International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Securing Data Storage in Cloud with Generating OTP using SHA Algorithm

Dr. T. Lucia Agnes Beena[1], S. Jegan Benish[2]

[1]HEAD, Asst. Professor, Department of Information Technology, St.Joseph's College(Autonomous), Trichy, Tamil Nadu, India

[2]Research Scholar, Department of Information Technology, St.Joseph's College(Autonomous), Trichy, Tamil Nadu, India

ABSTRACT

Cloud services have grown very quickly over the past couple of years, giving consumers and companies the chance to put services, resources and infrastructures in the hands of a provider. There is a big security concern when using cloud services. Security is very important in Cloud Computing since people and companies store confidential data in the Cloud. It must also be easy to use the services provided, since cloud services have so many users with different technical background.Since Cloud Computing is rest on internet, various security issues like privacy, data integrity, confidentiality, authentication and trust are encountered. This paper describes an enhanced approach for the data security model in cloud environment. The proposed data security model includes generation of onetime password (OTP) using SHA(Secure Hash Algorithm)for user authentication process.

Keywords : Cloud Computing, Authentication, OTP, SHA

I. INTRODUCTION

Cloud computing is an internet techniques that uses central remote servers to, store data and applications.Cloud computing enables consumers and firms' employees to use applications without the needs to install special softwares. 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]. They are:

Software as a service (Saas): Provide the consumers the Applications or Services created by Cloud Service Provider(CSP) and which are running on Cloud infrastructure.

Platform as a service (Paas): Provide the consumers with the ability to deploy their applications onto the cloud infrastructure. These applications are created by the consumers using the tools and programming

languages provided by the cloud provider. Thus, consumers have control over the deployed applications and possibly environment configurations of applications but not on the underlying cloud infrastructure including server machines(physical or virtual), storage drives, networks, or operating systems. [3]

Infrastructure as a service (Iaas):

Consumers are provided with the capability to provision storage, networks, processing and other computing resources, also allow the consumer to run arbitrary software, which include operating systems and applications on it.

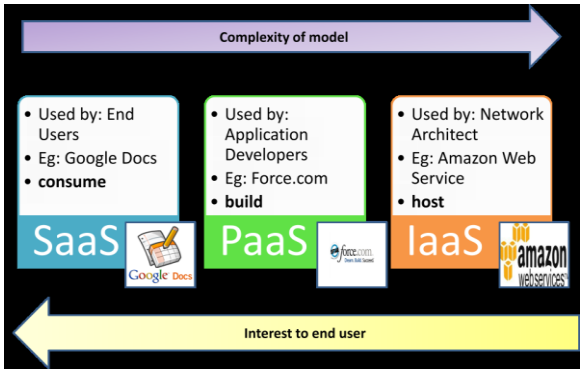

Fig 1: Cloud Computing Models

II. Security in Cloud Computing

The security of the cloud environment depends on the security provided by the cloud service provider. Cloud providers control the hardware and the hypervisors that stores the data and applications are run. Cloud Service provider security must be top-of the- line.

Various security concerns are discussed:

Data integrity and Reliability

In cloud computing, anyone from anylocation can access the data. Cloud does notdifferentiate between common and sensitivedata. Thus, the reliable availability of user's data is an important aspect of cloud service.

Data Confidentiality

Confidentiality refers to having the abilityto accessprotected data only by authorized systems orusers. Asthe number of users, devices and applicationsinvolvedincreases, the threat of data compromise on thecloudalso increases because number of accessibility increases day by day [6].

Multitenancy

Cloud computing is based on a computing modelwhereresources are shared at host, application andnetworklevel. As in multi-tenancy multiple tasks, orprocessesare shared, this presents a number of privacy and confidentiality issues. [8].

Loss of user identity/password

For an authorized access, authentication isrequired to be there in the cloud computingsecurity structure. Thus, if the identity andpassword of the user is lost or is revealed bymistake to any unauthorized person, the data can be at risk [8].

Data Tampering

There is always a concern for data beingtampered by unauthorized party. Tamperingrefers to the data which is entered by user arechanged without user's authorization. This isemployed by criminals or thieves to intentionallyobtain personal or business informationabout the user.

