ISSN 2278-3083
Volume 3, No.1, January - February 2014
International Journal of Science and Applied Information Technology
Available Online at http://warse.org/pdfs/2014/ijsait02312014.pdf

Data Security Framework for Offsite Storage of Data

Neha Upadhyay[1], Ajay Kumar[2]
[1]Master of Technology, Dehradun Institute of Technology, Dehradun, India, upadhyayneha1230@gmail.com
[2]Assistant Professor, Dehradun Institute of Technology, Dehradun, India,kumarajay7th@gmail.com

ABSTRACT

Cloud Computing is a transformation in IT Industry because of its low cost, high accessibility, high performance and also other characteristics. In this technology user can access services reside in the remote servers maintained by the third party. The data reside in cloud is of great value and its loss or damage could be a total disaster for its owner. So it is very much required to have secure method to preserve important data in order to prevent data loss. In this paper we proposed a framework deal with different techniques to provide secure data storage in cloud. The strategy projected different segments in which mutual authentication, password hashing and encryption of data is shown. It is possible to satisfy integrity, consistency and availability using this framework

Key words: Authentication, encryption technique, data privacy, data security.

1. INTRODUCTION

Cloud computing is an emerging technology in the IT sector which uses remote services through a network. It provides users all necessary service on their demand over the internet to access cloud resources. The user is just using a system which is capable of using a network that connect it to a server lies at some other location. Users do not need to store data on their own system as all data is stored at remote server. Storing data in the cloud seems to be quite attractive form of data management. One of the main advantage of storing data in cloud is unlimited access to the data i.e. user can retrieve their stored data from the server as and when required with no limitation. Cloud computing having three service models through which services are delivered to the end users. These models are Saas (Software as Service), Iaas (Infrastructure as Service) and Paas (Platform as Service). Cloud Service Providers (CSP) also provide easily accessibility, user friendly and money saving ways of storing and automatically backing up subjective data.

There are many prominent CSP like Microsoft, IBM, and Amazon etc. who provide cloud resources to the users. Functioning of public, private and hybrid cloud is not much different, the remarkable fact is users has to trust a third-party and their valuable data are being kept with them through cloud. So the security of the storage data is a primary concern in cloud computing. Storage data must be secure in such a way So that it is safe from malicious intruder and prohibited users. Some security threats in cloud are shown in figure 1.

Figure. 1 Security issues in cloud computing.

This is a general view of security issues within the scope of the threats presented by the Cloud Security Alliance. Malicious insider attempt SQL Injection attack in which malicious insider insert malicious code into a string and passed it to the cloud database for execution. Deletion and modification in the record without having there backup is an example of data loss or data leakage. Malicious entity affects the integrity and authenticity of the user's communication with CSP then it is said to be account or service hijacking.

These are some security threats which should be covered in order to provide better and secure environment for cloud storage. We introduce an authentication and authorization scheme comprising of different techniques and specialized procedures that can efficiently protect the data from the user to the cloud and then back to the user from the cloud.

2. RELATED WORK

Cloud Computing is a form of client server architecture where many user use the same infrastructure at a large scale. In order to proposed a secure scheme for cloud computing we have reviewed some existing approach and schemes based on client server architecture.

Mandeep et al. [1] proposed a work plan to eliminate the concern regarding data privacy using encryption algorithm to enhance the security in cloud.

Sandeep et al. [3] gave a framework which uses different cryptographic techniques to protect the data from the beginning till end i.e. from the owner of the cloud then to the user.

Zuzan et al.[5] gave model for data security. This model is divided into seven modules and each module describe specific situation when working with data.

Shay et al.[6] proposed a standard way to use SHA-256, also proving a method to reduce the size of SHA-512 constants table.

Ramazami et al.[8] analyses the issue including data storage security and depicts challenges and security measures to be overcome to have a good cloud computing infrastructure.

Some of the recent papers [9] has proposed authentication schemes which is based on sending one time token to the registered mobile number. But the SMS system doesn't guarantee to deliver the token at real time.

