TWO FACTOR AUTHENTICATION FOR WEB BASED CLOUD COMPUTING SERVICES

[1]Ch. Rajesh, [2]P. Harshita, [3]K. Narmada, [4]Ch. Eshwar, [5]V.Vani

[1,2,3,4] Students, [5]Assistant Professor,
Department of Computer Science and Engineering
St. Martin's Engineering College, Hyderabad, Telangana, India

***ABSTRACT*: Now days, the security and privacy of users data and files in cloud has become a big concern both for users and also for the cloud service providers. There should be proper security should be provided to data which is send to cloud. we introduce a new two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of a password, secret key and a Trustee response. As a user cannot access the system if they do not hold all these, 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 server 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. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.**

Index Terms: Two factor, authentication, cloud services.

I. INTRODUCTION

Data Security is an important concern for the business organizations and also for the users of the cloud computing services in this increasingly networked world these days. Illegitimate disclosure may have serious consequences for an organization in both long term and short term. To prevent from all these unwanted and nasty activities from happening, an organized effort is needed to control the security of the users files in cloud. Here is our attempt to demystify the jargon surrounding the security which will help you to protect the files security in the clouds. A virtual host computer system that enables enterprises to buy, lease, sell, or distribute software and other digital resources over the internet as an on-demand service is cloud computing. Though the new paradigm of cloud computing provides great advantages, there are meanwhile also concerns about security and privacy for web based cloud services. A multi-factor authentication and access control system for web-based cloud computing services is developed. In the proposed authenticated access control system, an attribute-based access control mechanism is implemented with the necessity of both user secret key and a trusted security key response. The login of the user is secured by one time key password system (OTP) and each login is secured with session keys i.e. The user is allowed to work only for a permitted time period. A user cannot access the system if she /he does not hold all the three factors: the OTP, secret key, secret key response, the mechanism enhances the security of the system, especially in those cases where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, the user. The cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user the cloud holds the user with attributes and the polices. The cloud servers cant access the files of the user i.e. the files stored are in an encrypted format the encryption key is given by only the user.

II. LITERATURE SURVEY

Patrick P. Tsang, Man Ho Au, Joseph K. Liu Ring mark that gives unavoidable endorser secrecy and unconstrained gathering arrangement. As of late ID-based ring mark plans have been proposed and every one of them depend on bilinear pairings propose the frst ID-based limit "linkable" ring mark conspire. We underline that the namelessness of the genuine endorsers is kept up even against the private key generator (PKG) of the ID-based framework. At long last we demonstrate to add personality escrow to the two plans. Due to the dierent levels of endorser obscurity.

Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen Cloud interfaces to abusing the cloud administrations for assaults on other systems.The fundamental issue that the distributed computing worldview verifiably contains is that of secure outsourcing of touchy and also business-basic information and procedures. At the point when considering utilizing a cloud administration the client must know about the way that all information given to the cloud supplier leave the claim control and security circle. Much more if sending information preparing applications to the cloud (by means of IaaS or PaaS).

Ming Li Member, IEEE, Shucheng Yu A high level of patient security is ensured at the same time by misusing multi-power ABE conspire additionally empowers dynamic adjustment of get to strategies or document qualities bolsters productive on-demand client/property renouncement and break-glass access under crisis situations. Broad logical and test comes about.

A. Existing System:

Though the new paradigm of cloud computing provides great advantages, there are meanwhile also concerns about security and privacy especially for web-based cloud services. As sensitive data may be stored in the cloud for sharing purpose or convenient access; and eligible users may also access the cloud system for various applications and services, user authentication has become a critical component for any cloud system. A user is required to login before using the cloud services or accessing the sensitive data stored in the cloud. There are two problems for the traditional account/password based system.

B. Disadvantages:

1. Account/password-based authentication is not privacy-preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems.

2. Second, it is common to share a computer among different people. It may be easy for hackers to install some spyware to learn the login password from the web-browser.

C. Proposed system:

Let us consider the two factor authentication system consists of software and the end users. The software is the key for determining access for users. The user will first enter Email id and password and then an OTP will be sent to the registered mail. That OTP should be entered. And then after signing into the system, website, the user can view the file names that are already present in the system. If the user wants to download a file for later use then the user has to request the Authority, who is the main admin for the system to issue a secret key. Then the Authority will check the request and will send the secret key. After receiving the secret key, the user has to send a request for the Trustee , who is responsible for issuing permissions for users to download files to issue a permission for downloading the file. Then the Trustee will see the request and will respond to the request by giving the permission to download the file. Then the user has to go to the file download page and click on the required file to download and then there the user has to enter the secret key that is being sent by the Authority to the user's registered Email in order to download the file.

D. Advantages:

1. 1. The knowing of password has nothing to do.

