ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Secure Fine Grained and Two Factor Based Access Control Data Sharing in Cloud Environment

Jyotsna Barpute [1], Prof.Shubhangi Suryawanshi[2]

M. E Student, Dept. of Computer Engineering, G.H.Raisoni Institute of Engineering And Technology, Savitribai Phule Pune University, Pune, India[1]

Assistant Professor, Dept. of Computer Engineering, G.H.Raisoni Institute of Engineering And Technology, Savitribai Phule Pune University, Pune, India [2]

ABSTRACT: In this system, fine-grained two-factor approval (2FA) get the chance to control structure for electronic dispersed figuring organizations. Specifically, in our proposed 2FA get the chance to control structure, an attribute-based get the chance to control system is executed with the need of both a customer secret key and a lightweight security contraption. As a customer can't get to the system if they don't hold both, the segment can enhance the security of the structure, especially in those circumstances where various customers have a comparable PC for online cloud organizations. In like manner, attribute-based control in the system besides engages the cloud server to confine the passageway to those customers with a comparative course of action of attributes while securing customer protection, i.e., the cloud server just understands that the customer fulfills the required predicate, yet has no idea on the right character of the customer. Finally, we furthermore do a multiplication to show the practicability of our proposed 2FA structure.

KEYWORDS: Key,Encryption, Fine grained, Access Control

I. INTRODUCTION

Cloud Registering is a virtual host PC system that enables dares to buy, lease, offer, or spread programming and other propelled resources over the web as an on demand advantage. It at no time in the future depends on upon a server or various machines that physically exist, as it is a virtual structure. End customers get the chance to cloud-based applications through a web program, thin client or adaptable application while the business programming moreover, customer's data are secured on servers at a remote zone. The upsides of electronic cloud enlisting organizations are gigantic, which consolidate the straightforwardness of openness, lessened costs besides, capital utilizations, extended operational efficiencies, flexibility, versatility and provoke time to promote. Regardless of the way that the new perspective of cloud figuring gives magnificent purposes of enthusiasm, there are then also stresses over security and protection especially for electronic cloud organizations. As fragile data may be secured in the cloud for sharing reason or supportive get to; and qualified customers may in like manner get to the cloud system for various applications and organizations, customer confirmation has transformed into a fundamental section for any cloud structure. A customer is required to login before using the cloud benefits or getting to the sensitive data set away in the cloud. There are two issues for the ordinary record/secret word based system. In the first place, the standard record/mystery word based affirmation is not protection sparing. In any case, it is very much perceived that protection is a key segment that must be considered in cloud figuring systems. Second, it is essential to share a PC among different people. It potentially basic for developers to acquaint some spyware with take in the login mystery key from the web-program. A starting late proposed get the opportunity to control demonstrate called attribute-based get the chance to control is an OK contender to deal with the essential issue. It not simply gives secretive affirmation moreover portrays get the chance to control approaches in light of different attributes of the requester, condition, or the data dissent. In an attribute-based

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

get the opportunity to control system,1 each customer has a customer secret key issued by the power. Eventually, the customer secret key is secured inside the PC. When we consider the already said second issue on online organizations, it is essential that PCs may be shared by various customers especially in a couple of broad attempts or affiliations.
.

II. RELATED WORK

Attribute-based encryption (ABE) is the foundation of attribute-based cryptosystem. ABE empowers fine-grained get to control over encoded information utilizing get to arrangements and partners attributes with private keys and ciphertexts. Inside this unique circumstance, ciphertext-arrangement ABE (CP-ABE) [6] permits a versatile method for information encryption with the end goal that the encryptor characterizes the get to strategy that the decryptor (and his/her attributes set) needs to fulfill to decrypt the ciphertext. Subsequently, unique clients are permitted to decrypt diverse bits of information as for the pre-characterized strategy. This can dispose of the trust on the capacity server to forestall unapproved information get to. Intervened cryptography was initially presented in [8] as a strategy to permit quick disavowal of open keys. The fundamental thought of interceded cryptography is to utilize an on-line go between for each exchange. This on-line go between is alluded to a SEM (SEcurity Go between) since it gives a control of security abilities. In the event that the SEM does not collaborate then no exchanges with the general population

