International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

SECURING DATA IN CLOUD USING GRAPHICAL PASSWORD AUTHENTICATION AND AES CRYPTOGRAPHY

Arockia Panimalar.S[1], Ramya.A[2], Subhashri.K[3]

[1,3]*Assistant Professors, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*
[2]*V M.Sc SS, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*

Abstract - *Security in data communication is a major important concern today. Cloud computing is a revolutionary mechanism that changes the way of enterprising the hardware and software design and procurements. Because of cloud simplicity everyone is moving data and application software to cloud data centre. The Cloud Service Provider (CSP) ensures integrity, accessibility and secrecy but it does not provide consistent data services to customer and to store customer data. Securely sending and receiving data in the above area is an important, as the data is crucial. In today's world the password security is very important. If the confidentiality of the information is of very high value, then it should be protected. If user wants to stop the unauthorized disclosure or alteration of the information, then it should be highly secured. Unauthorized persons access should be controlled and security for the files in the cloud should be provided. The main focus of this paper is to grant the graphical password technique for login security and AES cryptography for file security, thereby providing the user with highly secured file security system.*

Key Words: *Advanced Encryption Standard, Cryptography, Graphical Password Authentication, Cued Click Points.*

1. INTRODUCTION

Cryptography is a technique which is used to protect the important data. Encryption is the science of changing data so that it is unrecognizable and useless to an unauthorized person. Decryption is changing it back to its original form. For password protection various techniques are available. Cued Click Points is a click-based graphical password scheme and a cued-recall graphical password technique. AES cryptography and graphical password technique are well known and normally used techniques that operate information in order to cipher or hide their reality. Cryptography scrambles a message so it cannot be understood. A new system is developed which uses both AES cryptography and graphical password technique for better confidentiality and security. AES algorithm is a very secure technique for cryptography. Cued Click Points (CCP) is a proposed click-based graphical password scheme for graphical password authentication. Even if we combine these techniques straight forwardly, there is a chance that the intruder may detect the original message. Hence the idea is to apply both of them together with more security levels and to get a very extremely protected system for data hiding. The focus is to develop a new system with extra security features, where a meaningful piece of text message can be hidden by combining security techniques like AES cryptography and graphical password authentication.

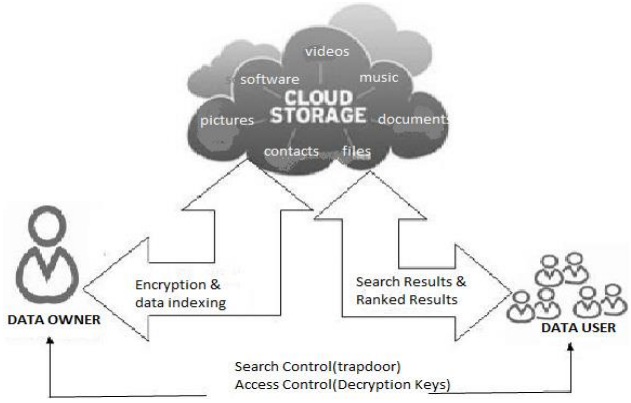

Figure1: Cloud Storage Process

2. AUTHENTICATION

Authentication is the process of determining whether a user should be allowed to access to a particular system or resource. User can't remember strong password easily and the passwords that can be remembered are easy to guess. This system allows user choice while influencing users towards stronger passwords. The task of selecting weak passwords is more tedious and it avoids user from making such options. In effect, this authentication schemes makes choosing a more protected password, the path-of-least-resistance rather than raising the trouble on users. It is easier to follow the system's suggestion for a safer password feature but it is absent in most login techniques.

3. GRAPHICAL PASSWORD AUTHENTICATION

Various graphical password methods have been proposed as an alternative to text-based passwords. According to various researches, passwords based on text are less protective and easier to hack. Various studies states that the human brain can easily recognize images and recalls it better than text. Graphical passwords are much more reliable and it mainly reduces the memory burden of the users. It is coupled with a larger full password space offered by images. More secure passwords can be produced and users will not resort to unsafe practices in order to cope.

Graphical password provides superior protection than text-based secret word as majority of people in an attempt to remember text-based passwords and plain terms.

A dictionary search can hit on a password and allow a hacker to gain entry into a system in seconds. But if a sequence of selected images is used on succeeding screen pages, and if there are many images on each page, a hacker must try every possible combination at random.

4. CUED CLICK POINTS

Cued Click-Point (CCP) is a graphical password scheme. In CCP, user clicks one point on every image rather than on four points on one image. It offers cued-recall and introduces image cues that immediately alert suitable users, if they have made a fault while entering their latest click-point. It makes the hotspot based attacks a more challengeable one.