3. PROPOSED SCHEME

Proposed framework has been designed to provide complete security to the data, be it in the cloud or in transit. Framework defined a minimal set of security desires and appropriate procedures to reach them that the cloud storage services have to be considered secure for usage. The detailed approach and its components are described as follow.

In our proposed schemes some notations are used. List of those notation and there meaning is listed in Table 1.

TABLE I .Notation used in our scheme

S.No	Notation	Meaning
1	PSWD	Password
2	||	Concatenation
3	H	Hash Function
4	O_PSWD	Old Password
5	N_PSWD	New Password
6	A_LINK	Activation Link
7	R_Link	Password Rest Link
8	C_Server	Confirmation Message

A. Registration and login phase

Before user are able to access the cloud resources and synchronize or backup there data, they need to register in cloud. Cloud Services commonly require users account before any services can be used. For this purpose user should have a valid email-id. Email id used during registration is verified by sending an activation link from Activation Server (AS) to registered email id to complete the process, using this process both CSP and user authenticate each other . This avoids the attacker to behave like a server. This process is called as Two Way Authentication.

1. User enters his EMAIL_ID through his system. AS checks whether Email ID is already registered or not. If not then process moves to Step 2 else ask user to enter new Email ID.
2. User enters valid EMAIL_ID to the server. AS generates random single time token attach with A_LINK and send it to registered EMAIL_ID.

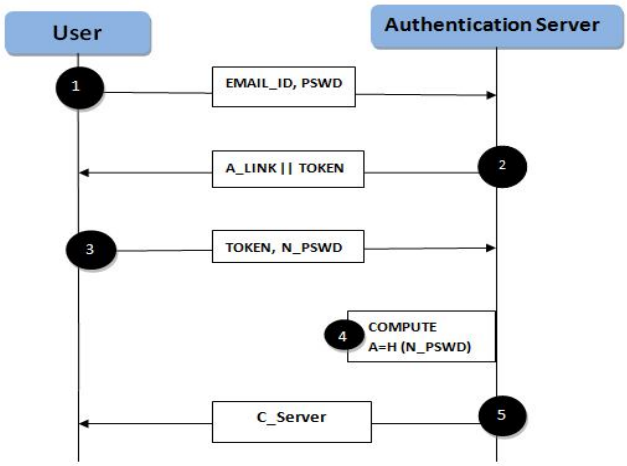

Figure 2. Registration Process

3. User click on A_LINK by checking his registered EMAIL_ID and enter that token and N_PSWD to confirm his registration.
4. AS calculate H of N_PSWD and store in database.
5. AS sends C_SERVER message to user's EMAIL_ID and redirect it to home page.

In order to prevent dictionary attack, brute force attack our scheme implement some methods to make them infeasible such as time penalties or temporary account lock after a minimum incorrect login attempts within a given time frame.

B. Password Hashing

Most important trait of a user's account is how user password is protected. Password is something that fits in the memory of user and user choose it. Sometimes mandatory rules are given to user to enter password like password should have at least two digits, minimum 12 characters, one uppercase, one lower case but those rules become unbearable limitation on their interest and user has to fight with them. So we use Cryptographic Hash Function in which user can enter password of his choice and that password is stored in hash form in database. We have used SHA-256 cryptographic hash function in which hash function with digest length of 256 bits is generated. It is a keyless hash function.

SHA256 works in the manner that the entered string is first padded with the input length in such a way that the digest generated is a multiple of 512 bits long, and then it is

passed into 512 bits message block $M^{(1)}, M^{(2)}, .. M^{(N)}$ message block handled one at a time.

Workflow for password hashing and authentication in a hash based account is as follow.

1. User creates an account with valid Email Id.
2. Then, password is hashes and stored in cloud database.
3. When user try to login, the hash of the password entered by user is check against the hash of their real password stored in database.
4. If the hash matched, then user is granted access, if not the user is told he entered invalid login or password.

