International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

# Design and Analysis of a Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services

**Badiganti Bhaskar [#1] & Komal Kashyap [#2]**

[#1] M.Tech Scholar, Department of Computer Science and Engineering,
Gitam Institute Of Technology, Gitam (Deemed To Be University),Visakhapatnam -530 032.

[#2] M.Tech Scholar, Department of Computer Science and Engineering,
Gitam Institute Of Technology, Gitam (Deemed To Be University), Visakhapatnam -530 032.

## ABSTRACT

*In current day's cloud computing has become one of the fascinating domains which are used by almost all MNC and IT companies. Generally this is formed by interconnecting a large number of systems connected all together for remote servers hosted on internet to store, access, retrieve data from remote machines not from local machines. As the cloud server has the capability to store a lot of valuable data on its memory block, a lot of users can connect with the centralized location to access, retrieve and modify the data which is stored on the cloud server. Till now there was no mechanism available to store the data in an encrypted manner in all public clouds and even private clouds. In this paper, we introduce a new fine-grained 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 both a user secret key and a lightweight security device. As a user cannot 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 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.*

**Key Words:** Two-Factor Authentication (2FA), Secret Key, Encryption, Decryption, Private Clouds.

## I. INTRODUCTION

As we all know that in recent days there was a lot of user's attention towards the cloud data storage for storing and retrieving the data to and from the cloud server. As the data is been increasing day by day almost all the companies are unable to store their valuable data on their own individual devices, so in this situation they opt for a new data storage area known as Cloud Data Storage [1], [2]. Generally cloud service providers allow the users to access their services for a low economical and ascendable marginal cost compared with primitive data storage services. Generally the data which is stored in the cloud server is mainly used for sharing within the users of same group or between the users of different group with a valid authentication. Some of the best cloud data storage services are as follows: Google Drive, DriveHq Server, DropBox and ICloud. As these all are the best among various types of cloud service providers in which the data can be stored either in public cloud or private cloud, sometimes can be stored in both

combine known as Hybrid Cloud. In our current application we try to use the DRIVEHQ hybrid cloud for data storage and accessing in a real time environment manner.


**FIGURE.1. REPRESENTS THE ARCHITECTURE OF VARIOUS CLOUD SERVICE PROVIDERS AND THEIR APPLICATIONS**

From the figure 1, we can clearly find out that there are various cloud service providers that are available in the real time environment that are used for storing various applications like word documents,pdf,excel and many more files. If you look at the above figure you can find out the various cloud service providers like Zip Cloud, Just Cloud, BOX, Google Drive, DROP BOX and a lot more.

As we all know that there are many applications of cloud computing, such as data sharing for remote systems [3], [4], [5], [6], data storage from a remote systems to a centralized location [7], [8], [9], big data management systems [10], medical information system etc.All the cloud users try to access cloud-based applications or cloud server through a web browser to store or access the data to and from the cloud server. There are several benefits of web-based cloud computing services like the ease of accessibility, reduced storage costs and on time data supply. Although they are many principles that govern the principle of cloud computing, still it provides great advantages especially in terms of security and privacy. As we all know that sensitive data will be reside in the cloud server for sharing and access to and from the remote access, the major

issue that arise in the cloud based services is authentication of the cloud server. Initially the cloud user or end user need to register into the cloud server and then once he/she got registered, then the user should substitute his valid credentials for login into the system for various applications and services access. During this login into the cloud, the two main problems that arise in the traditional cloud based systems is account/password based authentication is not strictly privacy preserving, the second mainly problem that arise in the primitive cloud based services is as we all know that the data from the cloud server will be accessed from different people from different locations and hence it may be very easy for a hacker to install some spyware software to learn the login password in any way from the web browser.