The Cued Click-Point method is much usable and provides huge security via hotspot technique. By taking advantage of user's ability to identify images and the memory trigger connected with seeing a new image. Cued Click Point is more secure than the Pass Point Graphical Password. CCP increases the effort for attacker by forcing them to first obtain image set for each user, and then considering for hotspot on each of these images. Cued Click-Point technique has more advantages than other password techniques in terms of usability, security and memorable authentication mechanism.

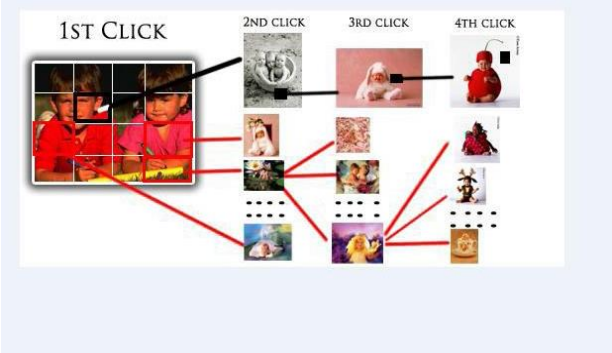

Figure 2: Cued Click Points Selection

5. SYSTEM DESIGN/GPA PHASES

The system design consists of three phase: user registration phase, picture selection phase and system login phase.

A. User Registration Phase

In user registration phase, user enters the user name in user name tab. When user enters user details in registration phase, the data are stored in the database and used during the login phase for verification. In picture selection phase, the pictures are selected by the user from the database of the password system.

B. Picture Selection Phase

In picture selection phase, user selects any image as passwords and it consists of a sequence of four click-points on a given image. Users can select any pixels in the image as click-points for their password. Users have to select a click-point in the image and then continue with the next image.

C. System Login Phase

In the system login process, the images will be displayed without shading or viewport. The sequence of clicks should be in the correct order within a system defined permutable square of the original click points.

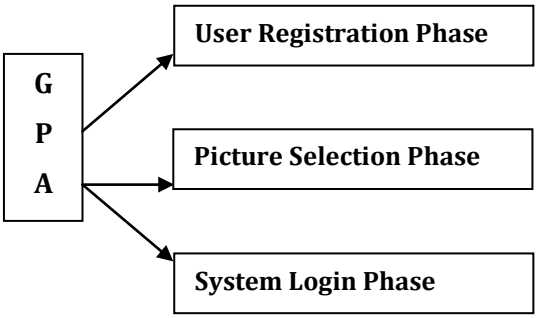

Figure 3: Phases of GPA

6. CLOUD DATA STORAGE CHALLENGES & ISSUES

The cloud computing does not provide control over the stored data in cloud data centers. The cloud service providers have full control over the data, they can perform any malicious tasks such as copying, destroying, modifying, etc. The cloud computing ensures certain level of control over the virtual machines. Due to this lack of control over the data, it leads to greater security issues than the generic cloud computing model. Encryption doesn't give full control over the stored data instead it gives security better than plain data.

7. IDENTITY MANAGEMENT & ACCESS CONTROL

The integrity and confidentiality of data and services are related with access control and identity management. It is important to maintain and track record of user identity for avoiding unauthorized access to the stored data. The identity and access controls are complex in cloud computing because of the data owner and stored data at different executive platforms. In cloud environment, different organization uses a variety of authentication and authorization agenda. By using different approaches for authentication and authorization, there may be a compound situation over a period of time. The cloud resources are dynamic and elastic for cloud user. IP addresses continuously changes, when service starts or restarts in pay-per- usage model. This allows the cloud users to join and leave feature to cloud resources, when they are required i.e., on-demand access policy. All these features need efficient and effective access control and identity management. The cloud has to maintain quick updating and managing identity management for joining and leaving users over cloud resources. There are many issues in access control and identity management, for

example weak credentials may reset easily, denial of service attack to lock the account for a period of time, weak logging and monitoring abilities and XML wrapping attacks on web pages.

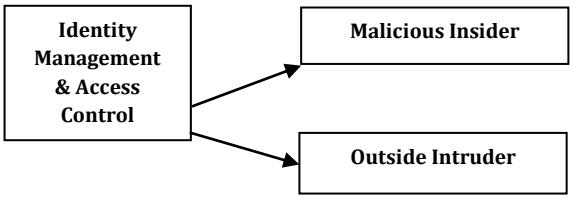

Figure 4: Types of Intruders

A. Malicious Insider

An insider threat can be posed by employees, contractors and /or third party business partners of an organization. In cloud environment i.e., at Cloud Service Provider (CSP) side attacks leads to loss of user's information integrity, confidentiality, and security. This leads to information loss or breaches at both environments. This attack is precious and it is well known to most of the organization. There is a variety of attack patterns performed by insiders because of sophistication about internal structure of an organization's data storage structure. Most organization ignores this attack because it is very hard to defend and impossible to find the complete solution for this attack. Attack ensures great risk in terms of data breaches and loss confidentiality at both organization and cloud level.

