International Journal of Science Engineering and Advance Technology

A New Double Security And Protection Schemes In Cloud Storage

Sk.Shammi[1],T.Naga Raju[2]
[1,2]Dept. Of CSE, Kakinada Institute Of Engineering And Technology, Korangi, EG.Dt,AP, India

ABSTRACT:

The first article is his/her secret key stored in the computer. The second thing is a singleprivatesanctuary device which joins to the computer. It is terrible to decrypt the ciphertext wanting both pieces. Supplementarysignificantly, once the haven device is stolen or lost, this device is rescinded. It cannot be used to decrypt any ciphertext. This can be finished by the cloud server which will instantlyaccomplish some algorithms to revolution the existing cipher text to be un-decrypt able by this device. This route is utterlytranslucent to the sender. Likewise, the cloud server cannot decrypt any ciphertext at any time. The safekeeping and efficiency enquiry show that our system is not only sheltered but also useful.

KEYWORDS: blocks, cloud server, deduplication

1 INTRODUCTION:

. Countless e-banking requestsneed a user to use both a password and a security device (two factors) to login system for currency transfer. The refuge device may exhibition a one-time password to let the user type it into the arrangement or it may be desired to join with the computer. The resolution by means of two factors is to boost the havenfortification for the access control. They will convert more searching and important, as if the e-banking analogy. Essentially, we have noted that the impression of two-factor encryption, which is one of the encryption trends for data protection1, has been meal into some real-world applications, for illustration, full disk encryption with Ubuntu system, AT&T two factor encryption for Smartphones2, electronic vaulting and druva - cloud-based data encryption3. A flexible and mountable two factor encryption device is actuallywanted in the age of cloud computing. That stimulates our work.

2] LITERATURE SURVEY:

we examine roxy provable data possession (PPDP). Out in the public clouds, PPDP involves urgent significance when the customer can't play out the remote information ownership checking. We think about the PPDP framework show, the security display, and the plan technique. In light of the bilinear blending strategy, we plan a productive PPDP protocol. Through security examination and execution investigation, our protocol is provable secure and effective.

we propose a dynamic audit benefit for checking the integrity of an untrusted and outsourced storage. Our audit service is built in light of the systems, part structure, arbitrary inspecting, and file hash table, supporting provable updates to outsourced information and convenient oddity discovery. Also, we propose a strategy in light of probabilistic query and intermittent check for enhancing the execution of audit services.

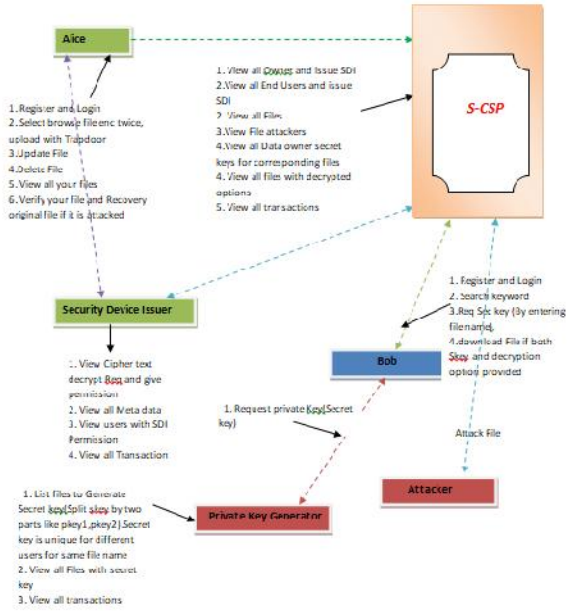
3] PROBLEM DEFINTION:

we have saw that the idea of two-factor encryption, which is one of the encryption tendencies for data protection, has been feast into particular real-world applications, for instance, full disk encryption with Ubuntu system, AT&T two factor encryption for Smartphones2, electronic vaulting and druva - cloud-based data encryption3. Though, these applications hurt from a possible risk about influence revocability that may boundary their feasibility.