III. RELATED WORK

This section emphasize recent researches in cloud data storage.

Choudhury et al. [9] proposes a new authentication system for cloud. As in this technique one time password is encrypted using public key of user to obtain encrypted onetime password. It removes dependency on third party but limit is its key size.

Fred et al. [10] proposes the Rubbing Encryption Algorithm (REAL) to implement a Mobile-based and a Cloud based OTP Token as design examples which can easily resists the security attacks.

Sood et al. [8] proposed a framework to provide data security to the data. It composed of two phases. Firstly it deals with secure transmission and storage

of data in cloud. Second it deals with retrieval of data from cloud. Message authentication code and double authentication with verification of digital signatures are combined to achieve reliability, integrity and availability of data. Patel et al. [11] proposed a model to maintain the computation and communication cost whileachieving storage correctness with provision to consider dynamic nature of cloud. Its main role is to develop client application for cloud customer which proved functionalities like encryption-decryption, key management, encoding, decoding, integrity checking functions like MAC, Hash.

Manjusha et al. [12] proposed a multi authority hierarchical attribute based encryption technique which gives highest security in NIST statistical test compared to key policy and cipher text attribute based encryption techniques. it preserves major issue of cloud computing which is confidentiality and integrity of data in cloud.

IV. PROPOSED SYSTEM:

The architecture proposed by us is as shown in the Figure. In this architecture two entities are considered and both shall have the web browser in their respective laptops or pc's.

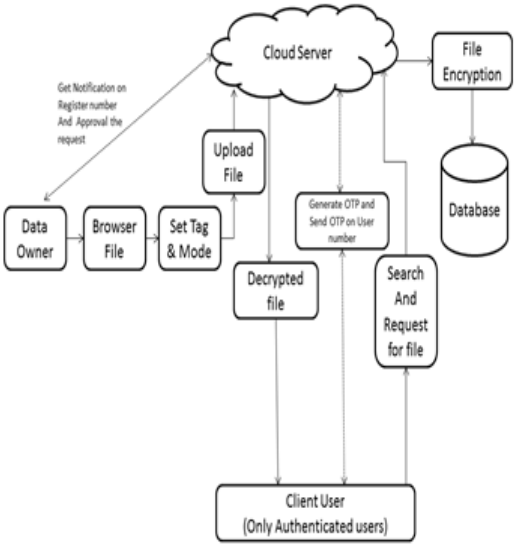

Fig: 2 Proposed System Architecture

In the initial stage the Data owner uploads the file in text or document form and then sets the tag to the file which make easy for searching the file. These uploaded Files are then encrypted by the Application on the cloud server using the RSA algorithm and these encrypted file can be accessed by the users only if permission is granted by the data owner. When the users want to access these files then, client users has to first log into the system. The user should be authenticated by the server if he is a regular user or he/she shall have to register himself with the application. Client user also needs to sign in into the system. Users can now search the required file by the file name and the tag.

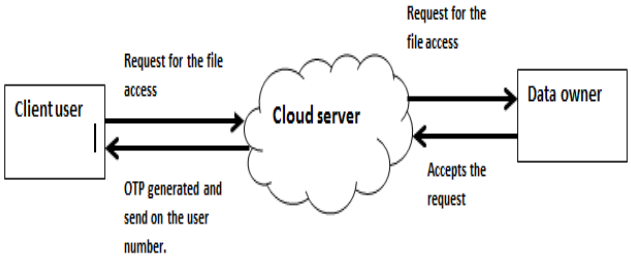

Fig: 3. Requesting file from owner

After searching the file, client user has to request for accessing file from the cloud as shown in figure 3. This request is forwarded by the cloud to the data owner. Data owner get notification on registered mobile number. The data owner can approve or deny the request. If the request is accepted then, the OTP is generated and sent to client user on registered mobile number. This one time password is generated using SHA algorithm and this OTP is valid for only specific time period. Only on entering this OTP client user get access to requested file. After accessing file, the access rights of that user for that file are taken away.

