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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Two-Factor Data Security Protection Mechanism for Cloud Storage System

Priya J. Khindre[1], Shital Y. Gaikwad[2]

M.E Second Year Student, Dept. of Computer Science and Engineering, Matoshri Pratishthan Group of Institutions Vishnupuri, Nanded. (M.S), India[1]

Asst.Prof.(B.E.M.Tech.), Dept. of Computer Science and Engineering, Matoshri Pratishthan Group of Institutions Vishnupuri, Nanded. (M.S), India[2]

ABSTRACT-Cloud storage is a model of networked storage system where data is stored in pools of storage which are generally hosted by third parties. **i**n this paper, we present another fine-grained two-variable validation (2fa) access control framework for electronic distributed computing administrations. in particular, in our proposed 2fa access control framework, a property based access control system is executed with the need of both a client secret key and a lightweight security device. The sender sends the data and that is stored on cloud. only two factor authenticated User is able to access the data if he has device and secrete key .Data stored on cloud is store by fragments.

KEYWORDS-Encryption,Cloud Computing, Fine-grained, two-factor, access control.

I.INTRODUCTION

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 fulfills the required predicate, however no piece of information has on the exact identity of the customer. Finally, proposed system In this paper, we introduced a novel two-factor data security protection mechanism for cloud storage system, in which a data admin uploads the file and user can access the file if he has two factor that is secret key and device .If they matched then only user is able to access the file.

II. REVIEW OF LITERATURE

In [1] proposed an architecture that ensures the privacy of data stored in cloud storage. The proposed architecture can directly applicable to existing clouds without any modifications or any changes in cloud database. It can be process that connects directly to an encrypted cloud database without an intermediate devices or systems with geographically distributed clients and it also allowed executing independent and operations including those changing the database structure.The proposed systemeliminates the limit on scalability, and availability properties of cloud based solutions.
In [2] described unidirectional proxy re-encryption schemes. This scheme is with chosen cipher text security in the standard model. The two contribution of this proposed system is fitted a unidirectional extension of the Canetti–Hohenberger security model and another one is how to change the scheme to attain security. It provides additional properties like as non-interactive temporary delegations.
In [3] proposed a solution for problem of efficiently delegating in key revocation [4] and generation in Identity Based Encryption (IBE) scheme. In this paper proposed realization of RHIBE, it is constructed based on the scheme called Boneh-Boyen HIBE (BB-HIBE) scheme. The size of cipher text and revocation cost was same for both RHIBE and

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

BB-HIBE schemes. But in RHIBE allows hierarchical structure of entities and selective ID was protected under Decisional Bilinear Diffie-Hellman (DBDH) assumption.

In [5] proposed new definition and security models for single-hop Identity-Based Proxy Re-Encryption (IBPRE) systems. This system holds the property of IBPRE along with conditional re-encryption technique. This new IBPRE overcome two problems are extension of IBPRE to support conditional re-encryption and construction of CCA-secure unidirectional single hop IBPRE without random oracles.

In [6] presented a security definition against chosen cipher text attack (CCA). This definition was for the purpose of certificate less proxy re-encryption. The proposed security model was allowed to adaptively corrupt users. After the corruption of security model and it displayed some proofs to show that a challenges involved in the construction of secure CL-PRE. Finally proved RCCA was secured in random oracle model.

In [7] proposed a solution for constructing a multi-use unidirectional IBPRE scheme problem by converting non-anonymous hierarchical identity-based encryption (NaHIBE) with strongly CPA security to CCA-secure and collusion-resistant multi-use unidirectional IDbased proxy re-encryption MUIBPRE. This technique tries to satisfy the security requirements are CCA security and collusion resistance.

In [8] proposed an approach to protect user's privacy data in cloud environment. This approach explained the compression applied in secret keys in public key cryptosystem to handle the cloud storage by supporting delegation of secret keys in various cipher text classes. This approach is more flexible and efficient than hierarchical key assignments. The hierarchical key assignments analyzed privileges of all key-holders if they allocate the same privileges it saved their space for privileges. The proposed approach used key-aggregate cryptosystem encryption technique where the cipher texts were categorized into various classes.

In [9] proposed an effective third party auditor (TPA) for privacy preserving public auditing to secure a cloud storage system. This technique allows without learning the data content in a cloud environment an external auditor audit user's outsourced data by using privacy-preserving auditing protocol. This technique used random masking andhomomorphic linear authenticator as privacy-preserving auditing protocol. Thus this technique removed burden for cloud user„s and expensive task in cloud.

In [10] presented a proxy-based storage system called NCCloud for fault-tolerant multiple-cloud storage. This system was developed on functional minimum-storage regenerating a network a network-coding- based storage scheme. This proposed system used less repair traffic than redundancy as in traditional erasure codes that sustain less monetary cost due to data transfer. This system removes the encoding operations within the storage nodes during repair thus it reduced the repair traffic in the cloud.