In our proposed work, we try to propose a fine-grained two-factor access control protocol for web-based cloud computing services, using a lightweight security device (I.e. a Token). The security token has the following properties: (1) it can compute some lightweight algorithms, e.g. hashing and exponentiation; and (2) it is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside. With this light weighted token mechanism, our protocol provides a 2FA security. First the user secret key (which is usually stored inside the computer) is required. In addition, the security device should be also connected to the computer (e.g. through USB) in order to authenticate the user for accessing the cloud. The user can be granted access only if he has both items. Furthermore, the user cannot use his secret key with another device belonging to others for the access. Our protocol supports fine-grained attribute-based access which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is also almost preserved. The cloud system only knows that the user possesses some required attribute, but not the real identity of the user. To show the practicality of our system, we simulate the prototype of the protocol.

## II. BACKGROUND WORK

In this section we will mainly discuss about the background work that was carried out in order to prove the performance of our proposed Two Factor Authentication (2FA) for web based cloud computing services. Now let us discuss about that in detail as follows:

### MAIN MOTIVATION

In this section we will initially try to find out the system model and assumptions that were used in the current paper. Now let us look about them in detail:

From the below figure 2, we can clearly find out that there are four different services available in the cloud storage and one among them is DaaS which is the main service that what we are using now for providing security for the current application that and prove that this service also gives the best security for the data which is stored inside the cloud memory locations [14]. Now let us discuss about each and every service in detail as follows:

A. IaaS (Infrastructure as a Service)
B. PaaS(Platform as a Service)
C. SaaS(Software as a Service)

D. DaaS (Data /Data Base as a Service)

### A. IaaS (Infrastructure as a Service)

This is the first service out of various services that are available in the cloud. This service mainly deals with application level and it is basically used to set the infra-structure for the users. This service is mainly used to create infrastructure for the set of PCs that are linked in an area. The persons who come under this service is IT Professionals, this is clearly shown in the figure 2.

### B. PaaS (Platform as a Service)

The second important service in the cloud computing is Platform as a Service, where this is mainly used for customization of cloud server. Here in this service we try to set the platform for the users, where the developer comes under this service. Here the cloud server customizes which type of platforms is needed for their company usage is seen in this service.

### C. SaaS (Software as a Service)

The third service one among the best services in cloud computing is Software as a Service, where this is mainly used for a consumer to use the cloud service provider's applications running on a cloud IaaS. Generally business end-users come under this service where all the software's that are required for running the cloud are processed in this service.

### D. DaaS (Data/Database as a Service)

This is the last one among the set of cloud services that was launched and included in various cloud client services is DaaS, which is clearly seen in above figure 2.This DaaS service is used mainly for storing the data in the form of encrypted manner [15]. As this is having various advantages compared with other cloud client services, it has a small limitation like the data which is stored in this DaaS is not stored in the encrypted manner which is stored in the plain manner. So in this proposed thesis we try to encrypt the data before it is uploaded into the cloud using DaaS service.