key are conceivable any more. As of late, an attribute-based form of SEM was proposed.The idea of SEM cryptography was further altered as security intervened certificateless (SMC) cryptography . In a SMC framework, a client has a mystery key, open key and a personality. In the marking or decryption calculation, it requires the mystery key and the SEM together. In the signature check or encryption calculation, it requires the client open key and the relating character. Since the SEM is controlled by a power which is utilized to handle client repudiation, the power declines to give any participation for any disavowed client. In this way denied clients can't produce signature or decrypt ciphertext. Take note of that SMC is not quite the same as our idea. The principle reason for SMC is to tackle the renouncement issue. Accordingly the SME is controlled by the power.Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li,Member, IEEE has proposed a paper on Public Auditing for Shared Data with Efficient User Revocation in the Cloud. Where it gives information of Shared data with efficient user revocation in the cloud.The cloud can improve the efficiency of user revocation. But it has disadvantage as Network Connections Dependency. Cost is more Cheng-Kang Chu, Sherman S.M. Chow, Wen- Guey Tzeng, Jianying Zhou, and Robert H Deng proposed a paper on Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.. More flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges.Allows efficient and flexible key delegation. Network Connections Dependency. Here also has disadvantage that Cost is more and algorithm used are Key Aggreegate Encryption,Decryption. Seung-Hyun Seo, Member, IEEE, Mohamed Nabeel, Member, IEEE, Xiaoyu Ding, Student Member, IEEE, and Elisa Bertino, Fellow, IEEE proposed a paper on An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds. Securely share sensitive data in public clouds.Improve efficiency. here also has disadvantage that Network Connections Dependency and Cost is more algorithm used are public key encryption algorithms. Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed a paper on Privacy Preserving Delegated Access Control in Public Clouds. Decomposition ACPs used to privacy preserving fine-grained delegated access control to data in public clouds.The Owner has to handle a minimum number of attribute conditions while hiding the content from the cloud here also has disadvantage thatNetwork Connections Dependency. Cost is more algorithm used are optimization algorithms, gen graph, random cover, policy decomposition.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