V. AUTHENTICATION

Steps involved in authentication process is listed below:

i) A client wishes to register himself by providing all the necessary details and those details are stored in the admin database.

ii) The client then enters into application by providing all the required credentials.
iii) After logging phase, the may user browse for the particular file or he/she can store some files in the database.
iv)If the user wishes to upload some content then browses for the particular file and uploads that file into the database.
v) If the userwishes to download some files there search for that particular file and an OTP is generated to the user mobile number, which is given during the registration phase.

By this way we can restrict the access to the user data and it is restricted very convenient system rather than encrypting thefile while uploading and again decrypting the file while downloading.

Cloud providers' APIs have authentication mechanisms put in place to ensure that only authorized API calls are made to their systems. Most cloud provider based APIs have an ID or Authentication Key which provides an authorization/authentication and is usually passed over HTTPS to ensure security. Cloud provider APIs also may use the ID or another Key to create a hash based token or a password to authenticate provide additional security this type of security by authentication control for theusers of the cloud; Can be applied they can enter by applying their user id and password which is monitored by the cloud environment.

For Encryption(uploading File):

RSA is one of the first practicable public key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. RSA, is based. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.

A user of RSA creates and then publishes a public key based on the two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.

The RSA algorithm involves three steps: key generation, encryption and decryption.
a) Key Generation Algorithm:

RSA public and private key pair can be generated by the following procedure. Choose two random prime numbers p and q such that the bit length of p is approximately equal to the bit length of q.
The key set is generated by using the following algorithm:
1. Select two large prime numbers p and q such that p
2. Compute modulus n = p*q
3. Compute (n) such that (n) = (p–1)* (q–1).
4. Choose a random integer e satisfying 1<e < (n) and gcd(e, (n)) =1
5. Compute the integer d, such that e*d = 1 mod (n).
(n, e) is the public key, and (n, d) is the private Key.
b) Encryption:
Encryption refers to algorithmic schemes that encode plain text into non-readable form or cipher text, providing privacy.
c) Decryption:
Decryption refers to algorithmic schemes that decode cipher text or non-readable text into readable form or pain text.

Secured File Sharing:
Algorithm used: (Secure Hash Algorithm)

The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST) and published as a federal information

processing standard (FIPS 180) in 1993; a revised version was issued as FIPS 180-1 in 1995 and is generally referred to as SHA-1. The actual standards document is entitled Secure Hash Standard. SHA is based on the hash function MD4 and its design closely models MD4. SHA-1 is also specified in RFC 3174, which essentially duplicates thematerial in FIPS 180-1, but adds a C codeimplementation.

Steps in SHA Algorithm:

Step 1: Append padding bits.

The message is padded so that its length is congruent to 896 modulo 1024 [length 896(mod 1024)]. Padding is always added, even if the message is already of the desired length. Thus, the number of padding bits is in the range of 1 to 1024. The padding consists of a single 1-bit followed by the necessary number of 0-bits.

Step 2: Append padded length:

A block of 128 bits is appended to the message. This block is treated as an unsigned 128-bit integer (most significant byte first) and contains the length of the original message (before the padding).

Step 3: Initialize hash buffer:

A 512-bit buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as eight 64-bit registers (a, b, c, d, e, f, g, h). These registers are initialized to the following 64-bit integers.

a = 6A09E667F3BCC908
b = BB67AE8584CAA73B
c = 3C6EF372FE94F82B
c = A54FF53A5F1D36F1
e = 510E527FADE682D1
f = 9B05688C2B3E6C1F
g = 1F83D9ABFB41BD6B
h = 5BE0CDI9137E2179

Step 4: Process blocks:

The heart of the algorithm is this module that consists of 80 rounds.

Step 5: Output

After all *N* 1024-bit blocks have been processed; the output from the *N*th stage is the 512-bit message digest. We can summarize the behavior of SHA-512 is Summarized as follows.

