Implementation Of Two Factor Access Control Mechanism Using Cloud

Apoorva Shankar [1], Ashwini. S [2], Chandana. S [3], Harshitha. P [4]

[1] Student, Computer science and engineering, National Institute of engineering, Karnataka, India
[2] Student, Computer science and engineering, National Institute of engineering, Karnataka, India
[3] Student, Computer science and engineering, National Institute of engineering, Karnataka, India
[4] Student, Computer science and engineering, National Institute of engineering, Karnataka, India

ABSTRACT

In the present scenario cloud computing had become one of the emerging trends. Cloud computing often referred to as describes the act of storing, managing and processing data online. Security and privacy is one of the indispensable concerns in cloud as sensitive data are stored in the cloud for sharing purpose or convenient access. This paper deals with the fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. In our proposed 2FA access control system, it is mandatory for the user to possess both user secret key, which will be generated by the admin when he authenticates the user's file request and an OTP which will be generated on successful login. This mechanism can intensify the security of the system, as a user cannot access the system if he does not hold both, especially in those scenarios where many users share the same computer for web-based cloud services.

Keyword: - *Sensitive data, two factor authentications, Secret key, and* Rijndael.

1. INTRODUCTION

Cloud computing, is the delivery of on-demand computing resources ranging from applications to data centers over the internet. The benefits of web-based cloud computing services are huge, which includes ease of accessibility, reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility and immediate time to market. As sensitive data are stored in the cloud for sharing purpose or convenient access, security and privacy are the major concern for web based cloud services. The stored data may be modified or misused by unauthorized access. So, only eligible users can access the cloud for various cloud services, where user authentication has become a critical component for cloud system. Even though username and password may serve as authentication for cloud, password can be easily hacked by installing some spyware to learn the login password from the web-browser or can possibly be guessed or stolen by undetected malwares. Passwords provide a first line of defense in most cases, but there is much more.

[4] Enforcing a strong password policy is a basic step that is often overlooked. In random audits of corporate networks, about 30% of user passwords are ridiculously easy to guess and appear in any hacker's dictionary. Strict password policies can also be a problematic scenario - make them too strong and your users will begin writing their passwords on sticky notes and keeping them in their desk drawers, under mouse pads, or taped to the bottom of the keyboard. If someone can guess a user's password, they can impersonate the user. Thus, in this project a secondary authentication system is proposed which initiates at cloud login.

Securing data in cloud is the most important concern in today's life. Many a times, it happens that the user's device password can be known by people, present in the user's vicinity. They can use this password to login secretly, and steal some vital data. Hence, securing the system, when the user is not in its proximity is an important task. To do so, some feature needs to be added to the system. A solution to this is to have additional one time password in order with the normal Username and password on login to ensure the authenticated user. In an attribute-based access control system, each user has a user secret key issued by the admin.

This project gives the insight of a new fine-grained two-factor authentication (2FA) system for web-based cloud computing services. Specifically, in the proposed 2FA system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a unique one time password. As a user is unable to access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user.

2. Literature survey

Joseph K. Liu, Member, IEEE, Man Ho Au, Member, IEEE, Xinyi Huang, Ron gxing Lu, Senior Member, IEEE, and Jin Li proposed a Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services by IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 3, MARCH 2016: This paper presents a system based on the idea that applies symmetric key encryption algorithm to keep your data secure against unauthorized reading and undetected mutilation. The main issue of tapping data is secrecy and confidentiality. Confidentiality has always played an important role in diplomatic and military matters. In order to keep this symmetric key secret this system encrypts this confidential symmetric key with the public cryptographic function. This system also uses the 2FA as the main technique to secure the sensitive data stored in cloud.

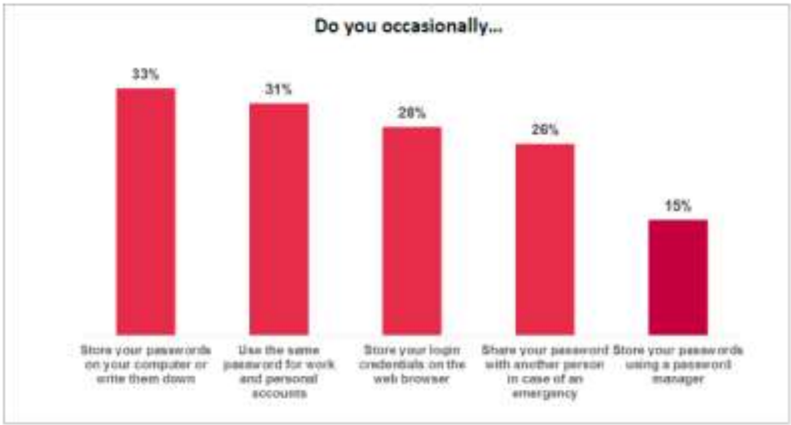

Chart -1: Survey on individual.