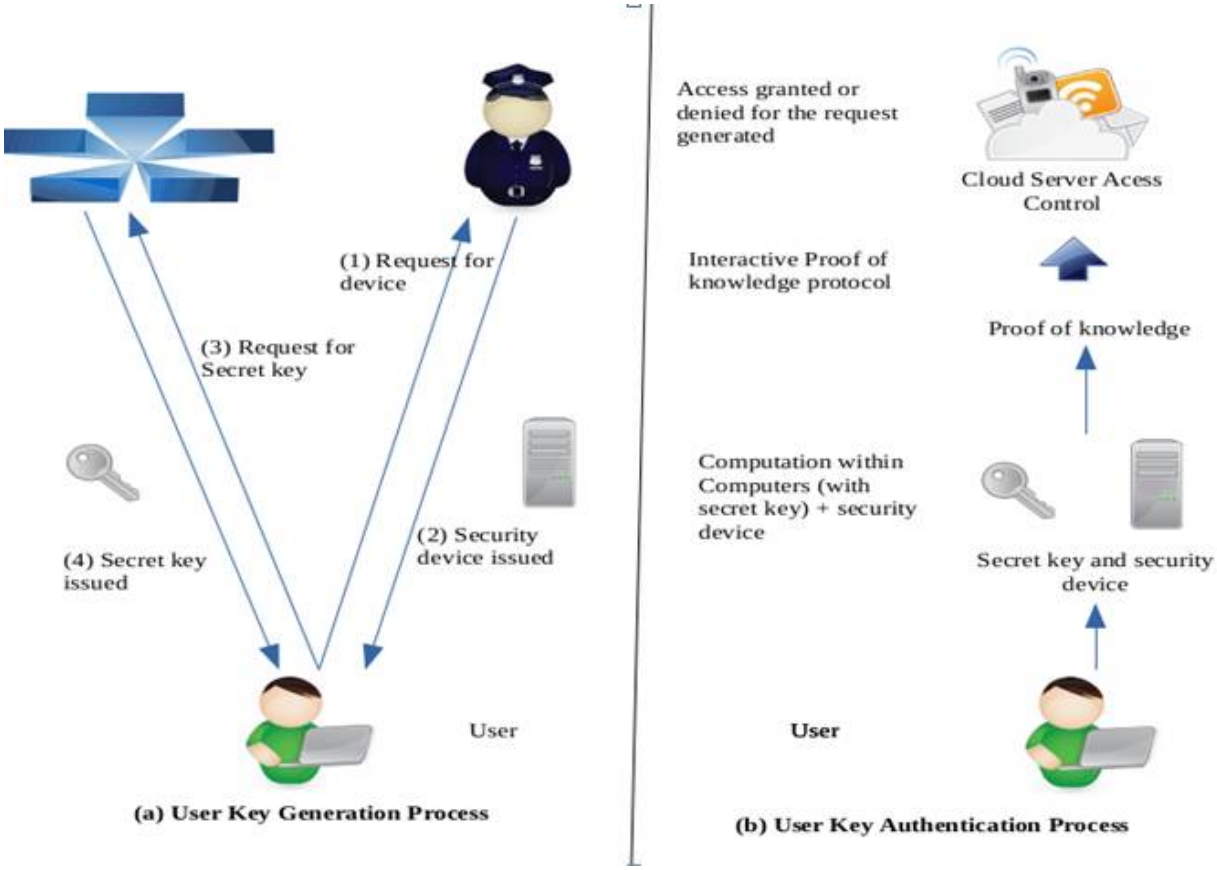

Fig:System Architecture

III. PROPOSED SYSTEM

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.Detailed security analysis shows that the proposed 2FA access control system achieves the desired security requirements. Through performance evaluation, we demonstrated that the construction is “feasible”. Modification of multiuser data, public auditing, probability for high error detection, effective user revocation and computational auditing performance can be characterized by a novel integrity auditing approach for data storage and sharing services. Attack of imitation can be avoid by given scheme. An important feature of cloud storage is data sharing. Sharing along with strong protection of data is the main aspect. Cryptography helps data owner to store data safely on cloud. While considering data privacy, we cannot rely upon traditional technique of authentication, because unexpected privilege escalation will expose all data. Solution is to encrypt data before uploading to the server with uploader’s own key. Data sharing is again important functionality of cloud storage, because user can share data from anywhere and anytime and to anyone. First the admin saves file in the cloud space so that it will be available to users at any time. So he will generate a public key, which is used to encrypt the file. Then he chooses the file to upload and it is encrypted using public key. After encryption the file is uploaded to the cloud space. IP generate hash code of each file which is get uploaded by the data owner. When the user needs to access the file, the admin will share the file details with the user. The generated key sent via secure Email to the user. When the user gets the Email from the admin, he will get the file details. He can now enter the file name and key to download it, in his system. After downloading the decryption is carried out with key. Then the file is saved in the predefined folder in the client system. Un authorized access prevented by giving few preventive measures such as role based access, attack detection and preventions such as if unathorised user trying to access data files then those are

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

identified and user gets blocked and he/she will not be log in to the system.The elimination of the costly certicate verication process makes it scalable and especially suitable for big data analytic.

1.Key issuing authority

In this module data owner will get the key from key issuing authority and that key will be a unique key for every data owner who are going to upload the data on cloud.This key will be used for authentiation of the user.This key is stored in a USB device.

2.File Upload and Encryption

Every time data owner upload the data to cloud that data will get encrypted using AES algorithm.This encryption is required to maintain the security of the data which is being uploaded.At the time of uploading the data user have to plug the USB device which contains the secreat key given by the key issuing authority then only that particulat user will get the cloud access.

3. File Download

When a user wants to download the particular file then that user required the file key to decrypt the file.That key will get shared through secure channel like email.

4.Unauthorized Access

Once the data owner share the encrypted file with its key to authorized user but after some time interval user found accessing some unauthorized things then there is a problem of key recovery.In this module system will identify the unauthorized access through certain keys.When user press certain keys which predefined by the system then because of this system performance get decrease and that get capture by the server.So to recover the given from the user we apply the resignature concept.

