International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 5, Issue 2, March-April 2016 **ISSN 2278-6856**

Enhancement of Data Security in Cloud Computing by Generating OTP

[1]N.Neelima, [2]Sasidhar Velpula, [3]Dorababu Gudapati, [4]Hasan Baig, [5]Kambala Venu Gopal

[1]Assistant Professor, Velagapudi Ramakrishna Siddhartha Engineering College

[2,3,4,5] B.Tech Students, Velagapudi Ramakrishna Siddhartha Engineering College

Abstract

Cloud computing is technology that offers populace the ability to share information, resources and provides certain services to the people connected through the network . In this the resources are provided according to the need and requirements of the user. In cloud the user's data are moved to the large data centers, where the data must be secure in the hands of providers.The problem we generally encounter in cloud computing is to provide security to cloud user's data when it is uploaded on cloud. The various organizations have expressed concerns about these security aspects that exist regarding the implementation of cloud computing. One of the major perspective is to provide securityto one's data which is stored remotely from the user's location.. This paper describes an enhanced approach for the already using data security model in cloud environment. The proposed data security model includesgeneration of onetime password (OTP) using SHA(Secure Hash Algorithm)for user authentication process. This paper also includes a comparative of MD5 and SHA algorithms for the better implementation of the model. This model best suits for any of the layers in it, e.g. PaaS, SaaS and IaaS

Index Terms—Authentication, Cloud Computing,OTP, SHA

1. Introduction

Cloud computing is the emerging trend in the recent times and also having rapid development over the past few years. There are certain problems present with the cloud services, as the resources are put in the hands of another provider, the user has no idea over regarding that environment. We are generally unaware, how our data is stored in the cloud, how securityis provided for data.[1].

Security in cloud computing is the major part and one of the most important aspect for any organization where they move their resources to the cloud. They need to have confidence that their data is safe, both at the provider's site and during transmissions between the cloud user and owner. Furthermore, to protect the data we need the best authentication procedure that uses encryption algorithms , that offers better security. [2].

Many cloud providers are still using the same old login forms which do not offer any security and there is need to tighten up their security to ensure that data present in the cloud database is trustworthy and riskfree.The authentication procedure in cloud computing must be comfortable to the user, but at the same time it should be very secure to protect the data that it stored in the cloud. An encryption method should be used during transmissions that offers security and that algorithm should not consume much computer power and processing time[3].

1.1 Problem Statement:

Authentication in cloud computing is achieved by using the static passwords that do not offer any security to the user's present in the cloud.Static password can be easily cracked by the hackers as they are non complex passwords preferred by the users for their convenience. So static passwords must be replaced by the dynamic password schemes that provides two way authentication in the cloud environment, and that should be cost effective both for the user and the provider as users cannot afford the device for the authentication. So cloud provides initiated the one time password schemes as a factor of two way authentication that sends a code to users mobile for every login session of the user. [9].

1.2Security issues

Security issues in cloud computing covers a wide range from the authentication part of the user to the availability of the data to that user as shown in the figure 1.1There are certain risks associated with the cloud computing that are evolving from the fact that the cloud environment makes use of large number of resources present in the network. Primary issue that can be found is the authentication that makes use of a user ID and password associated with that ID. Secondary is providing various services to the authorized users who are previously gets authenticated by the cloud owner.Next comes is the confidentiality associated with the data when it is being transmitted over the network. To achieve this we use certain encryption algorithms that converts our original text to the form that is not understand by the third party. Some protocols are used to ensure confidentiality for the data when it is being transmitted from one place to the anotherplace through internet. Finally data availability can be considered as a major concern which is viewed as threat associated with the cloud environment.To overcome this problem we generally replicate our data and store in various locations. [6]

Fig 1.1 Security issues in Cloud Computing

In this paper is an enhanced authentication solution, is presented that can be used for the various cloud services. It uses user mobile as two way authentication device that gets a random security key for every login session of the user and is valid only for a certain period of time. The security key is generated to the user only after he proves his authentication by entering the valid user id and password[8].

2. State of art

All business organizations use the concept of static passwords for authentication, which have certain drawbacks due to the carelessness of the employee or the particular user who stores them in a place which is visible to everyone. Some user's often save passwords in their systems which they are working on which becomes for the malicious user to get authorized with the resources which he cannot use them . Hence One time Passwords provides a secure environment as they are dynamically changing passwords and there is no chance for remembering them or reusing them.User gets new password generated for each login session and sent to his personally registered mobile phone. Hence the concept of one time passwords provide a secure, reliable and user friendly authentication and there are various hash algorithms for the generation of OTP where the hash code is sent as a OTP to the user. Some of the algorithms that are used for the purpose of OTP generation are MD4, MD5, SHA1, SHA256, SHA512, HMAC etc[9].,

These are various methods used previously for providing additional security in a cloud environment[8].