3. Existing System

[2] A 2002 survey from NTA, points out that 49% of users write their passwords on a piece of paper and 81% just choose very simple ones. Another recent survey indicates that 64% of users share their passwords with others and about two thirds of the people interviewed have actually revealed their passwords to the interviewer! The NTA survey has classified users into three groups: light users (36,8%, with less than 5 passwords), medium users (33,4% from 5 to 10 passwords) and heavy users (29,8%, with more than 10 passwords). To make things worse, 67% of all users rarely or never change their password and heavy users manage 21 passwords on average and some even 70. Passwords are costly to manage. Indeed, yet another survey from Meta Group showed that, on average, companies with an annual revenue greater than 400 million Euros can have more than 75 deployed applications, databases and systems requiring user authentication. A medium to large enterprise spends between 100 and 300 Euros per person every year to manage passwords. Finally, recent and significant data from the SANS Institute confirms that weak passwords represent the fifth major vulnerability in IT systems.

[1] In the existing system, the two-factor authentication process consists of two levels of verification i.e., OTP for the login page and secret key to access the file from the cloud. It consists of four modules namely, user, trustee, admin and cloud. User is the one who makes authentication with the cloud server each user has a secret key issued by the authority and a security device initialized by the trustee. The user will enter the OTP and request for a

file and then enters the secret key to download the file. Admin Authority uploads the file requested by the user and gives file access permission and is also responsible for generating user secret key for each file requested by the user. Trustee will login to authenticate the user either by accepting or denying the user's request and then generate the OTP and sends it to the user through mail. Hashing and exponentiation algorithms are used in this process.

4. ALGORITHM

Rijndael (pronounced rain-dahl) is the algorithm that has been selected by the U.S. National Institute of Standards and Technology (NIST) as the candidate for the Advanced Encryption Standard (AES). Rijndael will begin to supplant the Data Encryption Standard (DES) and later Triple DES. The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys.

Rijndael was designed based on the following three criteria [5]:

1. Resistance against all known attacks;
2. Speed and code compactness on a wide range of platforms;
3. Design simplicity

Rijndael uses a variable number of rounds, depending on key/block sizes, as follows:

9 rounds if the key/block size is 128 bits
11 rounds if the key/block size is 192 bits
13 rounds if the key/block size is 256 bits

The Add Round Key step generates a new round key for the following round of transformations. The derivation of the Sub key and the Key Schedules as follows [6],

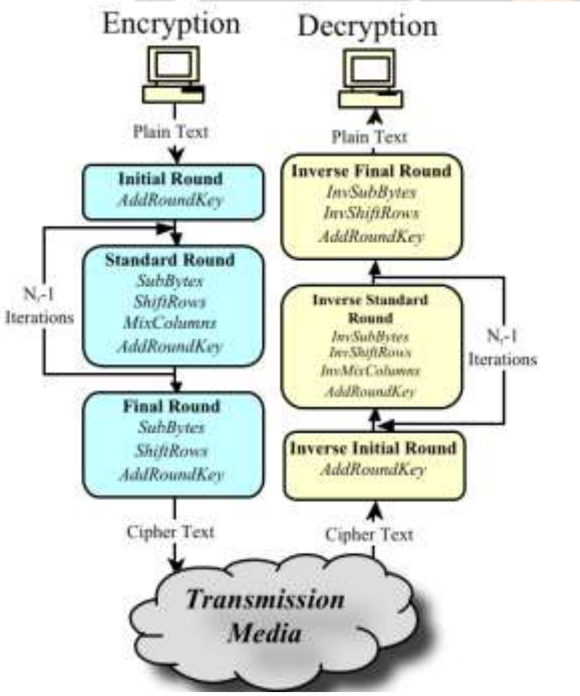

Fig 1: Rijndeal encryption/decryption.

Rijndael was evaluated based on its security, its cost and its algorithm and implementation characteristics. The primary focus of the analysis was on the cipher's security, but the choice of Rijndael was based on its simple algorithm and implementation characteristics. There were several candidate algorithms but Rijndael was selected because based on the analyses, it had the best combination of security, performance, efficiency, ease of implementation and flexibility.

5. PROPOSED SYSTEM

The proposed system is based on 3-tier architecture which includes three layers namely, presentation layer(PL), business logic layer(BLL) and data access layer(DAL). The Presentation Layer contains pages like .aspx or Windows Forms where data is presented to the user or input is taken from the user. BLL contains business logic, validations or calculations related to the data. Though a web site could talk to the data access layer directly, it usually goes through another layer called the Business Layer. The Business Layer is vital in that it validates the input conditions before calling a method from the data access layer. The data transfer object is used to transfer data between presentation layer and data access layer. DAL contains methods that helps the Business Layer to connect the data and perform required actions, whether to return data or to manipulate data (insert, update, delete and so on). In 3-tier architecture, the queries to be executed are stored in the stored procedure.