IV. ALGORITHM

1. AES
Input: Plain Text
Step1:
Byte state[4,Nb]
State = in
AddRoundKey(state, w[0, Nb-1])
Step2:
for round=1 to Nr-1
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey(state, w[round*Nb, round+1)*Nb-1])
end for
Step3:
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1]
Output:Cipher Text

V. RESULT

This system can access the data files of any type and maximum size allowed is 5 MB. In this system user can upload the data that data may be text file,word file,image etc. This data is encrypted and stored on cloud.User can share the uploaded files to another registered user.The analysis is generated based on total number of files shared by the data owners and their access by users.To measure the accuracy of files downloaded by the user we have taken three analysis

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

parameters.Precision,Recall,Fmeasure.Precision is calculated as total number of (accurate)times file is access divided by total number of files uploaded by the data owners.

precision=no/tcount;
Here no=Number of times file is downloaded correctly by user
tcount=Total number of file uploaded by the data owner
Recall is calculated as total number of files which are not retrieved or incorrectly accessed by the user divided by the total number of files uploaded by the data owner.
Recall=(tcount-no)/tcount
Fmeasure=2*precision* recall /(precision+recall)

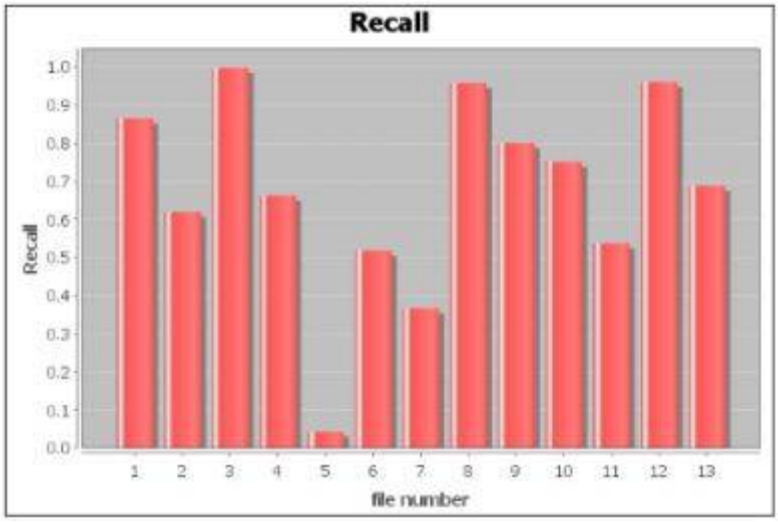

Fig:Recall Graph

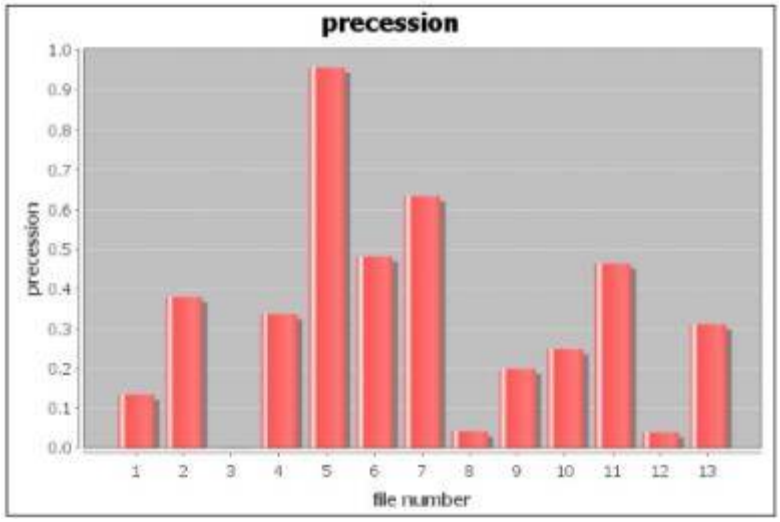

Fig:Precision Graph

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

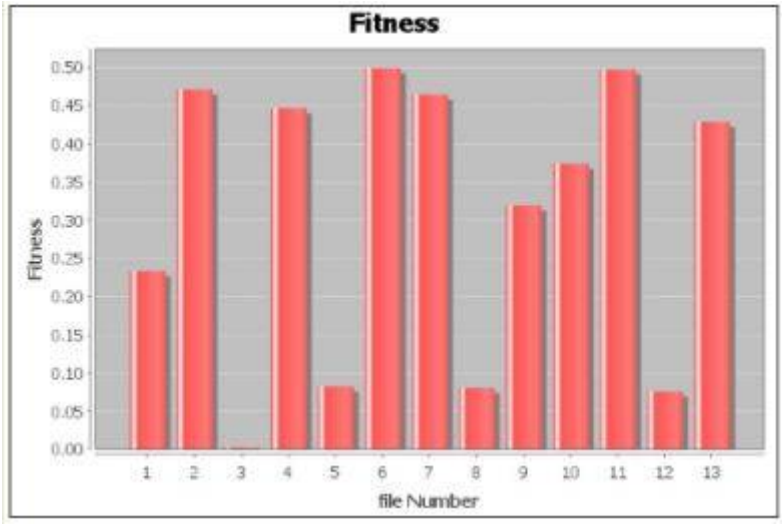

Fig:Fitness Graph

VI. CONCLUSION

This system have presented another 2FA (including both customer puzzle key and a lightweight security contraption) get the opportunity to control structure for online cloud handling organizations. In view of the attribute-based get the chance to control segment, the proposed 2FA get the opportunity to control structure has been recognized to not simply enable the cloud server to confine the passage to those customers with a comparative game plan of attributes also spare customer protection. Bare essential security examination exhibits that the proposed 2FA get the chance to control system achieves the needed security requirements. Through execution evaluation, we demonstrated that the improvement is "feasible". We leave as future work to help upgrade the viability while keeping each and every charming part of the system.

ACKNOWLEDGEMENT

I dedicate all my works to my esteemed guide, Prof. Shubhangi Suryawanshi , whose interest and guidance helped me to complete the work successfully. This experience will always steer me to do my work perfectly and professionally. I also extend my gratitude to (H.O.D.Computer Department)who has provided facilities to explore the subject with more enthusiasm. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Computer Engineering, for their co-operation and support. Last but not the least, I thank all others, and especially my friends who in one way or another helped me in the successful completion of this system.