2.1 Based on data Encryption:

Ateniese used a encryption method that encrypts the user data with their own private keys and these are again encrypted using public key present with the cloud owner. As these produces a continues encryption procedure ,this technique is called as the proxy re-encryption that transfers the user plain text into cipher text.

Zhoa et al proposed encryption method in which the user data is encrypted number of times using several keys and for the purpose of decryption we use one separate key that present within the cloud owner. It faces the problem for the user to be active in the internet all the times.

Miklau et al proposed a method that provides a wide range of security to the xml pages that are presented over the network. To accomplish this he used various keys for encrypting the various parts of the xml tree and also controls the access for the metadata nodes in the tress. [9].

Bennani et al proposed a method that uses the replication of the cloud database with a number equals to that of the users presented within the cloud. Whenever any particular user revoked his right from the database one replica of that particular user is removed from that cloud database This leads to the problem of maintaining same traces that consumes large amount of the space in the database and there is also the chance of occurring the data redundancy problem in the database.

2.2 Based on Image Recognition:

In image based recognition the user selects some set of images while he is registering his details in the cloud database. While logging he should identify those images that were selected by him during the registering phase. In this each image contains a code that acts as a secret key for the user to provide secure access for his each login session[9].

2.3 Based on HASH Algorithms:

Akula and Devisetty's proposed a technique uses hash algorithm that generates a hash code to present the authentication part of the user in a more secure manner. Most organizations presently working on these algorithms for the purpose of generating OTP, and gettingdeployed on various platforms like Internet, cell phones and PDAs.

Types of HASH Algorithms:

MD4,MD5
SHA
HMAC, etc

These algorithms take a random input and produce a hash code by using some functions. This paper deals with SHA algorithm and makes a comparative study of SHA with MD5 algorithms that best suits for the generation of OTP.

3. Proposed Method

There are ways to have a secure and easy-to-use cloud service that can satisfy these criteria's:

i. Provide better password solution for login procedures than the insecure method of staticpasswords.
ii. Provide better two-factor OTP authentication solution than those discussed above[12].
iii. Use an encryption algorithm that is secure but also fast, to be able to serve the vast amount of cloud users[10].
iv. Offer a solution that is free of charge in order to attract more customers to the cloud services.

The solution presented here will be free of charge for both the users and the provider, and at the same time easy and flexible for the clients to download, install and use as shown in the figure:

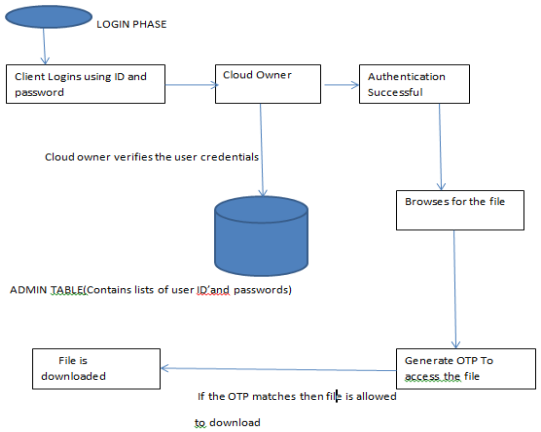


Fig 3.1 Proposed System

Steps which will going to involve during authentication 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 browse for the particular file or he can store some files in the database.

iv)If he wishes to upload some content then browses for the particular file and uploads that file into the database.

v) If he wishes to download some files he search for that particular file and an OTP is generated to the user mobile number, which is given by him during the registration phase.

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

Algorithm used: (Secure Hash Algorithm)

The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST) and published as afederal information processing standard (FIPS 180) in 1993; a revised version was issued as FIPS 180-1 in 1995 and is generally referredto as SHA-1. The actual standards document is entitled Secure Hash Standard. SHA is based on the hash function MD4 and its designclosely models MD4. SHA-1 is also specified in RFC 3174, which essentially duplicates the material in FIPS 180-1, but adds a C code implementation[13].

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 bitsis 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).[8]

Step 3: Initialize hash buffer:

A 512-bit buffer is used to hold intermediate and final results of the hash function. The buffercan 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 a module that consists of 80 rounds.