B. Outside Intruder

Attacks that come from external origins are called outsider attacks. Data security is one of the important issue in cloud computing. Since service providers does not have permission for access to the physical security system of data centre. But they must depend on the infrastructure provider to get full data security. In a virtual private cloud environment, the service provider can only specify the security setting remotely, and the user does not know exactly whether they are fully implemented. In this process, the infrastructure provider must reach the following objectives: confidentiality for secure data transfer and access and audit ability. So that outside intruders can't access sensitive data which is stored in cloud.

8. ADVANCED ENCRYPTION STANDARD (AES)/ RIJNDAEL ALGORITHM

In the year 1997, the National Institute of Standards and Technology (NIST) announced a contest to develop a new encryption system and asked for some important restrictions. The developed system had to be publicly disclosed, unclassified, free for use worldwide, usable with 128, 192, and 256 bit key sizes, and symmetric block cipher algorithms for blocks of 182 bits. On 26 May 2002, 3DES was replaced by Advanced Encryption Standard (AES). AES and 3DES are commonly used block ciphers and the selection depends upon the requirements. AES outperforms 3DES both in software and in hardware.

Advance Encryption Standard (AES) is also known as Rijndael algorithm. It was created by Joan Daemen and Vincent Rijmen and it has a strong algorithm with a strong key. The Rijndael block cipher can use different block and key lengths, such as 128, 192, and 256 bits. This versatility can produce faster and more secure symmetric block ciphers. Another algorithm which might be considered as an alternative to the Rijndael block cipher is the Twofish algorithm, which can use blocks of 128 bits with keys up to 256 bits. The Rijndael's algorithm is the combination of protection, performance, capability, implement ability and flexibility and it is made as an appropriate selection for AES.

A. Need for Rijndael Algorithm

When it comes to security, the winner is AES as it is considered strong in practical use. After discussing the flaws of DES and 3DES as well, it seems that DES is insecure and no longer of any use, but that is not the case. The 1997 attack required a great deal of cooperation and the 1998 machine is too expensive to implement, and so the DES and 3DES algorithms are still beyond the capability of most attacks in the present day. However, the influence of computers is increasing and powerful algorithms are required to face hacker attacks. The response to that requirement is AES. AES has been intended in software and hardware and it works fastly and powerfully even on small devices such as mobile phones. In general larger block size and longer keys using a 128 bits block and with 128, 192 and 256 bits keys. AES provides additional security in the long period.

B. AES Algorithm for Cryptography

AES also known as Rijndael algorithm is a symmetric block cipher that can process the data blocks of 128 bits with lengths of 128, 192, and 256 bits using cipher keys. The input, output and cipher key for Rijndael are bit sequences containing 128, 192 or 256 bits with the constraint that the input and output sequences should have the same length. Normally the length of the input and output sequences can be any of the three allowed values but for the Advanced Encryption Standard, the only length allowed is 128 bits.

C. ADVANTAGES

The algorithm provides some advantages for the users and is as follows:

- Very Secure.
- Reasonable Cost
- Flexibility
- Simplicity

9. WORKING OF AES

A. CRYPTO WORK

For Crypto work the following steps are considered for encrypting the data:

- Insert text for encryption.
- Apply AES algorithm using 128 bit key (Key 1).
- Generate Cipher Text in hexadecimal form.

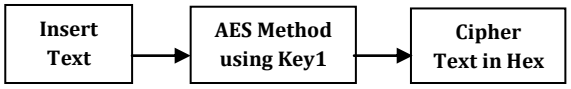

Figure 5: Text to Cipher Text Conversion

B. REVERSE CRYPTO WORK

For Crypto work the following steps are considered for retrieving the original text.

- Get the above retrieved cipher text.
- Reverse AES algorithm by using Key 1.
- Get the original message.

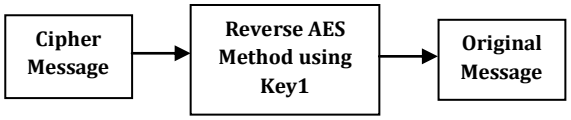

Figure 6: Cipher Text to Text Conversion

C. ROUND FUNCTION IN AES

The round function is used by AES algorithm for cipher and inverse cipher. The round function is composed of four different byte-oriented transformations:

- Byte substitution via substitution table (S-box)
- Shifting rows of the state array through different offset
- Mixing the data within each column of the State array
- Adding a Round Key to that State.

D. ENCRYTION

In the mode of encryption, the initial key is added to the input value at the very beginning which is called as initial round. This is followed by 9 iterations of a normal round and ends with a slightly modified final round as seen in Figure 7. During the first normal round, the operations like Sub Bytes, Shift Rows, Mix Columns, and Add Round key are performed in the same order. The last round is a normal round without the Mix Columns stage.