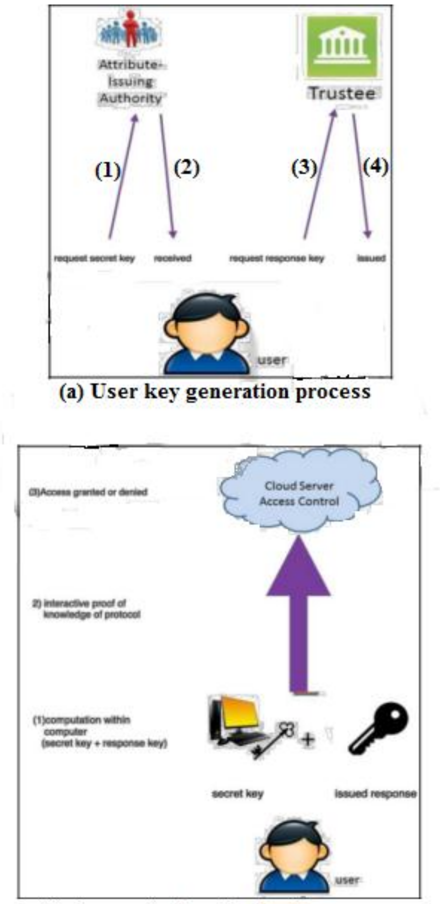
2. The files in the cloud are secured by using two factor authentication.

III. OVERVIEW

A naive thinking to achieve our goal is to use a normal ABS and simply split the user secret key into two parts. One part is kept by the user (stored in the computer) while another part is initialized into the security device. Special care must be taken in the process since normal ABS does not guarantee that the leakage of part of the secret key does not affect the security of the scheme while in two 2FA, the attacker could have compromised one of the factors. Besides, the splitting should be done in such a way that most of the computation load should be with the user's computer.

We specifically design our system in another manner. We do not split the secret key into two parts. Instead, we introduce some additional unique information stored in the security device. The authentication process requires this piece of information together with the user secret key. It is guaranteed that missing either part cannot let the authentication pass.

A. Architecture:


Attribute-Issuing Authority
Trustee
(1)
(2)
(3)
(4)
request secret key
received
request response key
issued
user
(3)Access granted or denied
Cloud Server Access Control
2) interactive proof of knowledge of protocol
(1)computation within computer (secret key + response key)
secret key
issued response
user

(a) User key generation process

(b) Access Authentication Process

Fig: 1 System Architecture

B. Modules:

1. Trustee: It is responsible for generating all system parameters and initializes the security device.

2. Attribute-issuing Authority: It is responsible to generate user secret key for each user according to their attributes.

3. User: It is the player that makes authentication with the cloud server. Each user has a secret key issued by the attribute-issuing authority and a security key initialized by the trustee.

4. Cloud Service Provider: It provides services to anonymous authorized users. It interacts with the user during the authentication process.

IV. METHODOLOGY

We are providing two factor authentication and security to users files on cloud and for this we have used AES encryption for encrypting the user files that are being uploaded on to the cloud. And user will need a password and also a one time password to log-in into the cloud and after logging into the cloud, if any file is needed for user and if he/she wants to download that file, then a request has to be sent to the Authority and Authority will send a secret key to the user’s registered mail. And then user has to send a request to trustee in order to get permission to download that file.

The Authority only has the privilege to upload the files on to the cloud server. For the system, the DriveHQ cloud server is used. The Authority has the right to send the secret keys to the user upon the request for the file to be downloaded.

The files when uploaded on the cloud are encrypted and are saved as encrypted files. So, even if the cloud is hacked the files are safe in the cloud as the encryption is applied on the files to encrypt them.

When the Trustee grants the permission to the user to download the file only then user will be able to enter the secret key that is being sent to the user’s registered mail and download the file. If either Authority doesn’t send the secret key or if Trustee doesn’t approve the request then file can’t be downloaded.

AES Algorithm:

The Advanced Encryption Standard is based on the concept of the symmetric block cipher. Accordingly, in order to provide protection to classified information and is implemented in software as well as hardware to encrypt sensitive data. Moreover, algorithm comprises of the three block ciphers: AES-128, AES-192 and AES-256. As the cipher encrypts and decrypts data in the blocks of 128 bits using cryptographic keys of 128, 192 and 256-bits, respectively. Certainly, AES encryption algorithm defines a varied number of transformations that are to be performed on data stored in an array. Nevertheless, the first step of the cipher is to insert the data into an array and the cipher transformations are repeated over in the form of encryption rounds. The number of rounds is determined by the help of key length, 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys respectively.

