ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

Fine Grained Authentication Method for Web Based Cloud Service

Karishma Tamboli

M.E. Student, Dept. of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Pune, Maharashtra, India

ABSTRACT: In this paper, proposed system exhibit another fine-grained two-variable approval (2FA) get to control structure for electronic distributed Computing organizations. Specifically, in proposed system proposed 2FA get to control structure, a property based get to control framework is executed with the need of both a customer secret key and a lightweight security device. As a customer can't get to the structure in case they don't hold both, the instrument can enhance the security of the system, especially in those circumstances where various customers have a similar PC for online cloud organizations. Similarly, trademark based control in the structure too enables the cloud server to restrict the access to those customers with a similar proposed system of action of properties while saving customer insurance, i.e., the cloud server just understands that the customer fulfils the required predicate, however no piece of information has on the exact identity of the customer. Finally, proposed system moreover entire a simulation to show the practicability of proposed system proposed 2FA structure.

KEYWORDS: Fine-grained, two-factor, access control, Web services, ASA, RSA.

I. INTRODUCTION

In particular, in proposed framework proposed 2FA get to control framework, a quality based get to control instrument is actualized with the need of both a client secret key and a lightweight security device. As a client can't get to the framework in the event that they don't hold both, the component can upgrade the security of the framework, particularly in those situations where numerous clients have a similar PC for web based cloud services. What's more, quality based control in the framework likewise enables the cloud server to restrict the access to those clients with a similar arrangement of characteristics while saving client protection, i.e., the cloud server just realizes that the client satisfies the required predicate, yet has no clue on the correct personality of the client. At long last, proposed framework additionally complete a reproduction to show the practicability of proposed framework proposed 2FA framework. A sincere theory to fulfil proposed framework will probably utilize an ordinary ABS, simply split the customer secret key enter into two segments. One segment is kept by the customer (set away in the PC) while another part is instated into the security gadget. Uncommon thought must be taken in the process since ordinary ABS does not guarantee that the spillage of part of the Secret key does not impact the security of the arrangement while in two 2FA, the attacker could have exchanged off one of the components. Furthermore, the part should to be done in a way that by far most of the calculation load should be with the customer's PC since the security device shouldn't be able. Despite the fact that the new worldview of distributed computing gives awesome preferences, there are meanwhile also concerns about security and protection particularly for web based cloud services.

As sensitive data information might be put away in the cloud for sharing reason or convenient access; and qualified clients may likewise get to the cloud framework for different applications and administrations, client validation has turned into a basic segment 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 existing traditional account/password based system. First, the existing traditional account/password-based authentication is not privacy-preserving. However, it is well acknowledged that privacy is a basic feature that must be considered in cloud computing systems. 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. An as of late proposed get to control model called attribute based access to control is a good candidate to handle the primary issue. It not only provides in nominate authentication but also further defines access control policies based on different attributes of the requester, environment, or the information protest. In a property based get to control system,1 every client has a client secret key issued by the power. Practically speaking, the client secret key is put away inside the PC.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

II. RELATED WORK

In [2] authors are described **a**. security challenges in Software as a Service (SaaS) model of cloud computing and also end eavors to provide future security research directions **b.** In this Paper proposed system have referred the solution On Cloud Computing Security. In [3] authors are described **a.** cloud security model and security framework that identifies security challenges in cloud computing **b.** proposed system have referred the solution for security challenges in cloud computing and proposed a security model and framework for secure cloud computing environment that identifies security requirements, attacks, threats, concerns associated to the deployment of the clouds. In [4] authors are described **a.** Authentication and access control security issues are still in loop of solutions, because of that so many organizations are waiting for adoption of cloud computing services. This is a review paper for authentication and access control for cloud computing. **b.** proposed system have referred a good solution authentication and access control for the cloud computing. In [5] authors are described **a.** The proposed scheme has been evaluated under various situations. Both of the graphical password schemes have been evaluated individually with various password combinations. The new multi-level graphical password scheme can be considered as a most secure scheme for cloud platforms **b.** proposed system have referred the model will be enhanced with more functionality and higher level of authentication security; it would be implemented by using security questions, image based security for the login protection and at the last level User Identification Number (UIN) would be used to access or view the data in cloud platforms on mobile devices and software systems for computers. In [6] **a.** proposed system propose a new notion called k-times attribute-based anonymous access control, which is particularly designed for supporting cloud computing environment **b.** Proposed system have referred an attribute-based access control mechanism which Can be regarded as the interactive form of Attribute Based Signature. In [8] a. Proposed system proposes a security of Group signature is based on strong Diffie-Hellman assumption and a new assumption in bilinear groups called linear assumption b. Proposed system have referred security of system.

