Two-Factor Data Security Protection Mechanism for Cloud Storage System

[1]MOHD IMRAN, [2] S MD ISMAIL

[1]PG Scholar, Department of CSE, Al Habeeb College Of Engineering And Technology, Village Damergidda, Mandal Chevella, District Ranga Reddy, Telangana, India

[2]Associate Professor, Department of CSE, Al Habeeb College Of Engineering And Technology, Village Damergidda, Mandal Chevella, District Ranga Reddy, Telangana, India

Abstract— In that projected an enhance the data security protection mechanism for cloud using two components. During this system sender sends an encrypted message to a receiver with the assistance of cloud system. The sender needs knowing identity of receiver however no would like of different data like certificate or public key. To decode the cipher text, receiver desires two components. The primary issue may be a unique personal security device or some hardware device connected to the computer system. Second one is personal key or secretes key hold on within the computer. While not having these two factors cipher text ne'er decrypted the necessary thing is that the security device lost or stolen, then cipher text cannot be decoded and hardware device is revoked or cancelled to decoded the cipher text.

Index Terms-- Cloud Storage System, Cloud Security, Cloud Protection, Two-Factor Data Security Protection;

I. INTRODUCTION

There are such an oversized variety of advantages, to store the data within the cloud storage. Data within the cloud storage server can be facilitated whenever and where as long as network access. Cloud service provider provides services to the cloud users; they can get any amount of a lot of resources any time. It provides no risk of data Storage maintenance tasks, like exploit further storage capability, is unloaded to the responsibility of a service provider easy to data sharing between numerous clients. in the event that sender needs to share a little of data, as an example, video, text, audio so forth to receiver it would be difficult for sender to send it by email as a result of the scale of data. Instead of that sender transfers the information into the cloud storage then receiver will easily transfer anytime from anywhere. Cloud storage usually refers to a proposal object storage services like Microsoft Azure and Amazon S3 Storage. There are totally different important challenges in cloud computing for securing information, provision of services and storage of data within the internet from differing kinds of attacks. Cloud computing provides an together with area for data storage, computer processing power, shared pool of resources, networks, user applications and specialized corporate. Cloud computing may be a lot of refined. it is simple to forecast that the protection for data protection within the cloud storage ought to be improved. In any cases, these applications go through a possible risk concerning component revocability that will limit their possibility. An expandable and flexible Two-Component encoding mechanism is actually a lot of appropriate

within the term of cloud computing that prompt our System. Cloud computing may be a common term for anything that involves scalable services, delivering hosted services like accessing, information sharing, etc. over the online on demand basis. Generally, user shares numerous kinds of documents through cloud storage networking application like Drop box, cloud me, Google drive. Citrix Cloud computing is thought as an alternative to traditional technology as a result of its low-maintenance and better resource-sharing capabilities. the most goal of cloud computing is to provide high performance energy of computing for numerous field like military and analysis organization for performing billions of computations. The essential security demand is attained by combining each the cryptographically cloud storage together with searchable encoding scheme. In cloud system overall value of data storage is less because it does not need managing and maintaining expensive hardware. Within which information owner first encrypts all information before storing on a cloud in such approach that only user whom having decoding keys is decipher or fetch the data.

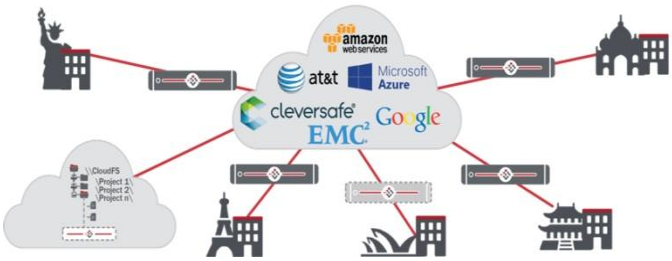


Figure 1: Architecture of Cloud Storage

II. RELATED WORK

In this scheme presents encoded cloud storage based on attribute-based encoded and a brand new keyword search notion: fine-grained access management aware keyword search. During this system initial group the decoded able files of users before execution the keyword search. It decreases data outpouring from the query method. A lot of system uses the easy search approach wherever for looking one encrypted keyword, the cloud server should look round all encrypted files on the storage to check that encrypted keyword to each keyword index, and this disadvantage is removed. Focused on drawback of Identity-Based proxy re-encryption, during which cipher-text are convert into one identity to a different. Proxy re-encryption scheme is used to convert the encrypted cipher-text into decrypted cipher text while not in behalf of underlying plaintext. This drawback removes in Inter-domain identity-based proxy re-encryption. The authors share information and privacy protective auditing theme with massive groups within the cloud. They are utilizing group signature to cipher verification data on shared data. That is the TPA those able to audit correctness of shared data however cannot reveal the identity of the signers on every block. The original user will efficiently add new users to the group and close the identities of signers on all blocks. This paper describes a system Identity based encoding in commonplace model and has distinct disadvantage of existing system like specifically, computation capability, less public framework and a compact safety reduction. Stronger assumption is based on personal key generation quires created by attacker to reduce this disadvantage using linear diff-hellman Exponent assumption. This paper focuses on trace out information for security concern. Using a log based audit services that concentrate on privileged information utilize and additionally contemplate their period of time of utilization for this instance information trace go into the cloud storage. This technique overcome numerous operations on information, additionally repeated creation of tag and sampling. In planned cloud storage systems is used to hold on cipher-text existing access management strategy are not any longer helpful, disadvantage cipher text-Policy Attribute-Based encoding (CP-ABE) may be a technique for access management of encrypted information.