III. SYSTEM ARCHITECTURE

PROPOSED SYSTEM ARCHITECTURE

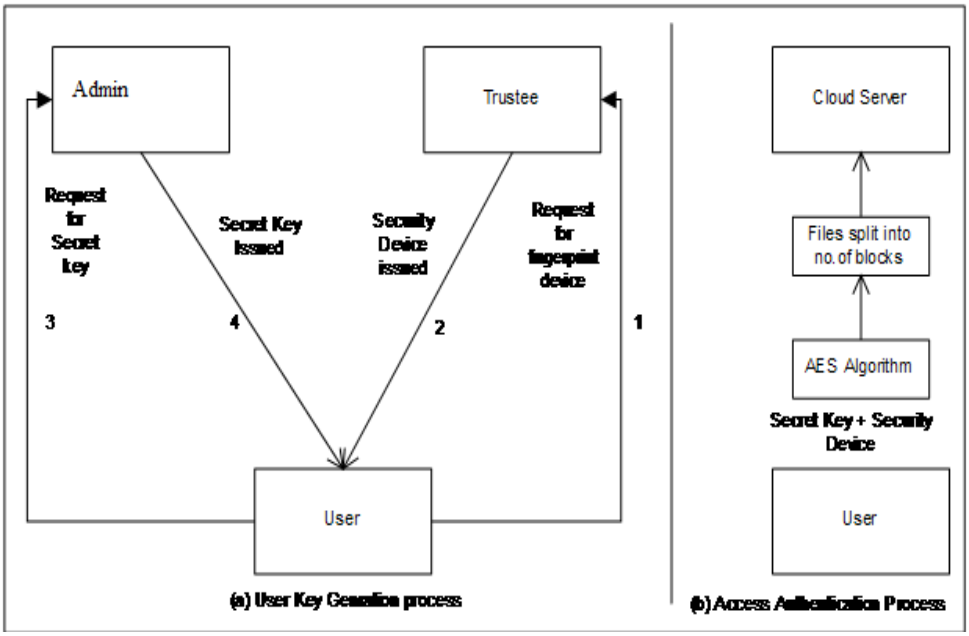


Fig.1: System architecture

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

SYSTEM OVERVIEW-

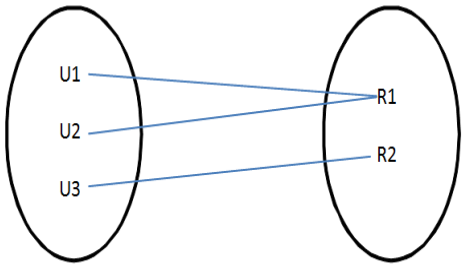
Our Protocol supports two factor access which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time , the privacy of the user is also preserved. File will store on cloud by fragments. Admin uploads the file on cloud. user register to system. user login to system and gives device image and send request for file. Admin send key to user and user enter secret key and get the file.

Algorithm

1) AES Algorithm :

This symmetric encryption Algorithm which are AES is an iterative rather than Festal cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).It takes plaint text as input and then encrypt it and convert into cipher text.

IV. MATHEMATICAL MODEL



U1: Data provided by the user. Eg: Registration user

U2: Data provided by user. Eg: Login

R1: Resulted OTP provided by the trustee

U3: Wrong or incorrect data submitted

R2: Error Occurred

Fig.2:Venn Diagram

Let us consider S as a system for Two-factor Authentication
S= {……
INPUT:

- Identify the inputs

F= {f_1, f_2, f_3 ……,f_n| 'F' as set of functions to execute commands.}
I= {i_1, i_2, i_3…|'I' sets of inputs to the function set}
O= {o_1, o_2, o_3….|'O' Set of outputs from the function sets}
S= {I, F, O}
I = {Enter otp,scanimage,Upload file,, ...}
O = {Get data after performing two factor}
F = {Functions implemented to get the output, AES Algorithm

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

V. RESULT TABLE

File Uploading Time	File Size	File Time(ms)
First File	12	296
Second File	15	332

Table1.Table shows file size and uploading time for file in ms.

