International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3850-3858 www.ijaem.net ISSN: 2395-5252

Fine-Grained Two-Factor Access Control forWeb-Based Cloud Computing Services

[1,3,4,5]K.Ramya, M.V.Rakshita, [2]Dr.G.V.Satya Narayana,
Department of CSE, Raghu Institute of Technology, Visakhapatnam, A.P.
N.Yashwanth, K. Navya Sri, Raghu Institute of Technology, Visakhapatnam,
Corresponding Author:Dr.G.V.Satya Narayana, Raghu Institute of Technology, Visakhapatnam, A.P., India

Submitted: 15-07-2021 Revised: 29-07-2021 Accepted: 31-07-2021

ABSTRACT:
In this paper, we have initiated a fine- grained two-factor authentication (2FA) access control system for web-based cloud computing services. Especially, in our proposed 2FA access control system, an attribute-based access control mechanism is used with the requisite of a user secret key. As a user cannot access the system if they do not contain the secret key, this mechanism can strengthen the security of the system, especially in the situations where many people/users share the same system for web- based cloud services. In addition, attribute- based control in the system also authorize the cloud server to control the ingress to those users with the similar set of attributes while protecting user privacy, i.e., the cloud server only knows that the user satisfy the necessary predicate, but has no idea on the exact identification of the user. Finally, we also carry out a simulation to illustrate the achievability of our initiated 2FA access control system.

Keywords: Two-factor authentication (2FA), Cloud computing, Cloud services, Security Mediator (SEM), trusted third party

I. INTRODUCTION:

CLOUD COMPUTING is a virtual host computer system that allowsbusinesses to buy, lease, sell, or distribute software and other digitalresources as a pay-as-you-go service over the internet. Because it is a virtualsystem, it no longer relies on a physical server or a group of machines.

Cloud computing has a wide range of applications, including data sharing, data storage, and big data management and medical data system. End usersuse a web browser, thin client, or mobile app to access cloud-based apps,while the business software and user data are stored on faraway servers. Theadvantages of web-based cloud computing services are numerous, including greater operational efficiencies, decreased costs and capital expenditures, and scalability flexibility and immediate time to market. Though the new cloud computing paradigm offers many benefits, there are worries regarding security and privacy, particularly for web-based cloud services. Becausesensitive data can be stored in the cloud for easy sharing or access, and because approved users can utilize the cloud system for a variety of apps and services, user authentication has become a critical component for any cloud system. Before using cloud services or accessing sensitive data stored in the cloud, a user must first log in. The typical account/password-based method has two drawbacks. To begin with, typical account/password-based authentication is insecure. Privacy, on the other hand, is widely accepted as an important characteristic to address in cloud computing systems. Second, it is typical for multiple people to share a computer. Hackers may find it simple to install spyware and learn the login password from the web browser. The first difficulty is well-suited to a recently developed access control approach termed attribute-based access control. It not only enables anonymous authentication but also establishes access control policies depending on the requester's, environment's, or data object's attributes. Each user has a user secret key issued by the authority in an attribute-based access control system. In practice, the user secret key is kept on the machine itself. When it comes to the second issue with web-based services, it is typical for computers to be shared by multiple users, especially in large corporations or organization.

The initial use of mediated cryptography was to allow for the rapid revocation of public keys. The main principle behind mediated cryptography is that each transaction is handled by an online mediator. Because it controlssecurity capabilities, this online mediator is referred to as a SEM (Security Mediator). If the SEM refuses to comply, no transactions with the public key will be permitted in the future. Key- insulated security was

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3850-3858 www.ijaem.net ISSN: 2395-5252

designed to store long-term keys in a physically safe but computationally restricted device. Users save short-term secret keys on a powerful but insecure gadget that performs cryptographic computations. Short-term secrets are then updated at regular intervals through interaction between the user and the base, but the public key remains constant throughout the system's lifespan. But the disadvantages are:

1. Traditional account/password authentication does not protect your privacy. Privacy, on the other hand, is widely regarded as an important aspect to address in cloud computing systems.
2. It is usual for many individuals to share a computer. Hackers may find it simple to install spyware and learn the login password from the web browser.
3. The adversary acts as the role of the cloud server and tries to find out the identity of the user it is interacting with cloud.

[1] M.H.Au and A.Kapadia have said that some users may misbehave under the cover of anonymity which means quality, for e.g., spoiling or misusing webpages on Wikipedia or posting vulgar comments on you tube. To prevent such misuse, a few anonymous or quality credential schemes have been preferred to reveal access for misbehaving users while maintaining their quality such that no trusted third party (TTP) is involved in the revocation process. [2] M.H.Au, W.Susilo, and Y.Mu have proposed the dynamic k-TAA that allows application providers to independently grant or revoke users from their own access group so as to provide better control over their clients in terms of time and space complexity and existing dynamic k-TAA schemes having complexities O (k), where k is the allowed number of authentication. In this journal paper, we have constructed a dynamic k-TAA scheme with space and time complexities of O (log (k)).However the public key size of this variant is O (k).We then describe a tradeoff between efficiency and set.

