TWO FACTOR DATA SECURITY MECHANISM FOR CLOUD STORAGE.

[1]V.Nareenkanth, [2]Dr. R. Jegadeesan, [3]V.Sowmya, [4]P.Laxmiprasanna, [5]Dr.S.Prabaharan, [6]B.Gangajala, [7] V.Gamana

[3,4,6,7]Final year Student Computer science and Engineering, [1]AssistantProfessor,[2,5]Associate Professor-CSE
[1,2,3,4,5,6,7]Jyothishmathi Institute of Technology and Science, Karimnagar, India

ABSTRACT

Data sharing in cloud storage is receiving substantial attention in information communications technology, as it can provide customers with systematic and beneficial storage services. To ensure the privacy of shared confidential data, cryptographic techniques are generally applied. However, data security so far shows imperative problems in cloud storage to share data. Among them, the basic challenge is how to secure and revoke the cryptographic key. To stop this, we suggest a new data security mechanism for cloud storage that supports the following properties. The cryptographic key is ensured by the two factors. Only if one of the two factors works, the secret of the cryptographic key is maintained. The cryptographic key can be systematically revoked through the combination of proxy encryption and key separation techniques. Data is protected in detail by acquiring the attribute-based encryption technique. In addition, the security review and the execution evaluation show that our advice is safe and beneficial, respectively.

Index terms: two factors, revocability, fine grain, attribute encryption based, proxy re-encryption, cloud storage.

1.INTRODUCTION

The characteristics and advantages, the development and implementation of cloud-based applications have gained enormous motivation in the industry and the research community in recent years. Cloud storage is one of the most successful cloud-based applications, as it matches quite well with the huge demand for data exchange. Huge data exchange with multiple data sharers is a costly task, and the cost on the owner side of the data is directly proportional to the number of data sharers. While this cost could be reduced to the size of the shared data with the help of cloud storage. The only thing the data sharer must do is upload the data to the cloud and grant the right of access to the data sharer. After that, those who share data can get the data from the cloud instead of the owner of the data. Despite the benefits of data sharing in cloud storage, it also presents many opportunities to oppose access to shared data without authorization. To ensure the privacy of shared data, cryptographic schemes are generally applied. The protection of cryptographic schemes comes from the security of the underlying cryptographic key. Currently, the cryptographic key is simply stored in the computer in most existing cryptographic schemes. Although it has been described that stored keys can be revealed by some viruses. To address the key exposure problem, many techniques have been proposed, such as the public key technique with an isolated key and the public key technique isolated with a parallel key. Our knowledge, the exposure of the cryptographic keys and the problems of revocation in the storage in the cloud have not been revealed; proposed a new two-factor data protection mechanism. The cryptographic key is divided into two parts. One is stored in the user's computer and the other is stored in a security device (for example, smart card), which is similar to electronic banking. Only if one of these two parts is kept secret from the opponent, the privacy of the cryptographic key is maintained. Therefore, "factor two" is named. In addition, once the user's security device was lost or stolen, it could be revoked by using the proxy re-encryption technique. While LLS + 15 aims to solve the security problem of data storage, but not the scenario of data exchange in cloud

computing. Especially, an encrypted text in LLS + 15 is essentially an encrypted text based on identity that can be deciphered by a single user but not by a group of users as in the data exchange scenario. Recently, the exchange of data is becoming a heated concern. While privacy remains the key concern and an equally surprising challenge that reduces the growth of data sharing in the cloud.

Naive solution:

At first glance, it seems that we can solve the problem of key exposure and revocation in the data exchange scenario by simply replacing the IBE scheme in LLS + 15 with the ABE scheme. In any case, it cannot work admirably to share data in cloud storage due to the logical inconsistency between the inefficiency of LLS + 15 and the "pay-per-use" nature of cloud storage. In LLS + 15, when the cloud server obtains the encrypted data, it encodes the data using a public key encryption (PKE) with a public key related to the client's security device. While with respect to the data exchange situation where the encrypted text waits for many clients, the cloud server would encode the data in numerous encrypted texts under numerous public keys. In addition, even data is shared with a client, it must be decrypted twice. Specifically, one is for the IBE encryption, the other is for the PKE encryption. This makes the arrangement inefficient. There is another potential failure for LLS + 15 to understand the revocation of the key, the key source middle in LLS + 15 needs to store the secret of each security device. The moment the EIE scheme is replaced directly by the ABE frame, the size of the secret will increase. It would be a weight for the key origination middle.