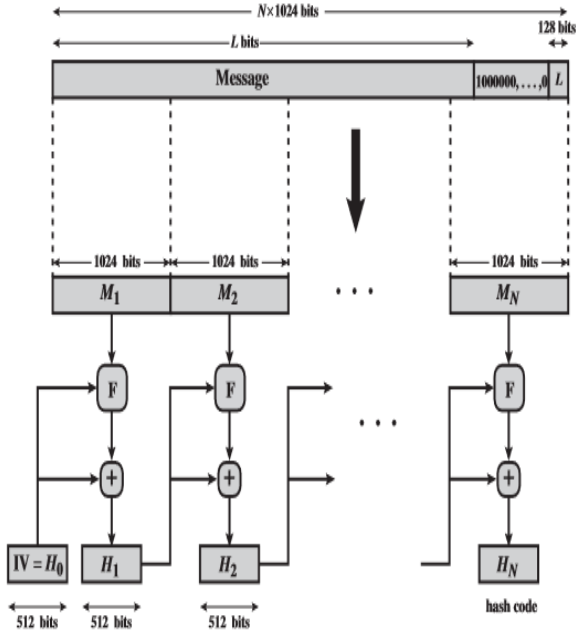


Fig 3.2 SHA producing Message Digest

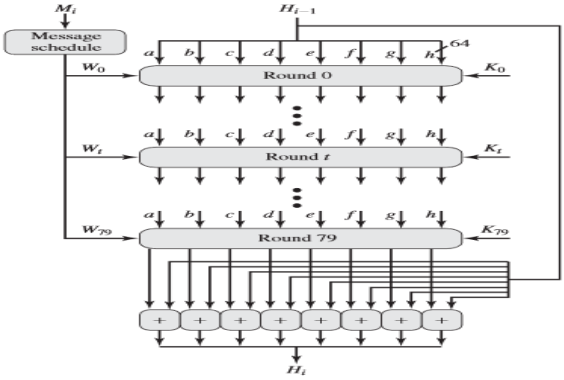


Fig 3.3 Processing of Single Block

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 behaviour of SHA-512 as follows.

*H*0 = IV
Hi = SUM64 (*Hi*-1, abcdefgh*i*)
MD = *HN*
where

IV = 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]

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.[10]

Sending of OTP to user:

The OTP generated should be sent to the user from our application via a gateway to the user mobile. For this we **cURL,** a command line tool and library that transfers data across the URL.

Stages of cURL:

1.curl_init():
It is used to initialize a session
2.**curl_setopt():**
Set an option for the URL transfer.
3.**curl_exec():**
Perform a cURL session.
4.**curl_close():**
Close a cURL session and frees all the resources.

4. Results

Generally data present in the internet is protected by using some cryptographic methods in which a code is generated that acts like signature for identifying one's data.Hash code is one the methos to produce a signature by using certain hash algorithms that provides better authentication and also acts like an message authentication code called as MAC. Each algorithm has its owm merits and demerits and performance of the system can be improves by choosing the respective algorithm based on our requirement[10].

Comparison of SHA and MD5 Algorithms:

MD5 Algorithm belongs to family of hash algorithms and similar to that of SHA the only difference is SHA processes the message in 80 rounds whereas MD5 does it in 64 rounds.So, SHA offers better security than MD5 but execution of SHA is more than MD5[11]

The differences presented below are built by using some sample random data given to each of the algorithms for predicting their performance independently. For this we need to implement them by using any one of the programming languages.

Table 4.1 Differences between MD5 and SHA

Keys for comparison	**MD5**	**SHA**
Security	Less Secure than SHA	High Secure thanMD5
MessageDigest Length	128 bits	160 bits

Attacksrequired to find out originalMessage	2^128bit operations required to break	2^160 bit operations required to break
Attacks to try and find two messages producing the same MD	2^64 bit operations to break	2^80 bit operations to break

Table 4.2 Similarities between MD5 and SHA:

Keys For Similarities	**MD5**	**SHA**
Padding	Yes	Yes
Message bit	Yes	Yes
Members (Hash Family)	Yes	Yes
Resource Utilization (same)	Yes	Yes

Execution of SHA and MD5 Algorithms

MD5 executes at a faster rate when compared to the SHA as number of rounds of processing in MD5 is less when compared to that SHA.Figure shown below helps in finding the hash lengths generated by various hash algorithms.