III. FRAME WORK

This paper describes a novel two-factor security protection mechanism for data stored in the cloud. This mechanism provides the subsequent nice features: 1) the system is associate IBE (Identity-based encryption) - primarily based mechanism. That is, the sender only needs to recognize the identity of the receiver in order to send associate encrypted information (cipher text) to him/her. No different data of the receiver (for example public key, certificate etc.) is required. Then the sender sends the cipher text to the cloud wherever the receiver will transfer it at any time. 2) The system provides two-factor encoding protection. So as to decode the data hold on within the cloud, the user must possess two things. First, the user must have his/her secret key that is hold on within the computer. Second, the user must have a novel personal security device which is able to be used to connect with the computer (for example USB, Bluetooth and NFC). It is impossible to decode the cipher text while not either piece. 3) A lot of significantly, the system, for the primary time, provides security device (one of the factors) revocability. Once the safety device is stolen or lost, this device is revoked. That is, exploitation this device you can no longer decode any cipher text. The cloud can immediately execute some algorithms to alter the existing cipher text to be un-decrypt ready by this device. While, the user must use his new/replacement device (together together with his secret key) to decode his/her cipher text; this method is completely transparent to the sender. 4) The cloud server cannot decode any cipher text at any time. Benefits of planned System: one. the answer not only enhances the confidentiality of the information, however additionally offers the revocability of the device so once the device is revoked; the corresponding cipher text are updated automatically by the cloud server with none notice of the data owner. 2. The cloud server cannot decode any cipher text at any time. during this implementation we have five Modules, 1) personal Key Generator 2) Security Device establishment 3) Sender Module 4) Receiver Module 5)Cloud Server Module. Modules Description: one. Personal Key Generator: a non-public Key Generator may be a trustworthy party responsible for issue the private key for each user. 2. Security Device establishment (SDI): A Security Device establishment may be a trustworthy party responsible for issue security device for each user. 3. Sender: This user is that the sender and also the creator of the cipher text. The sender only is aware of the identity as an example email address of the receiver however nothing else associated with the receiver. When the sender has created the cipher text, he/she sends to the cloud server to let the receiver for download. 4. Receiver: This user is that the receiver of the cipher text and includes a unique identity as an example email address. The cipher text is holding on cloud storage whereas he/she will download it for cryptography. The receiver contains a personal key (stored in his computer) and a security device (that contains some secret data associated with his identity). They are given by the PKG. The decoding of cipher text needs each the personal key and also the security device.