III. PROPOSED METHOD

Proposed system, proposes a fine-grained two factor access control protocol for web based cloud computing administrations, utilizing a lightweight security gadget. The gadget has the following properties:
(1) It can process some lightweight calculations, e.g. hashing and exponentiation.
(2) It is tamper resistant, i.e., it is expected that nobody can break into it to get the secret data put away inside

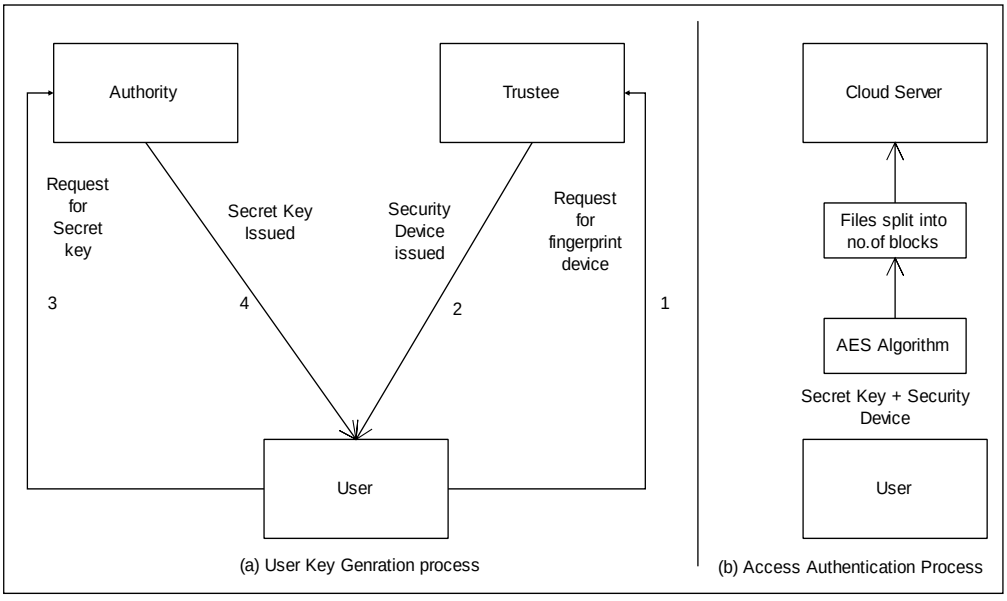

Fig 1: Proposed system Architecture.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

Here in fig [1] first of all user request fingerprint device to the trustee then trustee gives the fingerprint device to the user, if fingerprint of the user matches the fingerprint in the database, then that user is considered as the authorized user. And after that user request for the secrete key to the authority, then authority gives the secrete key to the user. Then with the use of the secrete key & security device the user approaches towards the cloud to upload the file. For security purpose system upload that file in the encrypted form, and divide one file into the no of blocks. System divide file into the number of blocks because, if hacker try to hack the file he cannot able to hack full file because we divide one file into the no of blocks.

