Information Security in Cloud Computing using Encryption Techniques

[1]Ninni Singh, [2]Nitin Kumar Singh

Abstract— Cloud computing play a vital role in communication as well as in enterprise environment.it extends beyond a single company.it facilitates its user by allowing to store its data on the cloud and able to access it from any computer when required. Clouds of computers are interconnected via internet and communicate by sending and receiving data, security become an important issue i.e. confidentiality, modification, authentication, impersonation, data security. In literacy work many researches proposed various approaches to solve these security threats. They use different combination of various encryptions techniques to resolve security threats in cloud computing In order enhance the security on cloud we proposed a scheme which is the combination of various cryptographic techniques i.e. AES is used for encryption and confidentiality, HMAC –SHA96 is used for authentication and generation of secret key .Our proposed approach provides the three layer security model to resolve all possible threats

Index Terms— AES, Digital Signature, HMAC, SHA-1

.

1 Introduction

Cloud computing is an emerging technology that consist of cluster of computers connected via internet and allow its authorized user to access its application without installing at client side and access its file via internet. It acts as central remote server that maintain data and server [1]. Cloud computing facilitates its user by providing resource's on demand.

Traditionally service provider in cloud computing performs two functions: *infrastructure providers*. It takes care of functionality of cloud, allocates required resources and leased according to the usage. *Service providers* it entertains its client by providing all the needed facilities and rent the services from other infrastructure providers.

Cloud computing provides services like scalability, no updating require, no server maintenance cost, demand metered at different level of abstraction IaaS (infrastructure as a service) ,PaaS(platform as a service), SaaS(software as a service)[2]

As explained earlier cloud computing uses internet utilities so it razed various type security issues like data theft, modification, eavesdropping, and impersonation. So in order to protect our data there is a need of such mechanism that provide authentication, confidentiality, data security and integrity.

In our proposed approach we incorporate various Symmetric encryption and key exchange techniques to fulfill all the requirements that lead to security. In which user first derived secret key from user password by using HMAC-SHA96 and then authenticate each other. If user want to store its data on cloud then in that case it encrypt its data by using AES algorithm and store it in cloud. If he want to access some previously stored file then it perform AES decryption algorithm.

This paper is classified in to five sections these are as follows.-

a) *In first section we have introduced the security challenges in Cloud computing.*
b) *In Second section we have elaborated the related works.*
c) *In third section we explore our proposed approach.*
d) *In fourth section we have shown the step wise execution of our proposed approach.*
e) *In Fifth section we have conclude our paper along with future work.*

2 Related Works

Volker Fusenig and Ayush Sharma [3]: proposed a scheme in which they introduce security check functionality when virtual resources transfer from cloud to its clients if needed. In this approach client demands its security requirements and service provider perform mapping operation that maps security requirements in to security functionality and if necessary then it moves the resources. The objective of their work is to represents a security architecture that allows its user to impose a security feature on cloud according to its need by specifying its security requirement.

As per Eman M.Mohamed and Hatem S. Abdelkader [4]: In cloud computing data is uploaded and stored at data centers. The management of data in data centers is not trustworthy this may leads to various types of security challenges. To overwhelm this service provider adopt various encryption technique. Their paper evaluates the performance of eight encryption techniques by measuring the encryption speed in both cloud as well as desktop environment.

G. Jai Arul Jose, C. Sajeev, and Dr. C. Suyambulingom[5] :They proposed a scheme in which they incorporate three security

- *Ninni Singh is currently pursuing masters degree program in Computer Science engineering from Jaypee University of Information and Technology, India, E-mail: ninnisingh1991@gmail.com*
- *Nitin Kumar Singh is currently pursuing bachelor degree program in Computer Sc ience fromShobhit University, India, E-mail: rockynitinsingh@gmail.com (This information is optional; change it according to your need.)*

International Journal of Scientific & Engineering Research Volume 5, Issue 4, April-2014
ISSN 2229-5518

techniques i.e. RSA is used for securely key exchange mechanism. SSl is used by the control node for securely transfer data after the certificate is generated and AES is used for encryption. The objective of their work is to provide a strong security features in order to overwhelm all possible network attacks.
As per Uma Somani, Kanika Lakhani and Manish Mundra[6]: They proposed a scheme in which they incorporate digital signature with RSA. Digital signature is used for authentication purpose and RSA is used for secure key exchange as well for encryption purpose. The strength of their work is that they provide dual security i.e. authentication and data security.
As per Prashant Rewagad and Yogita Pawar[7]: They proposed a scheme in which they integrate three cryptographic techniques to enhance the security features. They use diffiehellman key exchange and digital signature with AES encryption algorithm. Diffie-hellman key exchange is used for the generation of key pairs(secret key), Digital signature is used for authentication purpose and AES is used for encryption purpose. The strength of their works is to provide a three way protection scheme which is very hard for the intruders to breach the security.