4] PROPOSED APPROACH:

When the safety device is taken or reported as lost, this device is canceled. That is, using this expedient can no lengthier decrypt any cipher text in any condition. The cloud will directlyperform some procedures to alteration the existing ciphertext to be un-decryptable by this device. While the user needs to use his new / replacement device to decrypt his/her ciphertext. This procedure is totallyclear to the sender. The cloud server cannot decrypt any ciphertext at any time. We offeranguesstimate of the seriatim time of our model to show its levelheadedness, using some standard results.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

ALICE (OWNER)

Sender will have to register and get officialbeforehand he does any operations. After the approval the sender can upload file with hatch and will have the update, delete, verify and recovery options for the file uploaded.

S-CSP

S-CSP will topic SDI for both owner (Alice) and user (bob). And understanding the file uploaded and the attackers correlated to files in cloud. View the files in decrypted format and with the equivalent secret keys and its transactions.

BOB (USER)

User has to register and login, and hunt for the files by incoming keyword and appeal secret key and download the specific file from the cloud if both secret key and the decryption permissions are providing.

SECURITY DEVICE ISSUER

Opinions all the files decrypt permission request form the users and afford permission and view its connected metadata and the dealings related to the requests from users.

PRIVATE KEY GENERATOR

The private key generator causes the secret key. It ripping the key into two parts such as pkey1 and pkey2. This generated key is unique for different users for same file and understandings all the engendered secret keys and the relationscorrelated to it.

7] ENHANCED TWO FACTOR SECURITY ALGORITHM:

INPUT:S,R,SID,MK,SK,PK,C,M,PKG

STEP1: The public parameters are shared with all parties participating into the system the master secret key is given to the PKG.

STEP2: A SDI and a PKG will respectively generate a security device and a secret key for a registered user IDi in secure channel the user can combine the security device with the secret key to recover message from its encrypted format.

STEP3: a data sender encrypts a data using AES-256 algorithm under the identity of a data Receiver and further sends the encrypted data to the cloud server.

STEP4: the cloud server generates the second-level ciphertext.

STEP5: the user first reports the issue to the SDI. The SDI then issues a new device for the user.

STEP6: The SDI first sends a piece of information to the cloud server so as to inform the cloud to execute the ciphertext updated process.

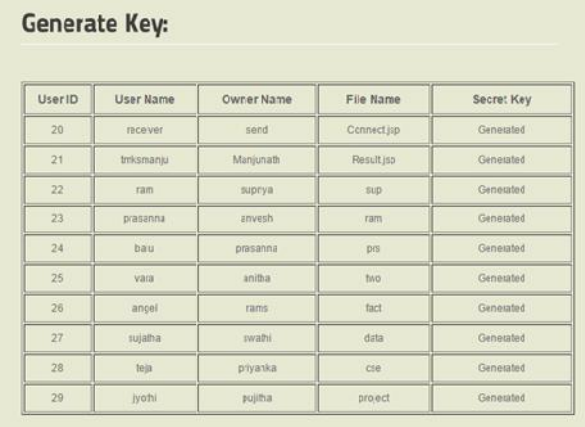
STEP7: After receiving the information the cloud server updates the ciphertext.

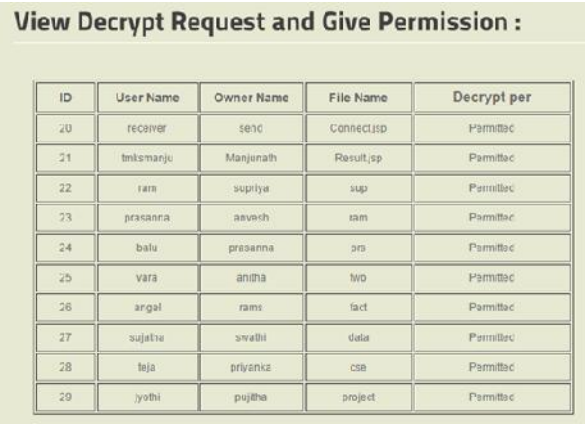
STEP8: A data receiver uses a decryption key and a device to recover the data.

EXTENSION WORK:

Proposed 2FA access control system having both user secret key and a lightweight security device 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 and to reduce communication and computation overhead AES-256 bit algorithm is used as well as for integrity SHA1 is used.