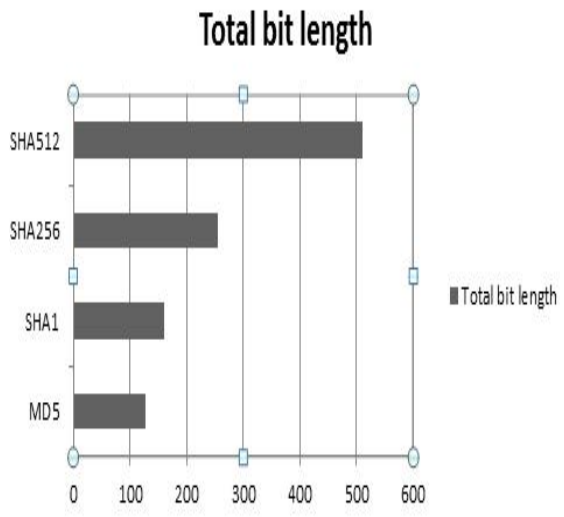
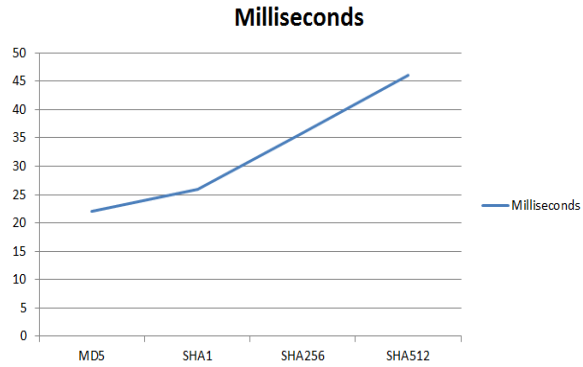


Fig 4.1 Total bit length

The figure shown below shows performance chart of various hash algorithms corresponding to the time taken by them to produce the hash value.



5. Conclusion

Certainly cloud computing will be a boon in enhancing information systems as its benefits out number its shortcomings. Cloud computing offers deployment architecture, with the ability to address vulnerabilities recognized in traditional IS but its dynamic characteristics are able to prevent the effectiveness of traditional counter measures.

Here, we have identified generic design principles of a cloud environment which stem from the necessity to control relevant vulnerabilities and threats. So, for this scenario we haveproposed to make use of Dynamic one time password with two factor authentication as a strongauthentication 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 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.

References

[1]. Dr. Mark D. Bedworth PhD BSc FSS. February 2008. A Theory of ProbabilisticOne-Time Password. Computer Science Computer Engineering and Applied Computing,Security and Management.
[2]. Kiddo. 2010. Hacking Website: Menemukan Celah Keamanan & MelindungiWebsite dariSerangan Hacker. Mediakita
[3]. Rivest, Ronald L. 1992.The MD5 Message Digest Algorithm.

[4]. Myung-Jun Kim, "Korea's Cloud Computing Strategy," IT21 Global Conference, 2009
[5]. Hyun-Seong Kim, Choon-Sik Park, "Cloud computing and the personal authenticationservice." Journal of the Information Security, vol. 20
[6]. "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.
[7]. N. Haller, Bellcore, and C. Metz. 1996. A One-Time Password System. KamanSciencesCorporation.
[8]. FadiAloul, Syed Zahidi, Wassim El-Hajj. 2009. Two Factor Authentication UsingMobilePhones. Digital Library Telkom Institute of Technology (IEEE).
[9]. AryaSapoetra Y. June 2010. RancangBangunArsitektur Library SistemAutentikasOne Time Password MenggunakanProsedur Challenge-Response.Informatics Engineering, Pembangunan Nasional "Veteran" University, East Java.
[10]. C.W. Lin, J. J. Shen, and M. S. Hwang, "Security enhancement for optimal strongpassword authentication protocol," ACM Operating Systems Review, vol. 37, no. 2, pp. 7-12, April 2003.
[11]. "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, IEEEconference.
[12]. "Eliminating Vulnerable Attacks Using One-Time Password and PassText –Analytical Study of Blended Schema" M. VijuPrakash, P. Alwin Infant and S.JeyaShobana, IJCA Proceedings on International Conference on VLSI, Communications andInstrumentation (ICVCI) (2):35–41, 2011. Published by Foundation of Computer Science.
[13]. William Stallings, Cryptography and NetworkSecurity: Priciples and Practice,5th Edit ionPrent ice Hall; 5 edit ion (January 24, 2010