3 Proposed Approach

In our proposed approach we consider a service interaction security environment where user or client accesses the services that are stored at cloud. Our proposed security model consists of three Layers. First layer is Authentication Layer. The authentication module provide two services, data integrity and data origin authentication. Second layer is Encryption and confidentiality layer and the third layer is data store.
Authentication module provide authentication by developing a secret key from user password and by digital signature. Encryption and confidential module encrypt the client data by using AES. Data store module store the Client's data. For implementation point of view we are using two different server's i.e. one for data store and other for encryption purpose.

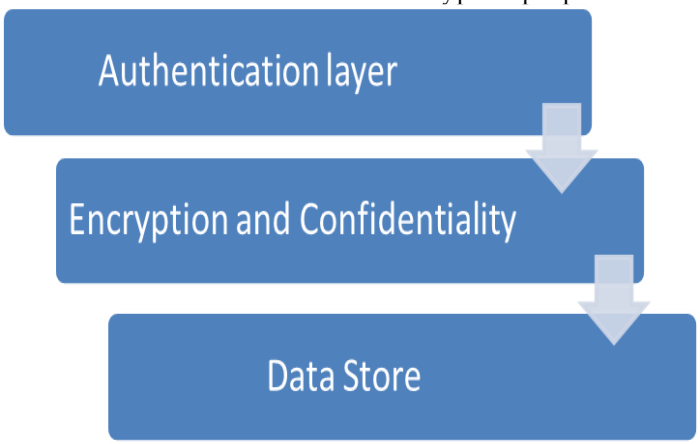

Fig.1 Proposed Security Model

When a client want to store data on cloud he has to login first i.e. the user interface provided client has to enter its user id and password. With the help of entered password cloud generate a secret key by using HMAC SHA-96 after this user is authenticated by digital signature. After authentication only cloud able to encrypt the user's data using AES symmetric encryption technique. Then only user's data uploaded on cloud data store. If user want to access the stored file on cloud then for this purpose firstly user login in to the system by entering its user id and password then from that password we generate a secret key. After this requested file is selected and authentication is performed using digital signature, then AES algorithm is used for decryption of selected file.

4 Step By Step Execution

1. Login via provided user interface.
   - Key generation from password and digital signature using HMAC SHA-96.
2. Downloading and uploading data using AES
3. Data is stored and accessed from data store.
4. Logout.