- **ALGORITHM**

1. **AES ALGORITHM :**

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
Nb-Block Size
begin
        byte state[4,Nb]
        state = in
        AddRoundKey(state, w[0, Nb-1])
        for round = 1 step 1 to Nr–1
                SubBytes(state)
                ShiftRows(state)
                MixColumns(state)
                AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
        end for
        SubBytes(state)
        ShiftRows(state)
        AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
        out = state
end
```

2. **DSS ALGORITHM :**

1. Generating Random pre message value k where k<0< q
2. Calculate r=(g k mod q) mod q
3. If unlike case that r=0 and start again different random k
4. Calculate s=k -1 (H (m)+xr) mod q
5. If unlike uncase s= then again start with different random k
6. Sign(r,k).

Purpose: For Key with the file.

IV. RESULT & ANALYSIS

- **Screenshots:**

This screenshots represents how this system is work. It describes the responsibilities of the Admin, User & Trustee.

1. **New user registration :**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

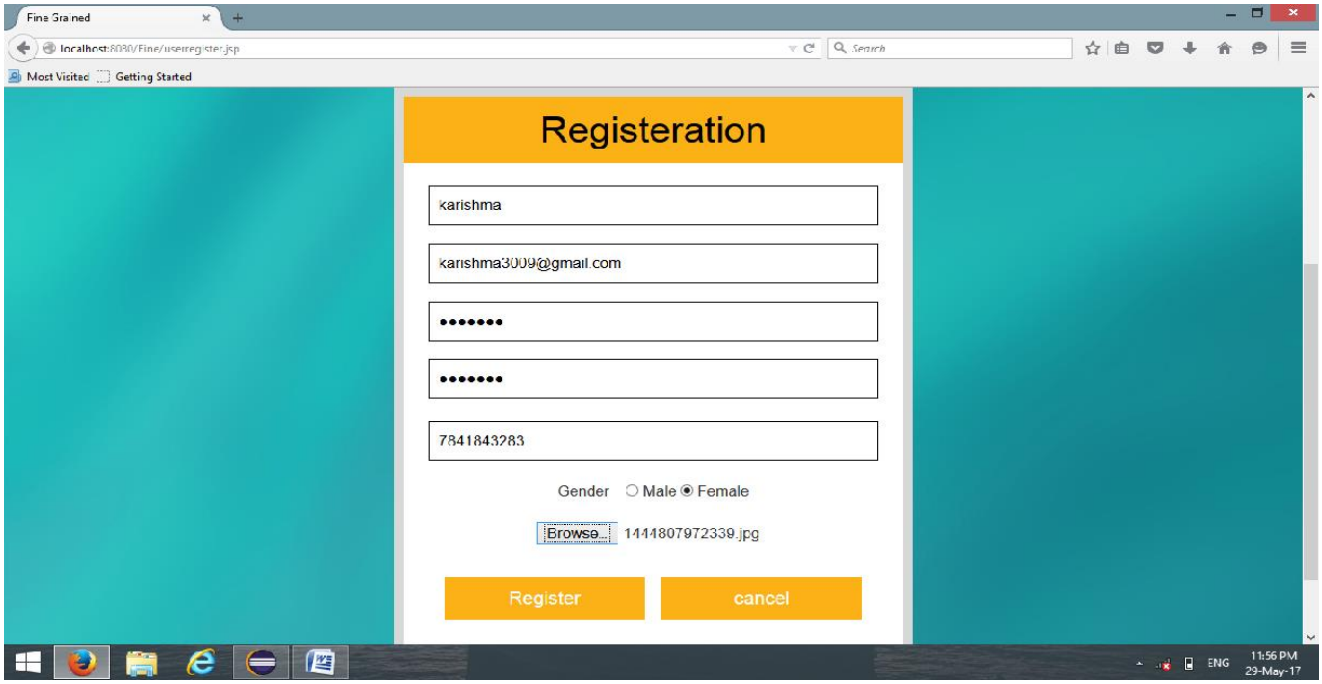

Fig2: New User Registration Form

2. New User registration with fingerprint:

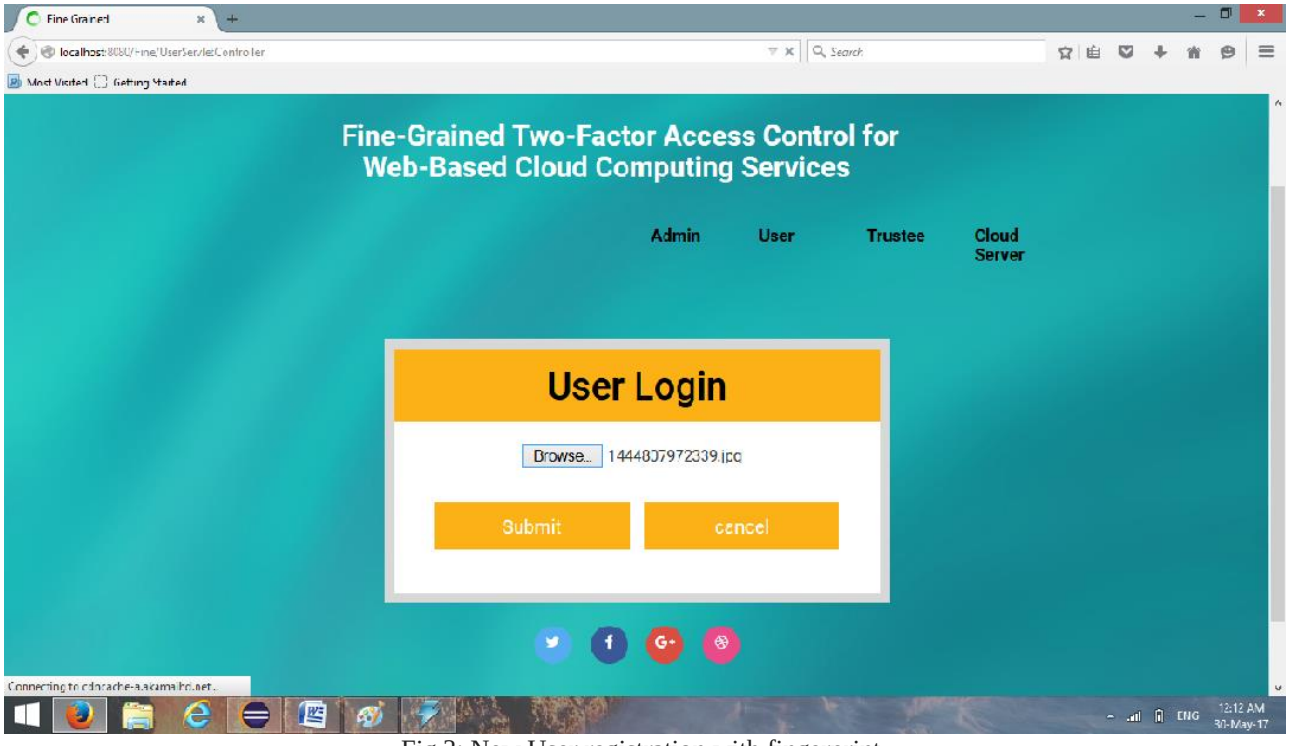

Fig 3: New User registration with fingerprint

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

3. Registered User request to trustee for fingerprint device for further operations :

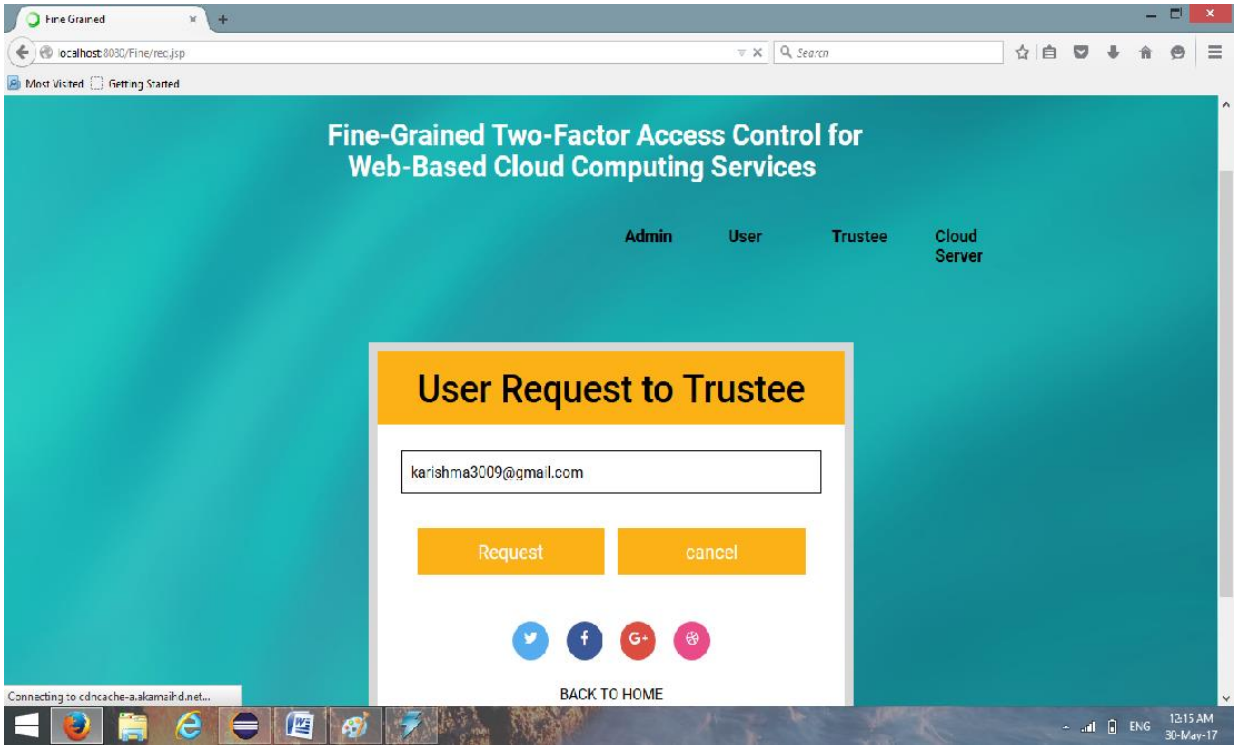

Fig4: Registered User request to trustee for fingerprint device for further operations

4. Registered user login with OTP:

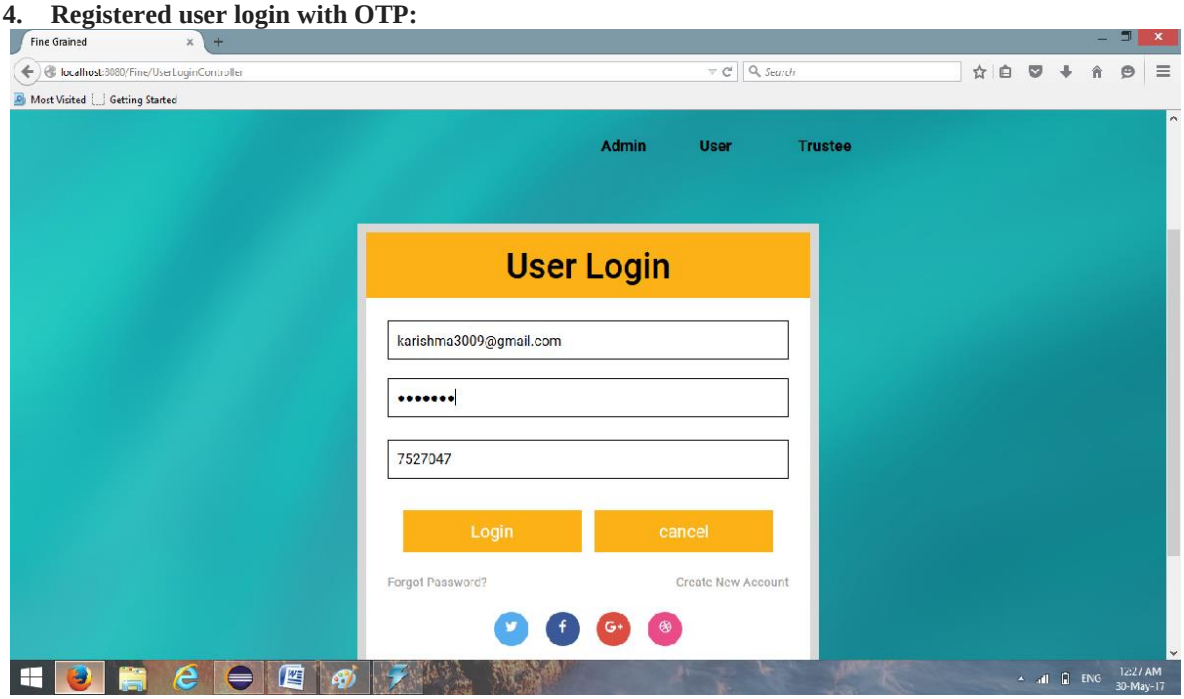

Fig 5: Registered user login with OTP

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

5. **Admin uploads the file in encrypted form and divide that file in no of block**