Steps in AES Encryption

i. Sub Bytes: A non-linear substitution step where each byte is replaced with another according to a lookup table.

ii. Shift Rows: A transposition step where each row of the state is shifted cyclically a certain number of steps.

iii. Mix Columns: A mixing operation which operates on the columns of the state, combining the four bytes in each column.

iv. Add Round Key: Each byte of the state is combined with the round key. Each round key is derived from the cipher key using a key schedule.

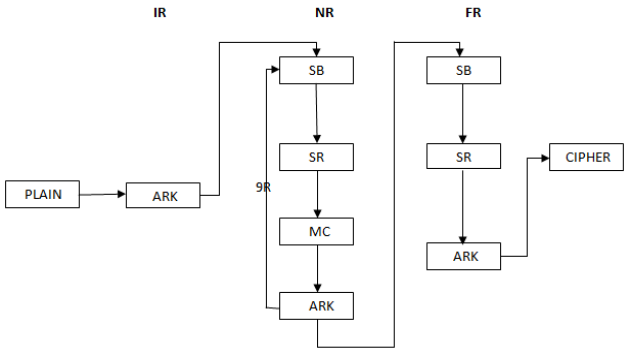

Figure 7: Encryption Process Flow

E. DECRYPTION

In the mode of decryption, the operations are in reverse order compared to the order in encryption mode. Here the mode of decryption starts with an initial round, followed by 9 iterations of an inverse normal round and ends with an Add-Round-Key. Operations like Add-Round-Key, Inv-Mix-Columns, Inv-Shift-Rows, and Inv-Sub-Bytes are performed in same order during inverse normal round. The initial round is an inverse normal round without the Inv-Mix-Columns.

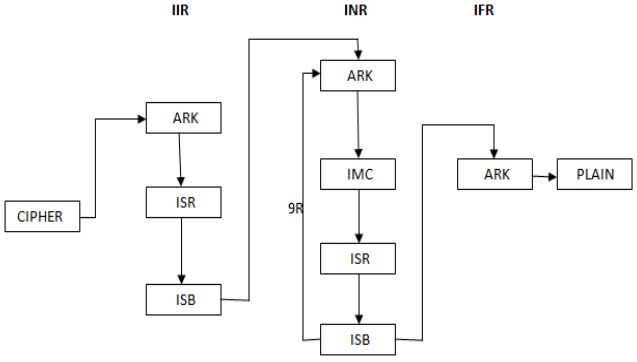

Figure 8: Decryption Process Flow

10. AES APPLICATIONS

AES encryption and decryption has many applications. It is used in cases where data is too sensitive that, only the authorized people are supposed to know and not to the rest.

The following are the various applications:

A. Secure Communication

- Smart Cards
- RFID
- ATM Networks
- Image Encryption

B. Secure Storage

- Confidential Cooperate Documents
- Government Documents
- FBI Files
- Personal Storage Devices
- Person Information Protection

11. CONCLUSION

The field of cloud storage security, especially cryptography can create a new safer environment in the present world and can change the threats related to the file security. A new system is proposed by combining Graphical Password Authentication (GPA) and AES cryptography.

The main advantage of this AES and GPA system is that the method used for encryption. AES cryptography is very highly secure and the Cued Click Points (CCP) technique is very hard to detect. Cued Click Points (CCP) especially combined with AES cryptography is a powerful tool which enables people to communicate with confidence about the security level of their data provided with.

This method is very usable and provides great security using hotspot technique. By taking advantage of user's ability to identify images and the memory trigger connected with seeing a new image. Cued Click Point is more secure than the previous graphical authentication methods. AES (Rijndael) algorithm provides safer and secured encryption and decryption of files to the users. AES works quickly and efficiently even on small devices such as smart phones. AES algorithm increases the workload for attackers by forcing to decrypt a file two times to hack the file's data. It provides security to user at the authentication level and also provides AES techniques for secured file maintenance in the cloud environment.

12. REFERENCES

[1].www.slideshare.net/RashmiBurugpalli/basic encryption-and-decryption

[2].www.manomayasoft.com/blog/item/163-encryption-and-decryption-algorithm

[3].www.storagecraft.com/blog/5-common-encryption-algorithms/

[4].http://searchsecurity.techtarget.com/definition/Rijndael

[5].www.seminarsonly.com/Labels/Graphical-Password-Authentication-Project.php

[6]. www.slideshare.net/harikrishnan89/ppt-for-graphical-password-authentication-using-cued-click-points

[7].www.cs.mcgill.ca/kaleigh/computers/crypto_rijndael

[8].www.codeproject.com/Tips/7074/How-to-Use-Rijndael–Managed Encryption-with-Csharp

[9].www.codeproject.com/Questions/382719/Cued-Click-Points-Design-Implementation