VI.PERFORMANCE MEASURES USED

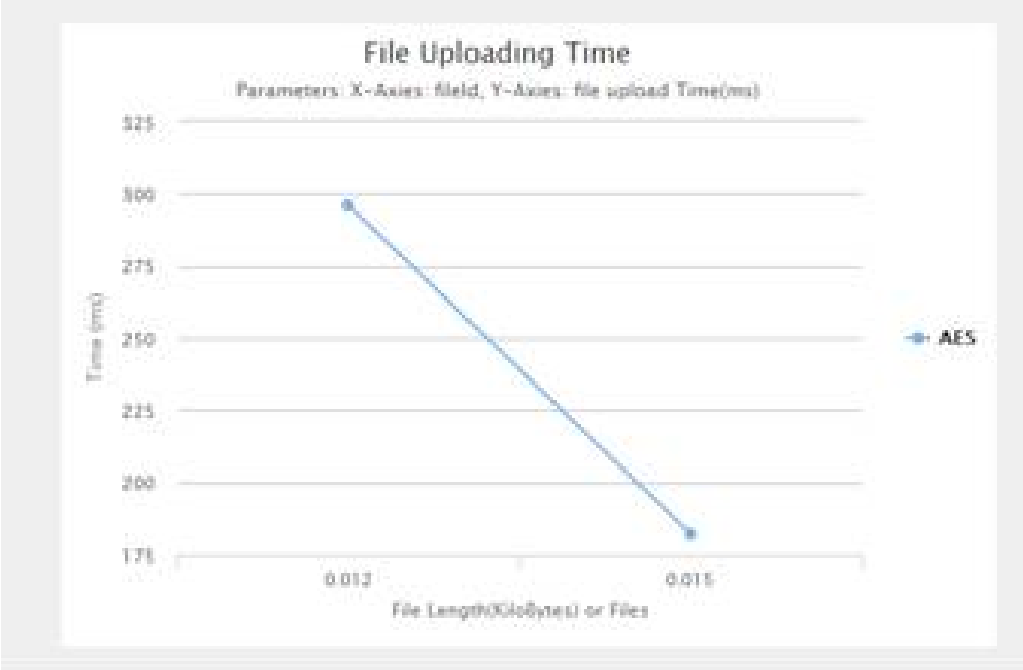


Fig. 2.File Uploading Time parameter x-axis file id and y-axis file upload Time(ms) using algorithm AES For Encryption.

VII. CONCLUSION

In this paper, we introduced a novel two-factor data security protection mechanism for cloud storage system, in which a data sender is allowed to encrypt the data while the receiver is required to use both his/her secret key and a security device to gain access to the data. Our solution not only enhances the confidentiality of the data, but also offers the revocability of the secret key so that once the secret key is revoked.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

REFERENCES

[1] A. Sahai, H. Seyalioglu, B. Waters. Dynamic credentials and cipher text delegation for attribute-based encryption. In: Advances in Cryptology–CRYPTO 2012. Springer Berlin Heidelberg. 2012; 199-217.
[2] B. Libert, D. Vergnaud. Unidirectional chosen-ciphertext secure proxy re-encryption. IEEE Transactions on Information Theory. 2011; 57(3), 1786-1802.
[3] C. Wang, S.S. Chow, Q. Wang, K. Ren, W. Lou. Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on computers. 2013; 62(2), 362-375.
[4] C.K. Chu, S.S. Chow, W.G. Tzeng, J. Zhou, R.H. Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Transactions on Parallel and Distributed Systems. 2014; 25(2), 468-477.
[5] H. Guo, Z. Zhang, J. Zhang, C. Chen. Towards a secure certificateless proxy re-encryption scheme. In: InternationalConference on Provable Security. Springer Berlin Heidelberg. 2013; 8209, 330-346..
[6] H.C. Chen, Y. Hu, P.P. Lee, Y. Tang. NCCloud: a network-coding- based storage system in a cloud-of- clouds. IEEE Transactions on Computers, 2014; 63(1), 31-44.
[7] J. H. Seo, K. Emura. Efficient delegation of key generation and revocation functionalities in identity-based encryption. In: Cryptographers‟ Track at the RSA Conference. Springer Berlin Heidelberg. 2013; 343-358.
[8] J. Shao, Z. Cao. Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. Information Sciences, 2012; 206, 83-95.
[9] J.K. Liu, F. Bao, J. Zhou. Short and efficient certificate-based signature. In: International Conference on Research in Networking. Springer Berlin Heidelberg. 2011; 167-178.
[10] J.K. Liu, K. Liang, W. Susilo, J. Liu, Y. Xiang. Two-Factor Data Security Protection Mechanism for Cloud Storage System. IEEE Transactions
[11] K. Liang, Z. Liu, X. Tan, D. S. Wong, C. Tang. A CCA-secure identity-based conditional proxy re-encryption without random oracles. In: International Conference on Information Security and Cryptology. Springer Berlin Heidelberg. 2012; 231-246. .
[12] L. Ferretti, M. Colajanni, M. Marchetti. Distributed, concurrent, and independent access to encrypted cloud databases. IEEE transactions on parallel and distributed systems, 2014; 25(2), 437-446.
on Computers, 2016; 65(6), 1992-2004.
[13] M. Vimala,K.Vishnukumar. A survey on data security mechanism for cloud storage system, 2016
[14]R. R. Pavithra, V. R. Nagarajan.A survey on certificate revocation scheme using various approaches.Indian Journal of Innovations and Developments. 2016; 5(5), 1-3.