REFERENCES

[1] Rakpong Kaewpuang, Sivadon Chaisiri ” Cooperative Virtual Machine Management in Smart Grid Environment” IEEE Transactions On Services Computing,Vol.7,No.4,October-December 2014.
[2] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H Deng proposed a paper on ”Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.” IEEE Transactions On Parallel and Distributed System Vol.25,No.2,February 2014.
[3] Seung-Hyun Seo, Member, IEEE, Mohamed Nabeel, Member, IEEE, Xiaoyu Ding, Student Member, IEEE, and Elisa Bertino, Fellow, IEEE” proposed a paper on ”An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds”. IEEE Transactions on Knowledge and Date Engineering, Vol. 26, No. 9, September 2014.
[4] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed a paper on ”Privacy Preserving Delegated Access Control in Public Clouds”. IEEE Transactions on Knowledge and Date Engineering, Vol. 26, No. 9, September 2014.
[5] Kaitai Liang, Man Ho Au, Member, IEEE, Joseph K. Liu, Willy Susilo, Senior Member, IEEE, Duncan S. Wong” proposed a paper on ”A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing”. IEEE Transactions On Information Forensics And Security, Vol. 9, No.10,October 2014.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

[6] Kaiping Xue, Member, IEEE and Peilin Hong, Member, IEEE proposed a paper on "A Dynamic Secure Group Sharing Framework in Public Cloud Computing". IEEE Transactions On Cloud Computing, Vol.2,No.4,October-December 2014.
[7] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma IEEE. proposed a paper on "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation". IEEE Transactions On Services computing Vol.8,No.1,January/February 2015.
[8] Jiawei Yuan and Shucheng Yu, Member, IEEE proposed a paper on "Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification". IEEE Transactions On Information Forensics And Security,Vol.10,No.8,August 2015.
[9] Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE, Jie Wu, Fellow, IEEE, and Siwang Zhou" proposed a paper on "Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing". JOURNAL Of Latex Class Files, Vol. 6, No. 1, January 2015.
[10] XinyiHuang,JosephK.Liu,ShaohuaTang,Member,IEEE, Yang Xiang, Senior Member, IEEE, Kaitai Liang, Li Xu, Member, IEEE, and Jianying Zhou" proposed a paper on "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security". IEEE Transactions On Computers Vol.64.No.4,April 2015.
[11] Xinfeng Ye" proposed a paper on " PrivacyPreservingandDelegatedAccessControlforCloud Applications". ISSN 1007-0214 04/10 pp40-54 Volume 21, Number 1, February 2016
[12] Ovunc Kocabas, Tolga Soyata, Member, IEEE " Emerging Security Mechanisms for Medical Cyber Physical Systems". DOI 10.1109/TCBB.2016.2520933.