Proposed system is more efficient as it contains 3 modules which is more advantageous over the existing system which contains 4 modules. During login process, user provides a secret sentence which is the added security in this proposed system. [3] Rijndael algorithm is a symmetric key encryption/decryption algorithm that generates OTP and a sec ret key. The secret key is of 128bits in length which decrypts the encrypted file automatically without human intervention. Secure Socket Layer(SSL) provides encrypted communication between web browser and the web user which is mainly used to secure the user details such as password, emailId and generates SSL certificate. Simple Mail Transfer Protocol(SMTP) is a TCP/IP protocol used in sending and receiving email. Admin can activate/deactivate the uploaded file based on the usage that serves in space optimization.

5.1 ADVANTAGES

1. The one-time password (OTP) is generated each time when the user log in to the clouds.
2. For each different file, a different secret key is generated which adds additional security.
3. Generation of secret key is done using Rijndael algorithm.
4. Rijndael algorithm generates a 128bit secret key, which is very difficult to be hacked easily.
5. Activation/deactivation of file is allowed which provides space optimization and avoid irrelevant access of files in the cloud.

6. IMPLEMENTATION

a. Admin

Step 1: Admin login using Login credential.
Step 2: Enter OTP.
Step 3: Upload the files.
Step 4: Activate/deactivate the uploaded file.
Step 5: Grant access to the user request.
Step 6: Admin logouts.

b. **User**

Step 1: User registers to the cloud.
Step 2: Login to the cloud using the user ID and password that is sent to his email ID.
Step 3: Enters OTP sent to his email and enters the secret sentence.
Step 4: Send a request to access to the file to the admin.
Step 5: User Logouts.

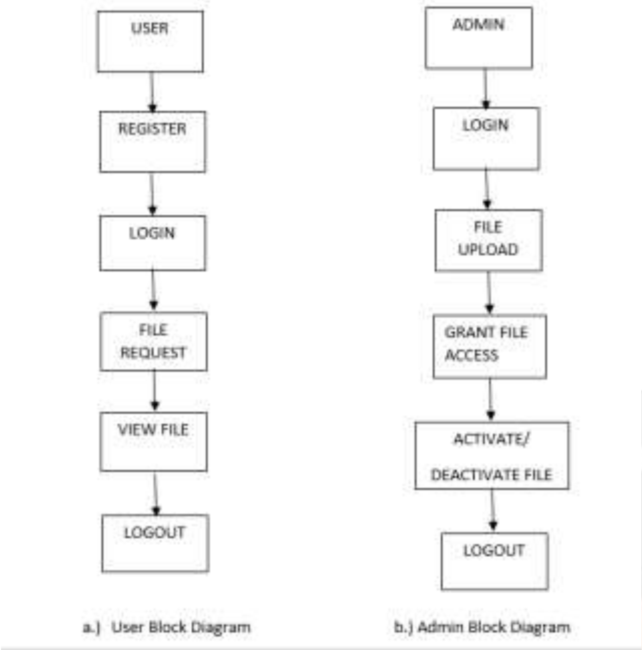

Fig 2: Block diagram

7. CONCLUSIONS

In this paper, we demonstrate a new form of fine-grained 2FA control security mechanism for web-based cloud services. This new form of security mechanism not only restricts unauthorized user access and preserves privacy but also controls redundancy as it makes use of separate secret keys for individual files rather than individual users.

The proposed system is constructed using 3 tier architecture which is a client-server architecture that allows one of the three tiers to be replaced or reused efficiently.

Therefore, the proposed system meets the desired security features for any web-based application and its construction is also feasible.

8. REFERENCES

[1] J. K. Liu, M. H. Au, X. Huang, R. G. Lu and J. Li, Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services, IEEE transactions on Information Forensics and Security, Vol 11, No 3, March 2016, ieeexplore.ieee.org/document/7305762/

[2] https://www.scribd.com/document/291399307/bluetooth-powered-secutiry.

[3] J. Daernen and V. Rijrnen (1965). *Rijndael*. Heidelberg, New York: Springer.

[4] http://www.arpnjournals.com/jeas/research_papers/rp_2015/jeas_0315_1713.pdf.

[5] Daemen, Joan; Rijmen, Vincent. AES Proposal: Rijndael.

[6] http://home.ecn.ab.ca/~jsavard/crypto/co040801.htm