*H*0 = IV
Hi = SUM64 (*Hi*-1, abcdefgh*i*)
MD = *HN*
whereIV = initial value of the abcdefgh buffer, defined in step 3
abcdefgh*i*= the output of the last round of processing of the *i*th message block
N = the number of blocks in the message (including padding and length fields)
SUM64 = Addition modulo 2^64 performed separately on each word of the pair of inputs
MD = final message digest value[13]

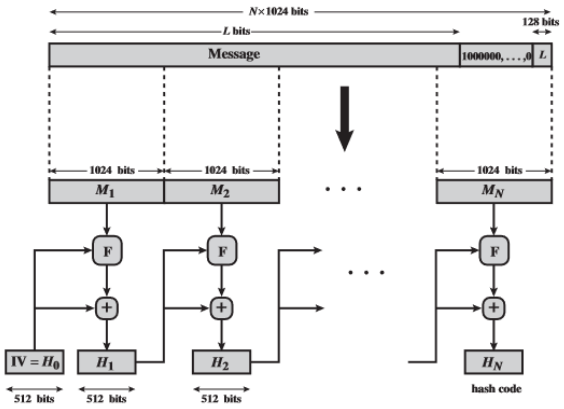

Fig 4: SHA producing message digest

Operation:

The algorithm can be described in 3 steps:

Step 1: Generate the SHA-1 value Let digest = SHA-1(Key, M) digest is a 20-byte string

Step 2: Generate a hex code of the digest. Hex digest=ToDec (digest)

Step 3: Extract the 6-digit OTP value from the string OTP = subString (digest)

The substring function in Step 3 does the dynamic truncation and reduces the OTP to 6-digit. Here we are going to generate a hash value by massing the message and key as the parameters to the hash function. Later the hash value obtained is converted to the decimal format from the hexadecimal form.

Later by using the substring function we are to choose our OTP length i.e., 4 digits or 6 digits etc.[14]

VI. APPLICATIONS AND FUTURE SCOPE

One time password is designed to prevent replay attacks, in which an attacker discovers a user's password and uses it to access a system. Here we use the OTP for secure file access. Hence the application of our system is in organisation were lot of data is confidential and it cannot be shared with any user. In such organisation data is only shared to authenticated user and so user authentication can be checked using two factor authentications. Also at applications where large amount of data is stored and need privacy to this data of data owner. Oursystem can be used on cloud where large data is stored and privacy is needed to every user. Further the system can be extended and Integrated with biometric authentication and OTP verification.

VII. CONCLUSION

This paper points the security constraints and how to overcome these issues. Here the security model is proposed which attempts to focus on providing security at cloud side. In this data OTP (One-Time Password) is used for two-factor authentication.The proposed data security model includes generation of onetime password (OTP) using SHA (Secure Hash Algorithm) for user authentication process.

VIII. 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]. D Zissis and D. Lekkas, Addressing cloud computing security issues, Future Generation computer systems, vol. 28, no. 3, pp. 583592, 2012.

[7]. C Alliance, Security guidance for critical areas of focus in cloud computing v3. 0, CloudSecurity Alliance, 2011.

[8]. S K. Sood, A combined approach to ensure data security in cloud computing, Journal of Network and Computer Applications, vol. 35, no. 6, pp. 18311838, 2012.

[9]. G. Choudhury and J. Abudin, Modified secure two way authentication system in cloud computing using encrypted one time password. International Journal of Computer Science & Information Technologies, vol. 5, no. 3, 2014.

[10]. F. Cheng, Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm, Mobile Networks and Applications, vol. 16, no. 3, pp. 304336, 2011.

[11]. H. B. Patel, D. R. Patel, B. Borisaniya, andA. Patel, Data storage security model for cloudcomputing, pp. 3745, 2012.

[12]. R. Manjusha and R. Ramachandran,Comparative study of attribute basedencryption techniques in cloud computing, inEmbedded Systems (ICES), 2014 InternationalConference on. IEEE, 2014, pp. 116120.

[13]. William Stallings, Cryptography and NetworkSecurity: Priciples and Practice,5th Edit ionPrent ice Hall; 5 edit ion (January 24, 2010

[14]. C.W. Lin, J. J. Shen, and M. S. Hwang, "Security enhancement for optimal strong password authentication protocol," ACM Operating Systems Review, vol. 37, no. 2, pp. 7-12, April 2003.