8] RESULTS:





9] CONCLUSION:

we familiarized a new two-factor data security protection device for cloud storage system, in which a data sender is allowable to encode the data with knowledge of the individuality of a headset only, while the receiver is obligatory to use both his/her secret key and a safety device to improvementadmission to the data. Our answer not only improves the privacy of the data, but also proposals the revocability of the device so that once the device is canceled, the consistentciphertext will be efficientmechanically by the cloud server deprived of any notice of the data owner. Also, we offered the security resistant and competenceexamination for our system.

10] REFERENCES

[1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan.Simultaneous hardcore bits and cryptography against memory attacks. In TCC, volume 5444 of Lecture Notes in Computer Science, pages 474–495. Springer, 2009.

[2] S. S. Al-Riyami and K. G. Paterson.Certificateless public key cryptography. In ASIACRYPT, volume 2894 of Lecture Notes in Computer Science, pages 452–473. Springer, 2003.

[3] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen. Certificate based (linkable) ring signature. In ISPEC, volume 4464 of Lecture Notes in Computer Science, pages 79–92. Springer, 2007.

[4] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang. Malicious kgc attacks in certificateless cryptography. In ASIACCS, pages 302–311. ACM, 2007.

[5] M. Blaze, G. Bleumer, and M. Strauss.Divertible protocols and atomic proxy cryptography. In K.

Nyberg, editor, EUROCRYPT, volume 1403 of LNCS, pages 127–144. Springer, 1998.

[6] A. Boldyreva, V. Goyal, and V. Kumar.Identity-based encryption with efficient revocation. In P. Ning, P. F. Syverson, and S. Jha, editors, ACM Conference on Computer and Communications Security, pages 417–426. ACM, 2008.

[7] D. Boneh, X. Ding, and G. Tsudik. Fine-grained control of security capabilities. ACM Trans. Internet Techn., 4(1):60–82, 2004.

[8] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In CRYPTO '01, volume 2139 of LNCS, pages 213– 229. Springer, 2001.

[9] R. Canetti and S. Hohenberger.Chosen-ciphertextsecure proxy re-encryption. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson, editors, ACM Conference on Computer and Communications Security, pages 185–194. ACM, 2007.

[10] H. C. H. Chen, Y. Hu, P. P. C. Lee, and Y. Tang.Nccloud: A network-coding-based storage system in a cloud-of-clouds. IEEE Trans. Computers, 63(1):31–44, 2014.

[11] S. S. M. Chow, C. Boyd, and J. M. G. Nieto.Security-mediated certificateless cryptography. In Public Key Cryptography, volume 3958 of Lecture Notes in Computer Science, pages 508–524. Springer, 2006.

[12] C.-K. Chu, S. S. M. Chow, W.-G.Tzeng, J. Zhou, and R. H. Deng.Key-aggregate cryptosystem for scalable data sharing in cloud storage.IEEE Trans. Parallel Distrib. Syst., 25(2):468–477, 2014.

[13] C.-K. Chu and W.-G.Tzeng.Identity-based proxy re-encryption without random oracles. In J. A. Garay, A. K. Lenstra, M. Mambo, and R. Peralta, editors, ISC, volume 4779 of LNCS, pages 189–202. Springer, 2007.

[14] R. Cramer and V. Shoup. Design and analysis of practical publickey encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput., 33(1):167–226, January 2004.

[15] Y. Dodis, Y. T. Kalai, and S. Lovett.On cryptography with auxiliary input. In STOC, pages 621–630. ACM, 2009.

Ms.Sk.Shammi is a student of Kakinada Institute of Engineering and Technology, korangi. Presently he is pursuing his M.Tech [Computer Science and Engineering] from this college and he received his MCA from V. S. Lakshmi Degree and PG College, affiliated to Andhra University, Kakinada in the year 2013. His area of interest includes Cloud Computer and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr.T.NagaRaju, well known Author and excellent teacher Received M.Tech (Ph.D)from JNTUK university is working as Associate Professor and HOD, Department of MCA, M.Tech Computer science engineering , Kakinada Institute of Engineering and Technology, korangi. He has 3 1/2 years of teaching experience in KIET engineering colleges.