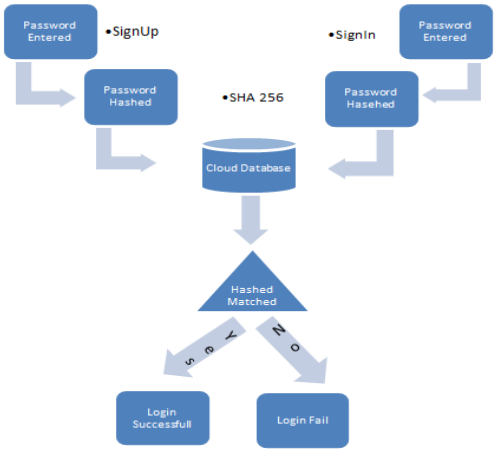

Figure 3. Password Hashing and authentication based on hash.

C. *Password Change*

This phase is used when users want to change his password from old to new. Password reset option is designed in such a way that it can prevent denial-of-service attack.

Workflow for password change is as follow.

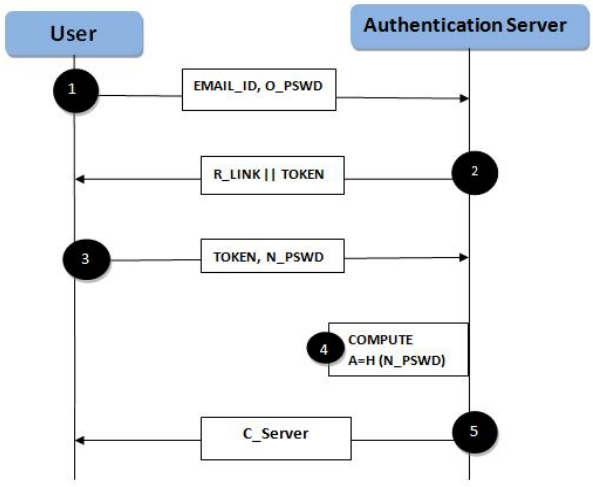

Figure 4. Password Change Process.

1. User enter his EMAIL_ID and O_PSWD in his system and send request message for password change to AS.
2. AS checks with the stored Password in the database, if both are matched then AS sends a random single time token including R_LINK to the registered EMAIL_ID.
3. When user click on the link, a new prompt window open a request user to enter N_PSWD as well as received token. Token is expiring within 15 minutes after when it is used.
4. H of N_PSWD is calculated by AS and stored in database.
5. AS send C_SERVER message to users EMAIL_ID.

D. *Encryption*

Motive of user's to use cloud resources are to have a backup of valuable data which resides at other location yet easily accessible. Data itself needs to protect in such a way that even successful attack, content of the stored data remain confidential. So all data needs to be stored in encrypted form in the remote server. Encryption is the transformation of data into an undisclosed code called as encrypted file. And to read this file, receiver must have access to a secret key or password that enables to decrypt file.

We use Triple DES i.e. Triple Data Encryption Algorithm for encryption and decryption of files (TDEA). This is a symmetric key block cipher, which applies Data Encryption Standard (DES) cipher algorithm three times to each data block. It provides a somewhat simple method of increasing the key size of DES without a need of to design a completely new block cipher algorithm. It has been common practice to protect and transport a key for DES encryption with triple-DES. It means that the plain text is encrypted three times. A number of modes of TDES have been proposed.

1. DES-EEE3: Three DES encrypt with three different keys.
2. DES-EDE3:3 DES operates in the sequence of encryption-decryption-encryption with three different keys.
3. DES-EEE2 and DES-EDE2: Same as the above format except that the first and third operation uses the same key.

Using TDES files is encrypted and then stored in database so a sin case of attack intruder can't read the original file. Decryption needs secret key to obtain the actual form of files. In cloud environment users want to share their files with others users. File sharing can be done in 3 ways.

1. Sharing file with other users of the same CSP.
2. Sharing file with a closed group of non-subscribers.
3. Sharing files with everybody.