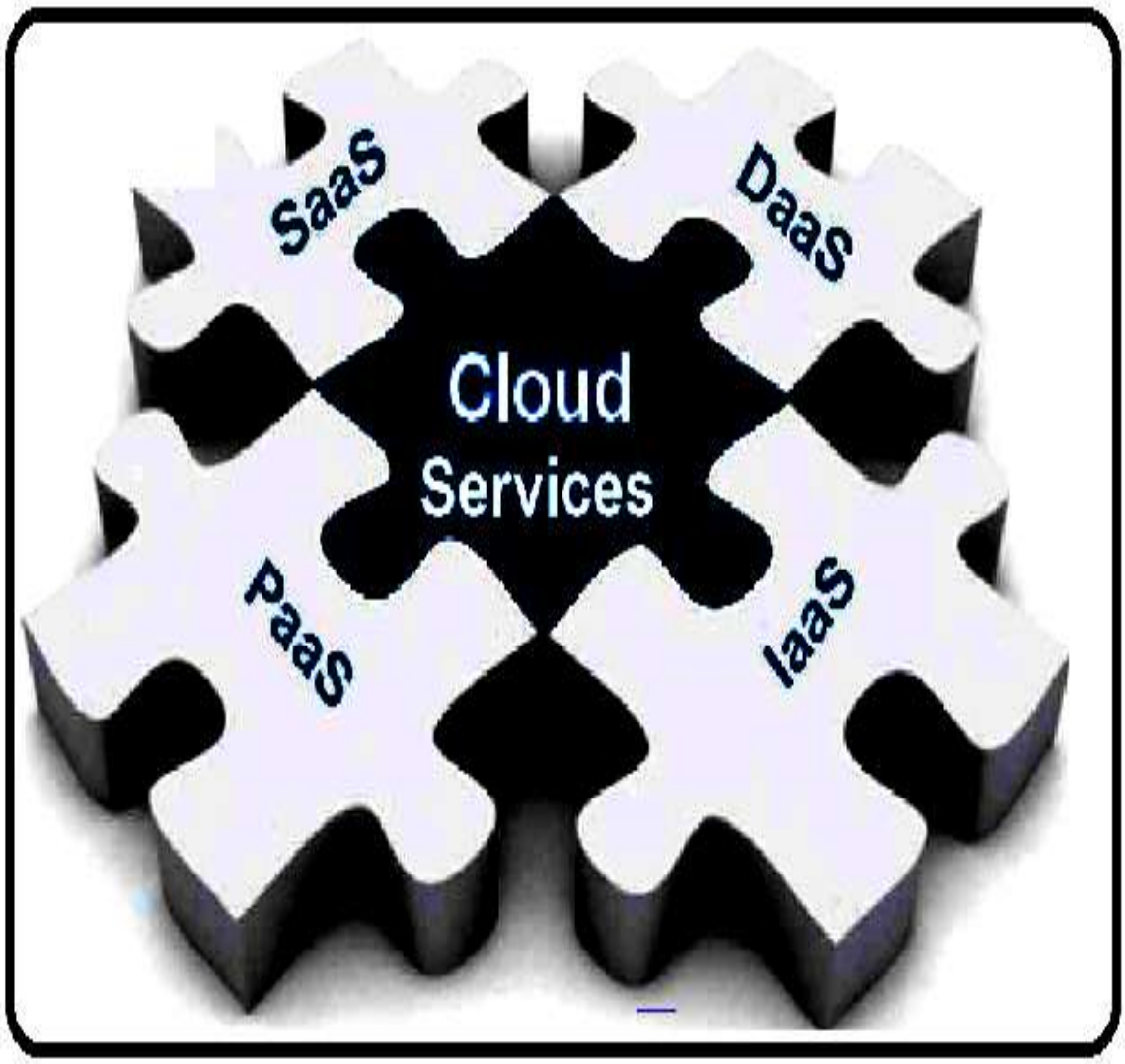


**FIGURE.2. REPRESENTS THE VARIOUS CLOUD SERVICES THAT ARE AVAILABLE IN REAL TIME CLOUD**

Also we enabled this DaaS service by providing extended security by using a dual server technique, where the cloud server will try to generate two keys for providing security for the sensitive data. The user need to have the two keys with him for downloading the data in a plain text manner from the cloud server, if he/she fail to enter valid keys during authentication, the data can't be downloaded in a plain text manner[16]-[18].

## III. PROPOSED NOVEL TWO FACTOR AUTHENTICATION (2FA) FOR WEB BASED CLOUD COMPUTING SERVICES

In this section we will find out the Two Factor Authentication (2FA) for web based cloud computing services mechanism that was used in current thesis in order to give high level of security for the sensitive data which is stored and accessed to and from the cloud server.

## PRELIMINARY KNOWLEDGE

A Two Factor Authentication (2FA) for web based cloud computing services mechanism mainly consists of following entities like

1. **Trustee:** It is responsible for generating all system parameters and initialise the security device(I.e. OTP).

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 device initialized by the trustee.

