziano Obertelli, Sunil Soman, Lamia Youseff and Dmitrii Zagorodnov, "The eucalyptus open-source cloud-computing system", 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, 2009. CCGRID '09.

[11] Sonali Yadav, "Comparative Study on Open Source Software for Cloud Computing Platform: Eucalyptus, Openstack and Opennebula", International Journal Of Engineering And Science, Vol.3, Issue 10, PP 51-54, October 2013, Issn:2319-6483.

[12] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, vol. 53, no. 6, p. 50, 2009. [Online]. Available: http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[13] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proceedings of the Third international conference on Applied Cryptography and Network Security, ser. ACNS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 442–455. [Online]. Available: http://dx.doi.org/10.1007/11496137_30.

[14] A. Yaar, A. Perrig, and D. X. Song, "Fit: fast internet traceback," in INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies, 13-17 March 2005, Miami, FL, USA. IEEE, 2005, pp. 1395–1406.

[15] T. Snia, "Cloud data management interface," Representations, pp. 1–173, 2010. [Online]. Available: http://www.snia.org/tech_activities/publicreview/CDMI_Spec_v08.pdf

[16] C. Schridde, T. Dörnemann, E. Juhnke, M. Smith, and B. Freisleben, "An identity-based security infrastructure for cloud environments," in Proc. of IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS2010), 2010.

[17] ——, "A dynamic key infrastructure for grid," in Proceedings of the 2005 European conference on Advances in Grid Computing, ser. EGC'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 255–264.

[18] A. Yaar, A. Perrig, and D. X. Song, "Fit: fast internet traceback," in INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies, 13-17 March 2005, Miami, FL, USA. IEEE, 2005, pp. 1395–1406.