[3] X.Huang, and Y.Xiang the main purpose for Big Data Information Management of Smart Grid is that this allows the higher insight and easier integration and also improves efficiency, reliability, economics, and sustainability of electricity services. It plays a crucial role in modern energy infrastructure.

[4] M.bellare and O.Goldreich have done analysis which is the notation of "Proof of Knowledge" has been used in many works as a tool for the creation of cryptographic protocols and other plans.

[5] A,Sahai and B.waters proposed the algorithm which will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message.

[6] S.F,Shahandashti and R.Safavi-Naini have done threshold attribute based signature holder to prove possession of signatures.

[7] Z.Wei, and R H.Deng supported resource-limited mobile devices by offloading computational intensive operations to cloud servers while without compromising data privacy.

In our proposed system, we generate a secret key by using the 3DES Algorithm and so user cannot use his secret key with another device belonging to the others for access and provides a greater flexibility.

Our protocol allows for fine-grained attribute-based access, giving the system a lot of flexibility in terms of setting alternative access restrictionsfor different circumstances. At the same time, the user's privacy is safeguarded. The cloud system merely knows that the user has a certain attribute, but not his or her true identity. We proposed a new 2FA access control system for web-based cloud computing services to demonstrate the feasibility of our system by simulating the protocol prototype. A two- factor authentication (two-factor) access control system has been recognized as a way for the cloud server to not only restricts access to users who have the same set of qualities, but also to protect user privacy.

II. PROBLEM STATEMENT:

In this paper our main goal is to provide more security while login toaccess the cloud services. In this we used the method 2FA to provide more security that user should enter the one time password that is sent to the mail by the authority. This prevents the attackers to access the information. Along with account, password user should enter the one time password that is generated.By using 2FA user will have more security.

III. METHODOLOGY:

In cryptography, Triple DES (3DES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies encryption three times to each data block. Originally the size of the DES cipher key is 56 bits as generally sufficient, but it makes brute-force attacks feasible. Triple DES provides a method of increasing key size to 168 bits by using

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3850-3858 www.ijaem.net ISSN: 2395-5252

3keys to protect against such attacks, without the need to design a completely new block cipher algorithm.
User first generates 3 TDES key k's and distributes them. 3TDES has three keys namely k1, k2, k3 whose individual size is 56 bits. So the actual size of thekey is 3*56=168 bits.

The encryption-decryption process is as follows Step1.Using the single DES key k1 encrypts the plaintext blocks.
Step 2. Using the single DES key k2 decrypt the output generated by the step 1.

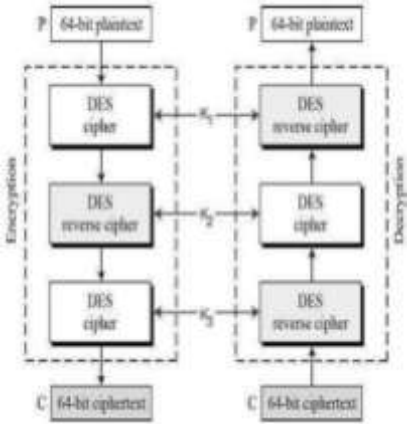

Figure 3.1 Encryption- Decryption process Step 3. Using the single DES key k3 encrypt the output generated by the step 2.
Finally output of step 3 is called cipher text.

IV. IMPLEMENTATION MODULES:

The data user sets their own login credentials. The user provides his or her username, password, e-mail address, and cell phone number. These particulars are saved in a database. The user then picks the login option after entering their username and password. Only the authorized user has access the files in the cloud. After registration, the user must enter a one-time key which is sent to user mail id by the cloud. One time key provides a security to the user account. After logging in to the user home, the user may see all ofhe files that have been uploaded to the cloud.

Here we introduce the two factor access control. To access the file, user must send file request to both TRUSTEE and AUTHORITY. The file request sent to trustee to get the get response and sent to authority to the Secret Key to access the file from cloud. To access the cloud, User should get the valid response from the Trustee and Secret key from the authority. The Secret key sent to the corresponding user's mail id. After getting the Secret key and response from trustee user can access the cloud services. By increasing more layers like Authority and trustee leads to increase in security. Secret key will be generated by using the random key generator which is used to generate a secret key of 6 digits.

2FA is very common among web-based services. Users will feel more secure utilizing shared computers to access web- based services if they utilize2FA. For the same reason, having a two-factor authentication mechanismfor customers of web-based cloud services will improve the system's security. The file will be uploaded to the cloud by the authority. And the submitted file will be encrypted and stored in Drive HQ. Authority will give the secret key to give authentication to the user login and keys to access for file upload and download requests is generated using a random function.The trustee will respond with a security answer for all files. The advantageof doing this is that it provides authentication to the user login and file requests and provides privacy to the data and it uploads files to the cloudanddownload files from the cloud.

Data User Module

- Every user need to register while accessing to cloud.
- After user registered, at the time of user login then user need to provide onetime key to access user home.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3850-3858 www.ijaem.net ISSN: 2395-5252

- One time key will be provided by cloud. Key will be sent to corresponding user mail id.
- After user access the user home, User can view the all files uploaded in cloud.
- User need to send the file request for both trustee and authority.
- After user have the two factor access control, user can download the corresponding file.