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

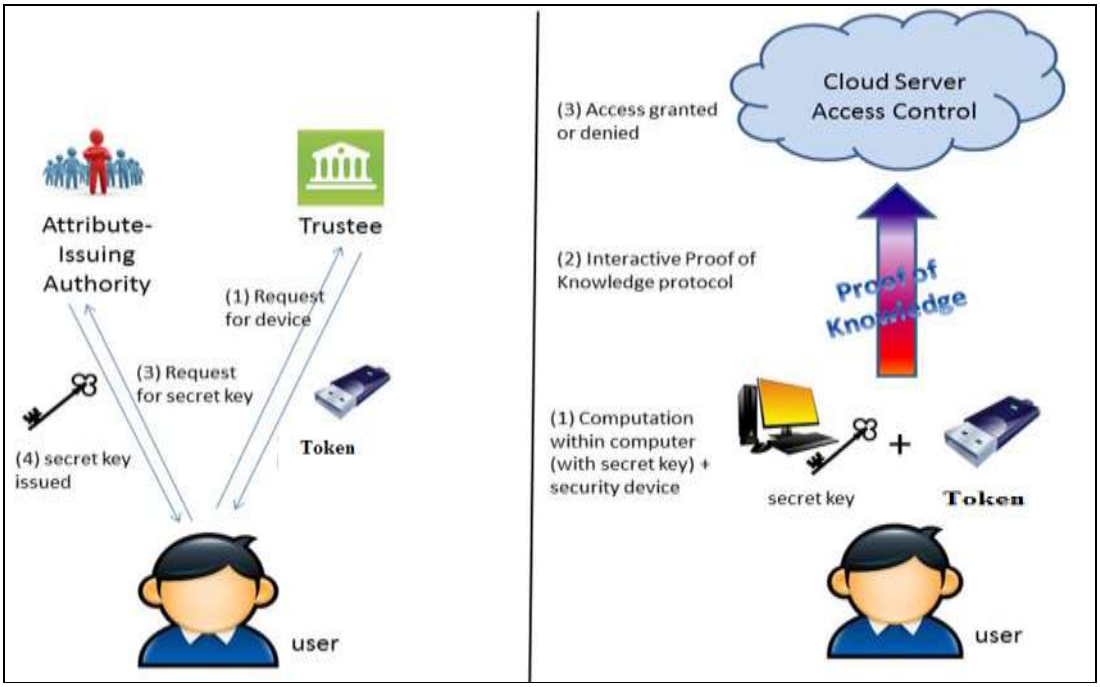


**FIGURE.3. REPRESENTS THE PROPOSED ARCHITECTURE 2FA FOR SECURE DATA STORAGE FOR WEB BASED CLOUD COMPUTING SERVICES**

In this paper, we consider the following threats:

1) Authentication: The adversary tries to access the system beyond its privileges. For example, a user with attributes
{Student, Physics} may try to access the system with policy

"Staff" AND "Physics". To do so, he may collude with other users.

2) Access without Security Device: The adversary tries to access the system (within its privileges) without the security device, or using another security device belonging to others.

3) Access without Secret Key: The adversary tries to access the system (within its privileges) without any secret key.Here device is nothing but OTP [19].

4) Privacy: The adversary acts as the role of the cloud server and tries to find out the identity of the user it is interacting with.

## IV. IMPLEMENTATION PHASE

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed novel IPath protocol. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My-SQL Server. Here we used a live cloud server like DRIVEHQ for showing the performance of our proposed application. The application is divided mainly into following 5 modules. They are as follows:

1. Data User Module
2. Two Factor Access Control Module
3. Trustee Module
4. Attribute Authority Module
5. Cloud Server Module

Now let us discuss about each and every module in detail as follows:

### 1. DATA USER MODULE

In the first module, every user need to register while accessing to cloud. After user registered, at the time of user login then user need to provide one time key to access user home.One time key will be provided by cloud. key will be corresponding user mail id.After user access the user home, User can view the all files upload 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.

### 2. TWO FACTOR ACCESS CONTROL MODULE

If user need to access file in cloud. They need to get the two factor access control.

1. **Trustee:** Need to get security response from trustee for corresponding file.

2. **Authority:** Need to get secret key from authority for corresponding file.