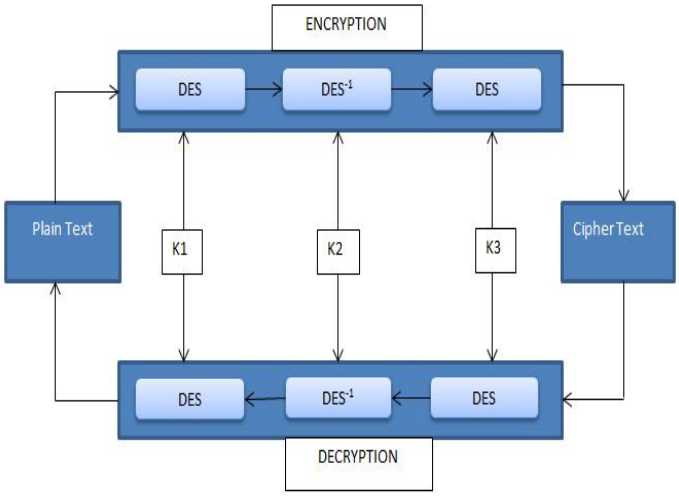

Figure 5. Triple DES.

For file sharing users have authority to share their key with those users whom he wants to be. And also user has that right of sharing file in encrypted form or in plain text. For example, if user wants to share a notice with everyone then user can share it in plain text only according to his interest, or if he want then he can share in encrypted format to. Once user uploads their files on cloud, in backend CSP categorize their files like text files are listed in one column, media files are listed in other and so on. And during downloading user just type which kind of file he wants to download whether it is media file, zip file, text file etc. and files are shown to the user in listed format. User can manage their circle by adding and removing other users from his circle, this feature provide more security to the user and freedom to share data with only those whom he wants to be.

In our proposes framework main security features are maintained by CSP and some feature like selecting user to add and remove is given to users which make our framework a user friendly effect. Required validation are implement to protect database from SQL Injection (SQLIA).Our proposed protocol resist many popular attacks like dictionary attack, brute force attack, malicious insider, data loss as different schemes are used to prevent these attacks.

4. CONCLUSION AND FUTURE SCOPE

In this paper, we proposed an authentication scheme which authenticate user to cloud server and cloud server to user. In addition, we provide a secure storage for user's valuable data as cryptographic mechanism is used to protect the data like SHA 256 is used to secure password and encryption is used to hide the original form of data. Currently study on cloud computing is moving on and time to time new schemes are derive with high security and flexibility. Future work also includes caring the privacy of the users information provide to the serve. So applying new security mechanism to authenticate users with each other in cloud using authentication protocol like Kerberos will be the next future goal for cloud computing.

REFERENCES

[1] Using encryption Algorithms to enhance the Data Security in Cloud Computing, Mandeep kaur and Manish Mahajan.". International Journal of Communication and Computer Technologies (2278-9723)
Volume 01 – No.12, Issue: 03 January 2013.

[2] An analysis of security issues for cloud computing,
Keiko Hashizume, David G Rosado, Eduardo Fernandez Medina. Journal of Internet Services and Applications2013, 4:5.

[3] A combined approach to ensure data security in cloud computing, Sandeep K. Sood. Journal of Network and Computer Applications 35 (2012) 1831–1838

[4] Privacy-Preserving Public Auditing for
Secure Cloud Storage, Cong Wang, Student Member, IEEE, Sherman S.M. Chow, Qian Wang, Student Member, IEEE.

[5] Model of solution for data security in cloud computing, Zuzana Priščáková and Ivana Rábová. International Journal of Computer Science, Engineering and Information Technology (IJCSEIT).

[6] SHA-512/256, Shay Gueron, Simon Johnson, Jesse Walker. Department of Mathematics, University of Haifa, Israel, Mobility Group, Intel Corporation, Israel Development Center, Haifa, Israel, Intel Architecture Group, Intel Corporation, Security Research Lab, Intel Labs, Intel Corporation, USA.

[7] Securing the Private Cloud: Exploring the value of tokenization.

[8] Survey on Data Security Issues and Data Security Models in Cloud Computing, Ramasami S., Umamaheswari P. International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 3, March 2012.

[9] A Strong User Authentication Framework for Cloud Computing, Choudhury A. J., Kumar P., Sain M.,Hyotaek L. and Hoon , Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, 2011.

[10] Data Security Policy In The Cloud Computing, RAN Shuanglin. The 7th International Conference on
Computer Science & Education (ICCSE 2012).