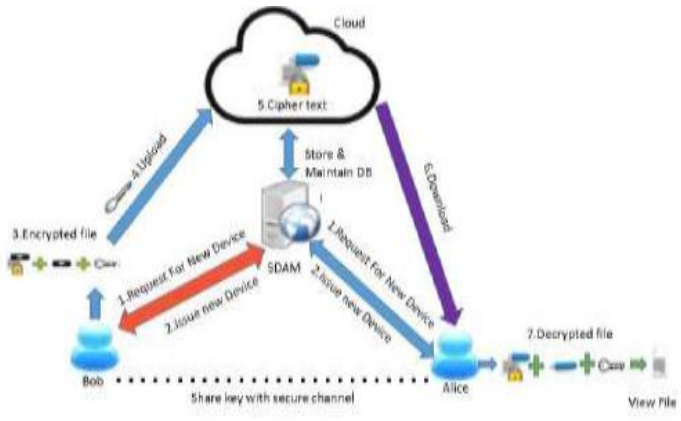


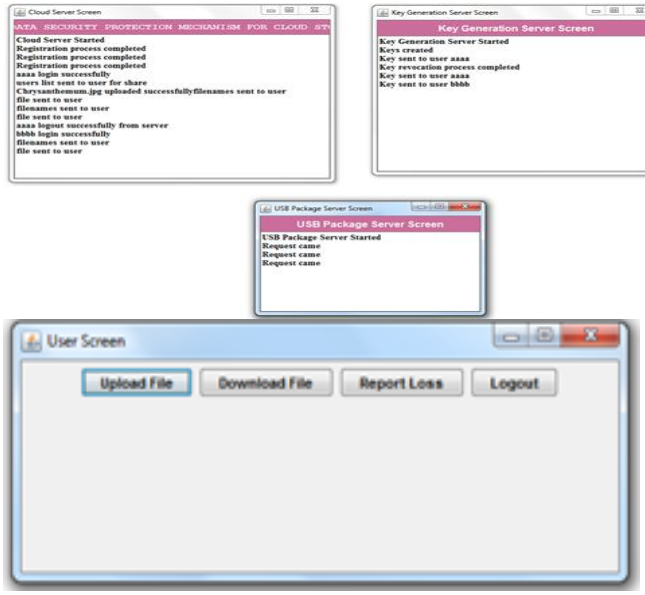
Figure 2: Proposed System Architecture

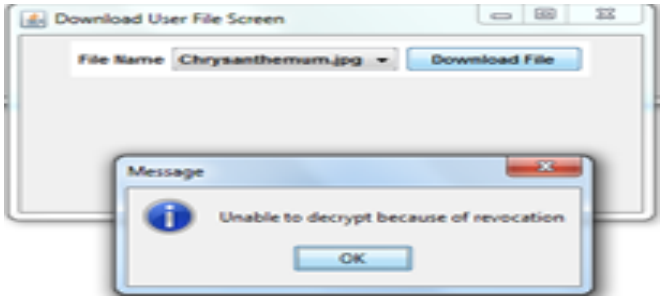
5. Cloud server: The cloud server is responsible for storing all cipher text (for receiver to download). Once a user has reportable loss of his/her security device (and

has obtained a new one from the PKG), the cloud acts as a proxy to re-encrypt the entire past and future cipher text equivalent to the new device. That is, the recent device is revoked.

IV. EXPERIMENTAL RESULTS

In our experiments, initially start the three servers like Cloud server system, Key generator system (The first factor is his/her secret key stored in the computer) , USB package server (The second factor is a unique personal security device which connects to the computer), and finally User applications in that user application initially one or more users register into the system after registration into the system authorized user login into the system after login into the system authorized user upload the file into the system the file is stored into cloud storage server while uploading the data onto cloud, we can create the access policy for different users after successfully uploading the file onto cloud The owner can download the data into local system, after that Owner/ user can report the loss of device, if they lost the device then wont able to decrypt the data after reporting the loss of device Unable to decrypt the data or unable to access the data and try to login as a different user (Owner/ user) and try to downloading the data Owner/ user can download the data to shown in below screens.





Through our implementation authorized owner upload the file into the cloud we can define the access policy for different users and also generate the keys and owner/user can download the file into the local system after that Owner/user can report the loss of device, if they lost the device then wont able to decrypt the data after reporting the loss of device Unable to decrypt the data or unable to access the data and try to login as a different user (Owner/ user) and try to downloading the data Owner/ user can download the data based on that we can send or store the data in efficient and secure manner at lower cost then compare to current methods.

V. CONCLUSION

In this paper, we tend to introduced a novel two-factor data security protection mechanism for cloud storage system, within which data sender is allowed to code the information with knowledge of the identity of a receiver only, whereas the receiver is needed to use each his/her secret key and a security device to realize access to the information. Our resolution not only enhances the confidentiality of the information, however additionally offers the revocability of the device in order that once the device is revoked; the corresponding cipher text are updated mechanically by the cloud server with none

notice of the information owner. Moreover, we tend to confer the protection proof and efficiency analysis for our system.

REFERENCES

[1] A. Sahai, H. Seyalioglu, B. Waters. Dynamic credentials and cipher text delegation for attribute-based encryption. In: Advances in Cryptology–CRYPTO 201 Springer Berlin Heidelberg. 2012; 199-217.

[2] B. Libert, D. Vergnaud. Unidirectional chosen-cipher text secures 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 certificate less proxy re-encryption scheme. In: International Conference 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 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] C.-K. Chu and W.-G. Tzeng, "Identity-based proxy re-encryption without random oracles," in Proc. 10th Int. Con. Inf. Security, 2007, pp. 189–202.

[11] R. Cramer and V. Shoup, "Design and analysis of practical public key encryption schemes secure against adaptive chosen cipher text attack," SIAM J. Comput., vol. 33, no. 1, pp. 167–226, Jan. 2004.

[12] Y. Dodis, Y. T. Kalai, and S. Lovett, "On cryptography with auxiliary input," in Proc. 41st Annu. ACM Symp. Theory Comput 2009, pp. 621–630.

[13] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2002, pp. 65–82.

[14] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Strong key-insulated signature schemes," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2003, pp. 130–144.

[15] L. Ferretti, M. Colajanni, and M. Marchetti, "Distributed, concurrent and independent access to encrypted cloud databases," IEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 437–446, Feb. 2014.