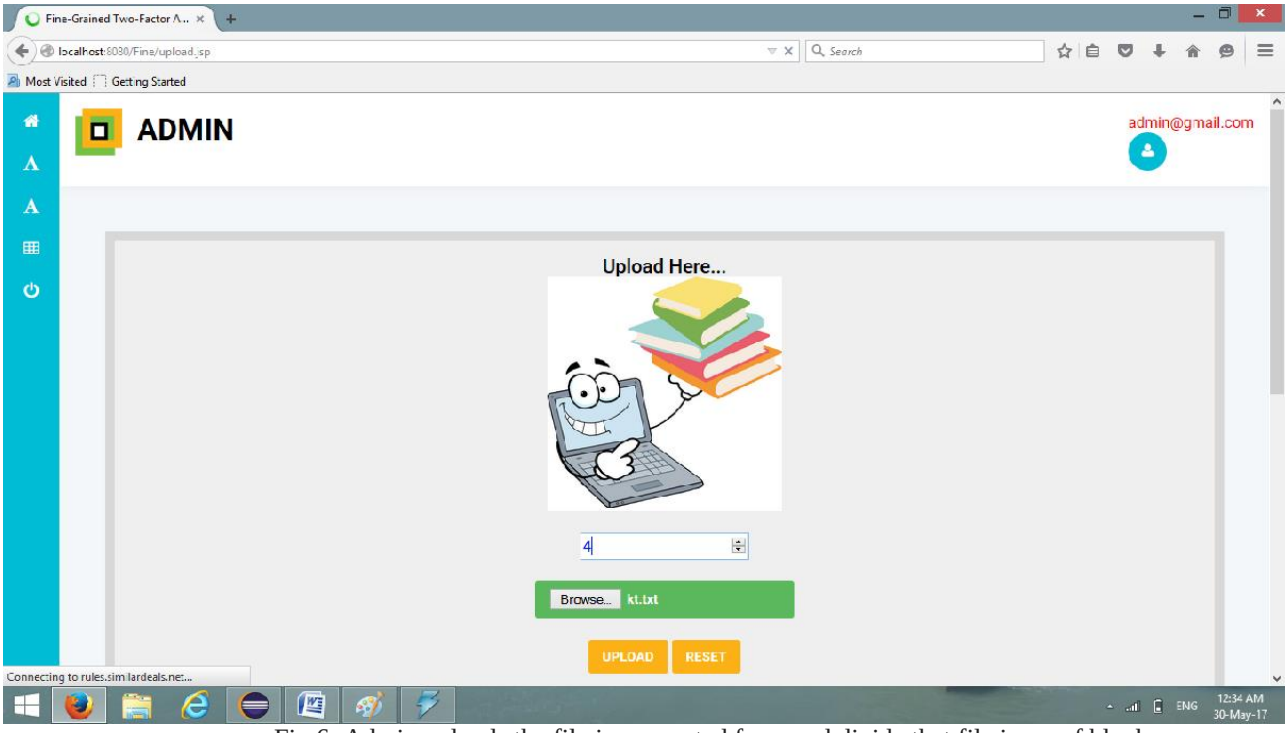

Fig 6: Admin uploads the file in encrypted form and divide that file in no of block

6. **User request file key for uploaded file to the admin:**

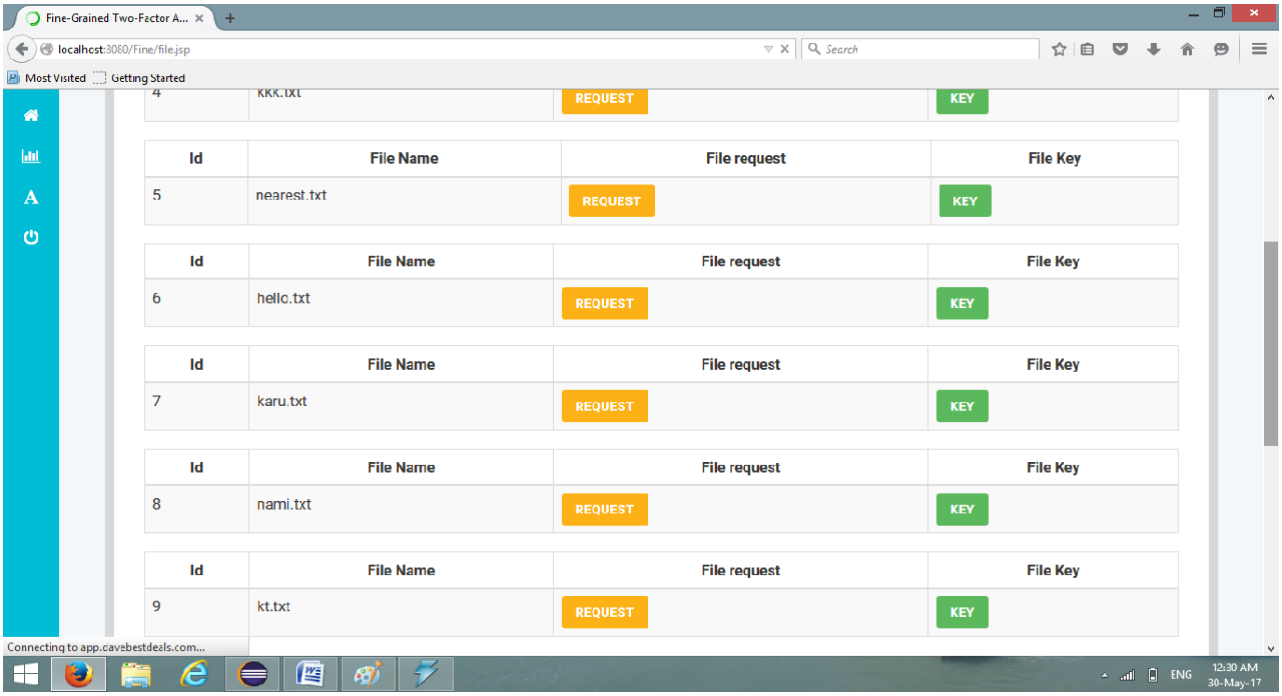

Fig 7: User request file key for uploaded file to the admin

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

7. **User got the key from admin and user gives that key to download file and downloads file:**

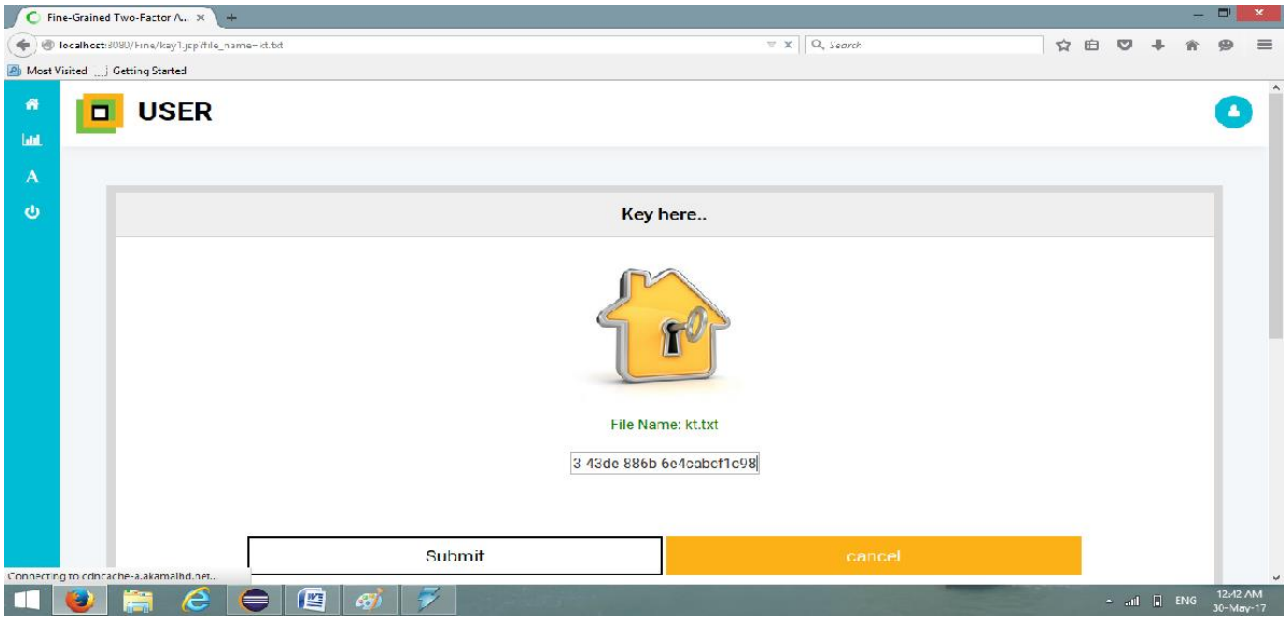

Fig 8: User got the key from admin and user gives that key to download file and downloads file

➢ **FILE UPLOADING GRAPH:**

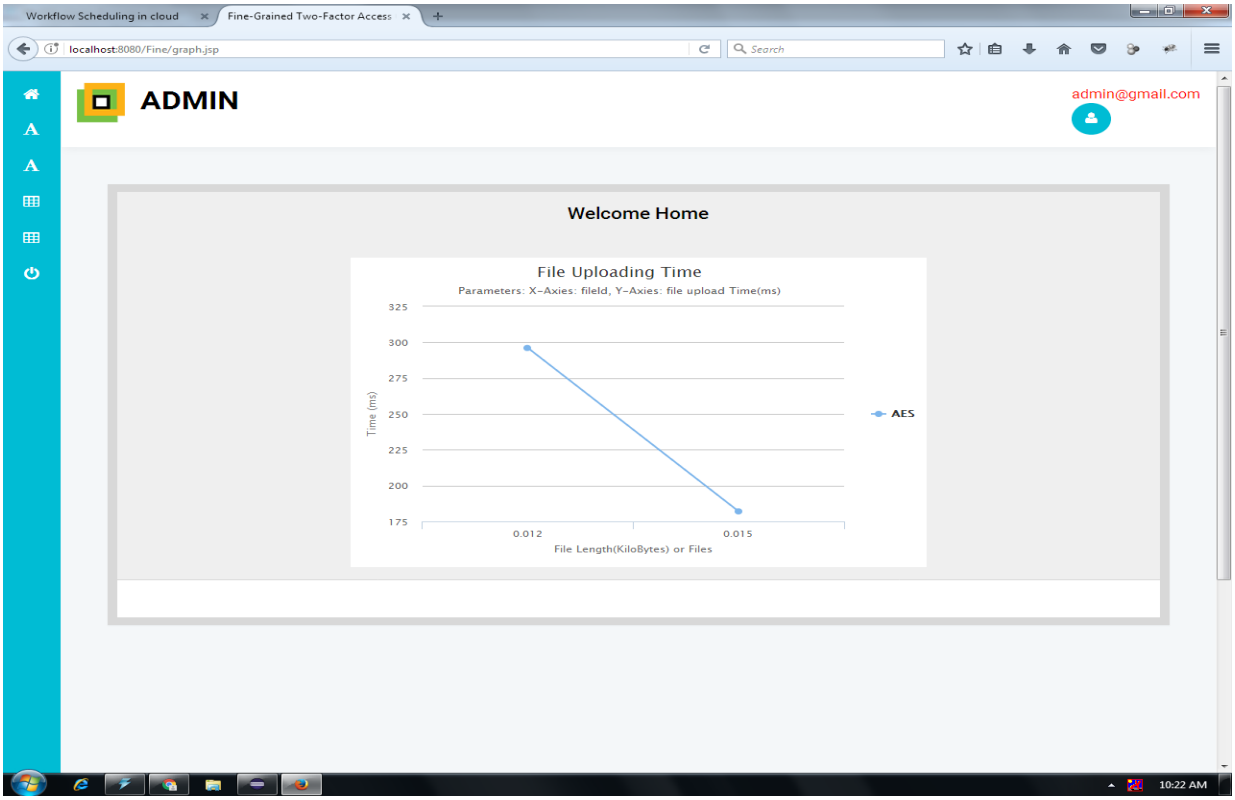

Fig 9: File Uploading Graph

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

➢ **RESULT TABLE:**

File Uploading Time parameter x-axis file id and y-axis file upload Time(ms) using algorithm AES For Encryption.