Two Factor Access Control:

- If user need to access file in cloud, they need to get the two factor access control.
- Trustee: To get security response from trustee for corresponding file.
- Authority: From authority we need secret key for corresponding file.

Authority:

- Authority will upload the file in cloud and uploaded file will store in driveHQ in encrypted format.
- Authority will give secret key to the corresponding mail id that gives access to the all files.

Trustee Module

- It plays a vital role for cloud server.
- Trustee will give request for all files security response when user request for any file.

Cloud Server Module

- Uploaded files can be viewed in cloud.
- User can download files from cloud.

V. RANDOM FUNCTION USED:

Random function is used to generate the secret key to provide authentication to the user login and keys to access for file upload and download requests. Coding is done using C#.

```
public string CreateKey(int length)
{
const string valid =
"abcdefghij12345ABCDEFGHIJklmnopqrstuv
wxyz67890KLMNOPQRST UV WXYZ=@&? ";
StringBuilder res = new StringBuilder(); Random
rnd = new Random();
while (0 < length--)
{ res.Append(valid[rnd.Next(valid.Length)]);
}
return res.ToString();
}
```

VI. RESULTS AND OUTPUT SCEENS:

Figure 6.1 Home Page

Figure 6.2 Registration Page

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3850-3858 www.ijaem.net ISSN: 2395-5252

Figure 6.3 Login Page

Figure 6.4 Request OTP

Figure 6.5 User Details

Figure 6.6 Trustee Login

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3850-3858 www.ijaem.net ISSN: 2395-5252

Figure 6.7 Accept User Request

Figure 6.8 Request Sent

Figure 6.9 Authority Login

Figure 6.10 Authority Request Key

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3850-3858 www.ijaem.net ISSN: 2395-5252

Figure 6.11 Authority Send Key

Figure 6.12 File Upload

Figure 6.13 Uploaded Files

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3850-3858 www.ijaem.net ISSN: 2395-5252

Figure 6.14 Key for File Download

VII. CONCLUSION:

We've unveiled a new two-factor authentication (two-factor) access control solution for web-based cloud computing services. The suggested 2FA accesscontrol system has been identified based on the attribute-based access control mechanism to not only enable the cloud server to restrict access to those users with the same set of attributes but also to safeguard user privacy.

The proposed 2FA access control system meets the intended security requirements, according to a detailed security study. We proved that the construction is "viable" through performance evaluation.

VIII. FUTURE SCOPE:

Currently, this is being developed to meet the needs for preventing private information leakage during the authentication step. As a result, we make some assumptions about the system's configuration and communication channels. We'll suppose that each user contacts with the cloud service provider anonymously or via IP-hiding technologies. We also assume that the security parameters are generated by the trustee using the methodology specified. We'll leave it to future effort to improve the efficiency while maintaining all of the system's good features.

REFERENCES:

[1]. M. H. Au and A. Kapadia, "PERM: Practical reputation-based blacklisting without TTPS," in Proc. ACM Conf. Comput. Commun. Secur. (CCS), Raleigh, NC, USA, Oct. 2012, pp. 929–940.

[2]. M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," in Proc. 5th Int. Conf. SCN, 2006, pp. 111–125.

[3]. 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 Trans. Cloud Comput., vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.

[4]. M. Bellare and O. Goldreich, "On defining proofs of knowledge," in Proc. 12th Annu. Int. CRYPTO, 1992, pp. 390–420.

[5]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.

[6]. S. F. Shahandashti and R. Safavi- Naini, "Threshold attribute-basedsignatures and their application to anonymous credential systems," Progress in Cryptology (Lecture Notes in Computer Science), vol. 5580. Berlin, Germany: Springer-Verlag, 2009, pp. 198–216.

[7]. Y. Wu, Z. Wei, and R. H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing networks," IEEE Trans. Multimedia,vol. 15, no. 4, pp. 778–788, Jun. 2013.

[8]. Z. Wan, J. Liu, and R. H. Deng, 9HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.

[9]. F. Xhafa, J. Wang, X. Chen, J. K. Liu, J. Li, and P. Krause, "An efficient PHR service system supporting fuzzy keyword search and fine-grained access control," Soft Comput., vol. 18, no. 9, pp. 1795–1802,2012.

[10]. Y. Dodis, J.Katz, S Xu, AndMYung,"Key-insulated publickey cryptosystems," inProc. EUROCRYPT, 2002, pp. 65–82.

[11]. R. Cramer, I. Damgård, and P. D. MacKenzie, "Efficient zero- knowledge proofs of knowledge without intractability

assumptions," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 1751, H. Imai and Y. Zheng, Eds. Berlin, Germany: Springer- Verlag, 2000, pp. 354–373.

[12]. T. H. Yuen, J. K. Liu, M. H. Au, X.Huang, W. Susilo, and J. Zhou, "k- times attribute- based anonymous access control for cloud computing," IEEE Trans. Comput., vol. 64, no. 9, pp. 2595–2608, Sep.2015.