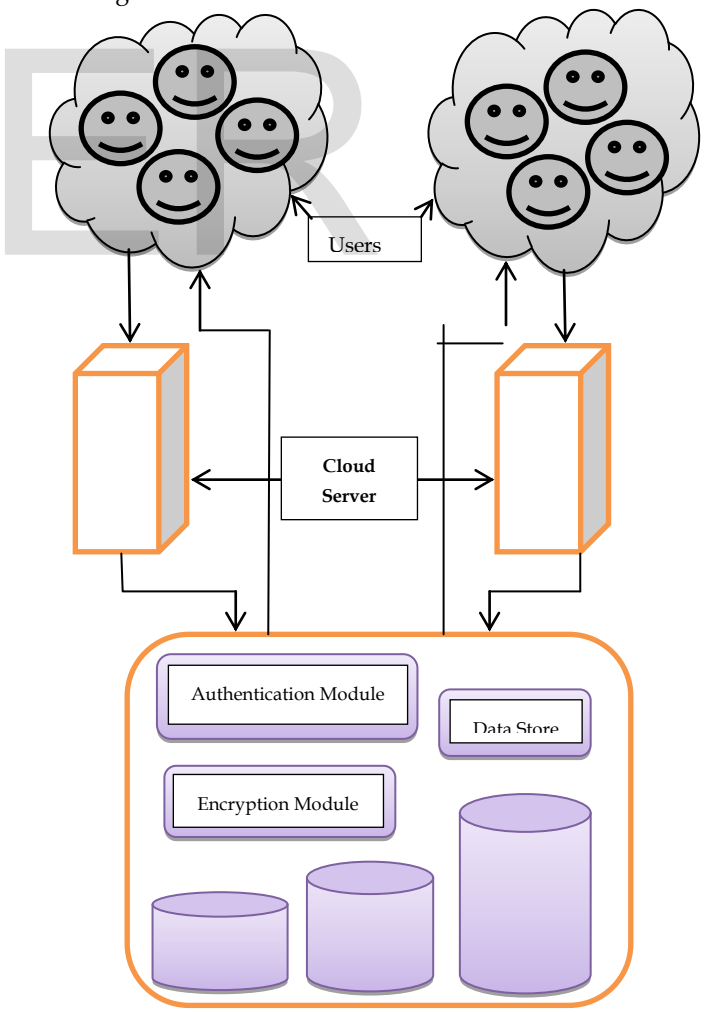

Fig.2 Cloud data server architecture

International Journal of Scientific & Engineering Research Volume 5, Issue 4, April-2014
ISSN 2229-5518

4.1 Secret Key Generation

The authentication key i.e. secret key for authentication purpose is derived from user password.

Step1: Firstly the password is repeated until it forms the exact 2^{20} octets of string. The resultant string is called digest 0.

Step2: After this the resultant digest 0 is hashed using SHA-1 and form 20 octets of string. The resultant string is called digest 1.

Step3: Now we concatenate digest 1 with service id(the service we are trying to access. Each service has a unique id).this string is again fed as an input to a hashing function. The resultant string is called digest 2 or key

Step4: Now from key we derive two functions K1 and K2 .Two different fixed string ipad and opad are defined.

$$Ipad = the\ hexadecimal\ byte\ repeated\ 64\ times.$$
$$Opad = the\ hexadecimal\ byte\ repeatred\ 64\ times.$$

Step5: An extended 64 bit authorization key derived from key (digest 2) by adding zeros.

$$K_1 = (extendedauthkey \oplus ipad)$$
$$K_2 = (extendedauthkey \oplus opad)$$

HMAC $= H\left(K_2, H\left(K_1, message\right)\right)$

Step6: To avoid sharing of same password for different services it's better to have different password in security point of view so to accomplish this we generate another key names localized key. This is different for different service.

$$Localised\ key = H(digest1, Service\ Id, digest\ 1).$$

5 Conclusion

In this paper we have shown the possible attacks in cloud communication environment. We have proposed a mechanism which guard against these attacks. In our proposed approach security is provided by deriving a secret key and client is authenticated using digital signature. Further we have shown the execution of our proposed approach. Our proposed schemes provide high security and avoid unauthorized access, maintain integrity, confidentiality.

There are still future work is to be done in order to reduce the communication overhead, fast accessing data, computation overhead and further increasing the availability of data.

References

[1] Farhan Bashir Shaikh and Sajjad Haider "*Security Threats inCloud Computing"* 2011 IEEE 6th international conference on Internet Technology and secured transactions, 11-14 December 2011,

[2] Abu Dhabi United States of Arab Emirates Balachandra Reddy Kandukuri, Ramacrishna PaturiV, Atanu Rakshi, *"Cloud Security Issues"* 2009 IEEE InternationalConference on Services Computing.

[3] Volker Fusenig and Ayush Sharma "*Security Architecture for Cloud Networking"* 2012 IEEE International Conference on Computing, Networking and Communications, CloudComputing and Networking Symposium

[4] Sherif el-etriby , Eman m.Mohamed and Hatem s. Abdelkader published *"Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing "* in the third international conference on communications and information technology ICCIT 2012.

[5] G. Jai Arul Jose, C. Sajeev, Dr. C. Suyambulingom "*Implementation of Data Security in Cloud Computing"* International Journal of P2P Network Trends and Technology- Volume1 Issue1- 2011 .

[6] Uma Somani, Kanika Lakhani and Manish Mundra "*Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing"* 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[7] Prashant Rewagad and Yogita Pawar "*Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing*" 2013 IEEE International Conference on Communication Systems and Network Technologies 6-8 April 2013

[8] Qi Zhange , Lu Cheng and Raouf Boutaba *"Cloud Computing :state –of-the –art and research challenges*" Journal of Internet Services and Applications Volume 1, Issue 1 -may 2010

[9] Mohamed Al Morsy, John Grundy and Ingo Müller "*An Analysis of The Cloud Computing Security Problem*" Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30thNov2010.

[10] Feng-qing Zhang and Dian-Yuan Han "*Applying Agents to the Data Security in Cloud Computing*" IEEE 2012 International Conference on Computer Science and Information Processing (CSIP) 26 Aug. 2012.