Steps:

1. Rijndael's key is used to derive the round keys from the cipher key. It requires a 128-bit round key block for each round and adds one more.
2. The bitwise xor is used for a block of the round key as it is combined with each byte of the state.
3. According to a table where each byte is replaced with another substitution step in a non-linear manner.
4. A certain number of steps in a cyclic manner are shifted to the last three rows of the state by performing the transposition.
5. Combining the four bytes in each column. an operation is employed where it operates on the columns of the state by mixing it.
6. Finally, Add the Round-Key.
7. The final round consists of the same rounds that are mentioned above except the Mix-columns.

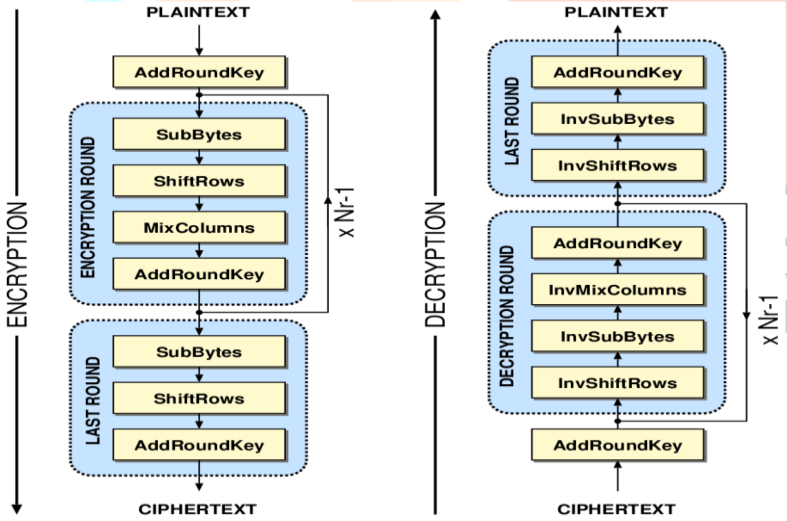


Fig: 2 Execution of AES Algorithm

V. RESULTS

Developed cloud computing services provider system and have some unique features like DriveHQ File manager, DriveHQ online backup and cloud sharing facility. The files uploaded are saved in DriveHQ in an encrypted format, making it more secure.

We have used this and have got the desired results. We have a few users registered with the project and then we have logged in to the system by using the Authority login page and there after logging in we have uploaded some files into the cloud storage by using the File upload section and then we have logged in to the user profile by using the email-id and password and the secret key that is being sent to the user's registered email Id.

Then under the Authority Secret Key, a secret key request has been sent to the Authority for the desired file to be downloaded and then granted the secret key to the user from Authority page. Then when tried to download the file it didn't (we were checking). Then a request has been sent to Trustee to issue a response for the user to download the file desired. Then a response has been sent to the user and then user was redirected to a page where a secret key that has been sent to the mail was asked to enter. And when the secret key was entered and they are matched and then the user was able to download the file from the cloud.

VI. CONCLUSION

The two factor access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also is privacy preserving. The detailed security analysis is as follows:

The mechanism uses OTP services and session keys for login of the user.

Accessing of files by the user is secured twice in the system by trustee response and the secret key.Files stored in cloud server are encrypted making it more secure and non-accessible by the third party authorities. The encryption key is known only by the user.

This paper has a vast future scope of work. It is highly extensible. The security issues are increasing day by day. Since the technologies and its secure use is an important concern we use different and secure access control and authentication mechanism. The major concern is more user friendly and highly secure measures must be developed and implemented. So the future work has a scope on this area where more user friendly security measures has to be concentrated.

BIBLIOGRAPHY

[1] M. H. Au and A. Kapadia. PERM: practical reputation-based blacklisting without TTPS. In T. Yu, G. Danezis, and V. D. Gligor, editors, the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012, pages 929–ACM, 2012.

[2] M. H. Au, A. Kapadia, and W. Susilo. Blacr: Ttp-free blacklistable anonymous credentials with reputation. In NDSS. The Internet Society, 2012.

[3] M. H. Au, W. Susilo, and Y. Mu. Constant-Size Dynamic k-TAA.In SCN, volume 4116 of Lecture Notes in Computer Science, pages111–125. Springer, 2006.

[4] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A secure cloud computing based framework for big data information management of smart grid. IEEE T. Cloud Computing, 3(2):233–244, 2015.

[5] D. Boneh, X. Boyen, and H. Shacham. Short Group Signatures. In Franklin [19], pages 41–55.

[6] J. Bethencourt, A. Sahai, and B. Waters. Cipher text-policy attribute-based encryption. In IEEE Symposium on Security and Privacy, pages 321–334. IEEE Computer Society, 2007.

[7] M. Bellare and O. Goldreich. On defining proofs of knowledge. In CRYPTO, volume 740 of Lecture Notes in Computer Science, pages390–420. Springer, 1992.