File Uploading Time	File Size	File Time
First File	12	296
Second File	15	182

Table 1: File uploading With Respect To File Uploading Time

V. CONCLUSION AND FUTURE WORK

In this paper, proposed systems have showed another 2FA get to control structure for online disseminated processing organizations. In view of the characteristic based access control framework, the proposed 2FA access control system has been recognized to not simply give control the cloud server to restrict the path into those customers with a similar plan of properties additionally save client protection. Point by point security examination shows that the proposed 2FA get to control structure finishes the coveted for security essentials. Through execution evaluation, proposed system showed that the advancement is "probably". Proposed system leave as future work to help improve the efficiency while keeping each and every satisfying part of the structure.

REFERENCES

1. Jooseph K. Liu,Member, IEEE, Man Ho Au, Member, IEEE, Xinyi Huang, Rongxing Lu, Senior Member,IEEE, and Jin Li "Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services" IEEE transaction on information forensics and security, vol. 11, no. 3, march 2016
2. Rashmi 1, Dr.G.Sahoo2, Dr.S.Mehfuz3, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", IJCCSA ,Vol.3, No.4, August 2013.
3. KashifMunir and Prof Dr. SellapanPalaniappan," FRAMEWORK FOR SECURE CLOUD COMPUTING", IJCCSA,Vol.3, No.2, April 2013.
4. Mr. AnkushKudale,Dr. Binod Kumar," A STUDY ON AUTHENTICATION AND ACCESS CONTROL FOR CLOUD COMPUTING", Vol. 1(2), (ISSN: 2321-8088) July 2014.
5. Harvinder Singh1, Amandeep Kaur2," Access Control Model for Cloud Platforms Using Multi-Tier Graphical Authentication", Volume 4 Issue 11, November 2015.
6. Joseph K. Liu, Tsz Hon Yuen, Man Ho Au, Xinyi Huang, Willy Susilo, and JianyingZhou,"k-times attribute-based anonymous access control for cloud computing", IEEE Transactions on Computers, 64 (9), 2595-2608.
7. J. Bethencproposedsystemt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp.Secur. Privacy, May 2007, pp. 321–334.
8. D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 41–55.
9. D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," ACM Trans. Internet Technol., vol. 4, no. 1, pp. 60–82, 2004.
10. J. Camenisch, "Group signature schemes and payment systems based on the discrete logarithm problem," Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 1998.

BIOGRAPHY

Karishma Musa Tamboli is a M.E Student in the Computer Engineering Department, Smt. Kashibai Nawale College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India. She received Bachelor of Computer Science and Engineering (BE) degree in 2015. Her research interests are Cloud Computing and Network Engineering etc.