### 3. TRUSTEE MODULE

It acts as admin for cloud server. Trustee will give request for all files security response when user request for any file.

### 4. AUTHORITY MODULE

Authority will upload the file in cloud. And uploaded file will store in drive HQ in encrypted format. Authority will give secret key for all files when user request for any file and the secret key will be send to corresponding user mail Id.

### 5. CLOUD SERVER MODULE

In this module the cloud server can view uploaded files in cloud.It cab also view the details and log information of downloaded files by user in cloud.

## V. CONCLUSION

In this paper, we for the first time have proposed a Novel 2FA (including both user secret key and a lightweight security device like token) access control system for web-based cloud computing services. Based on the attribute-based access control mechanism, the proposed 2FA 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 preserve user privacy. By conducting various experiments on our proposed 2FA access control system, our comparison results clearly tell that our proposed approach is best in providing security for the sensitive data which is stored inside the server space. As a future work we try to further improve the efficiency while keeping all nice features of the system.

## VI. REFERENCES

[1] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.

[2] X. Huang *et al.*, "Cost-effective authentic and anonymous data sharing with forward security," *IEEE Trans. Comput.*, vol. 64, no. 4,pp. 971–983, Apr. 2015.

[3] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in *Proc. 19th ESORICS*, 2014,pp. 257–272.

[4] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, "Secure sharing and searching for real-time video data in mobile cloud," *IEEE Netw.*, vol. 29, no. 2, pp. 46–50, Mar./Apr. 2015.

[5] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," *IEEE Pervasive Comput.*,vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[6] Raul Isea The Present-Day Meaning Of The Word Bioinformatics, Global Journal of Advanced Research, 2015.

[7] Ilzins, O., Isea, R. and Hoebeke, J. Can Bioinformatics Be Considered as an Experimental Biological Science 2015

[8] *Ehrlich, M; Wang, R. (19 June 1981). "5-Methylcytosine in eukaryotic DNA". Science.**212** (4501): 1350–1357*

[9] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Secure and reliable cloud storage against data re-outsourcing," in *Proc. 10th Int.Conf. ISPEC*, 2014, pp. 346–358.

[10] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symp. Secur. Privacy*, May 2000,pp. 44–55.

[11] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *Proc. ACM SIGMOD Int. Conf. Manage.Data*, 2004, pp. 563–574.

[12] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions,"in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, 2006,pp. 79–88.

[13] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. Int. Conf. EUROCRYPT*,2004, pp. 506–522.

[14] G. Di Crescenzo and V. Saraswat, "Public key encryption with searchable keywords based on Jacobi symbols," in *Proc. 8th Int. Conf.INDOCRYPT*, 2007, pp. 282–296.

[15] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Cryptography and Coding*. Cirencester, U.K.: Springer,2001, pp. 360–363.

[16] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. Int. Conf. EUROCRYPT*,2004, pp. 506–522

[17] M. Abdalla *et al.*, "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," in *Proc. 25th Annu. Int. Conf. CRYPTO*, 2005, pp. 205–222.

[18] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in *Proc. Int. Conf. Comput. Sci.Appl. (ICCSA)*, 2008, pp. 1249–1259.

[19] R. Cramer and V. Shoup, "Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption," in *Proc. Int.Conf. EUROCRYPT*, 2002, pp. 45–64.

## VII.ABOUT THE AUTHORS

**BADIGANTI BHASKAR** is currently pursuing his 2 Years M.Tech (CST) in Department of Computer Science and Engineering at Gitam Institute of Technology, GITAM (DEEMED TO BE UNIVERSITY), Visakhapatnam, AP, India. His area of interest includes Data Structure, Software Engineering, Operating System, C and Java Programming.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

**KOMAL KASHYAP** is currently pursuing her 2nd years M.Tech (CST) in Department of Computer Science and Engineering at Gitam Institute of Technology, GITAM (DEEMED TO BE UNIVERSITY), Visakhapatnam, AP, India. Her area of interest includes Data Structure, Software Engineering, Operating System, C and Java Programming.