Our technique:

To solve the defects of the naive solution, we combine the attribute-based encryption technique, the proxy re-encryption technique and the key separation technique to eliminate the use of PKE and the secret of the storage of the security device in the middle. origin of keys. the key issues of exposure and revocation and fine grain access control support. In LLS + 15, the encrypted texts are of two formats. One is the IBE encrypted text, the other is the encrypted PKE text. Although, in our structure proposal, all the encrypted texts are ABE encrypted texts. The main problems in making our structure work well are how the old security device is revoked and how the new decryption device can be successfully implemented.

To revoke the old security device, we need the cloud to update the old encrypted texts before sending them to the user using the proxy re-encryption technique. When the client requests the new security device, the client must provide a secret to the key source middle to generate a new secret that can be used for the decryption of the updated encryption texts. Compared with LLS + 15, our proposed solution has the following properties.

LLS + 15 is primarily aimed at secure data storage, while our main focus is the secure exchange of data. These are two different functionalities provided by different types of cryptographic solutions. We use a different approach to understand the two-factor methods to solve the key exposure and key revocation difficulties. As a result, there is only one type of encrypted text present in our solution, which makes our solution easier to understand and implement. In addition, the originating middle of keys in our proposal does not require to reserve any other secret, except its own private key. We definitely show how decryption is performed without revealing the secret stored in the security device. Although this part is not mentioned in LLS + 15. When we use ABE as an IBE, our proposal is more efficient than LLS + 15 in terms of computational cost and storage cost.

EXISTING SYSTEM

The cryptographic advantage that supports revocability is the reciprocation of intermediate persons (PRE) proposed by Blaze et al. In a delegate re-encryption project, an intermediate person (for example, semi-trusted in the cloud) can change an encrypted text for one client to another encrypted

text that another client can decrypt, while the mediator can obtain the blocking of only The length of the encrypted text. PRE can be formalized in two classes similar to the progress heading: bidirectional and unidirectional. In Bidirectional PRE, the broker can change the encrypted text from one client to another client and in a different way. In unidirectional PRE, the mediator can simply change more than one way. To expand the efficiency and security of PRE, several plans were proposed.

PROPOSED SYSTEM

To understand the shortcomings of the credulous agreement, we coordinated the feature-based encryption procedure, the intermediary recipient strategy and the key partition system to expel the use of PKE and the mystery capability of the security device in the age approach key while we take care Key issues of presentation and denial and support for detailed access control. In LLS + 15, the encrypted texts are of two arrangements. One is the IBE encrypted text, the other is the encrypted PKE text. Be that as it may, all the texts encrypted in our proposed system are ABE encrypted texts. The fundamental problems in making our system work admirably are the way in which the old security device is discarded and how the new security device can decipher it properly.

2.LITERATURE SURVEY

[9] Cryptographic operations (decryption, signature generation, etc.) are done on insecure device(for example a mobile device). Whose objective is to reduce the damage caused by secret key exposures . The secret key is stored in insecure device are updates at discrete time periods via interaction but a physically -secure device but computationally limited device which stores a “auxiliary key”. we construct in a scheme isolated with key (t, M), an opponent that compromises the insecure device and you get secret keys for up to t periods of your choice you can not violate the security of the encryption system for any of the remaining M-t periods.[10] The physically-secure device (or an opponent who compromises only this device) is not able to duplicate signatures for any time period. Signature operations frequently done on insecure device.[11] Provides Forbearance in opposition to key exposures. their scheme provides a “auxiliary key “which is used to regularly refresh the decryption key. The most interesting part of this scheme is that even if a decryption key of a time period is revealed , the security of the rest of the periods are not affected. In which two different helper keys one after the other refresh a decryption key. The auxiliary key of one system is unconventional from one another. Not only does it decrease the chance of helper key exposures, it also allows frequent refreshing of the decryption key, and over all, increases the security of the system.[12] Key-insulated cryptography is a important technique for securing private keys. The idea of parallel key-insulated encryption (PKIE) where different t physically-secure devices (called helpers) are independently used in key refreshes. The intention was to reduce the risk of exposure for helpers by minimizing the frequency of their association to insecure environments. [13]Our System allows a sender to send an encrypted message to a receiver through a cloud storage The sender only needs to know the identity of the receiver no other information .The receiver should have two things in order to decrypt the cipher text .The first one is his/her secret key stored in the computer .The second one is a unique personal security device which connects to computer.

3.FRAMEWORK AND DESIGN GOAL

In this section, we formalize the system model and attack models considered in this paper, and identify the design goals.

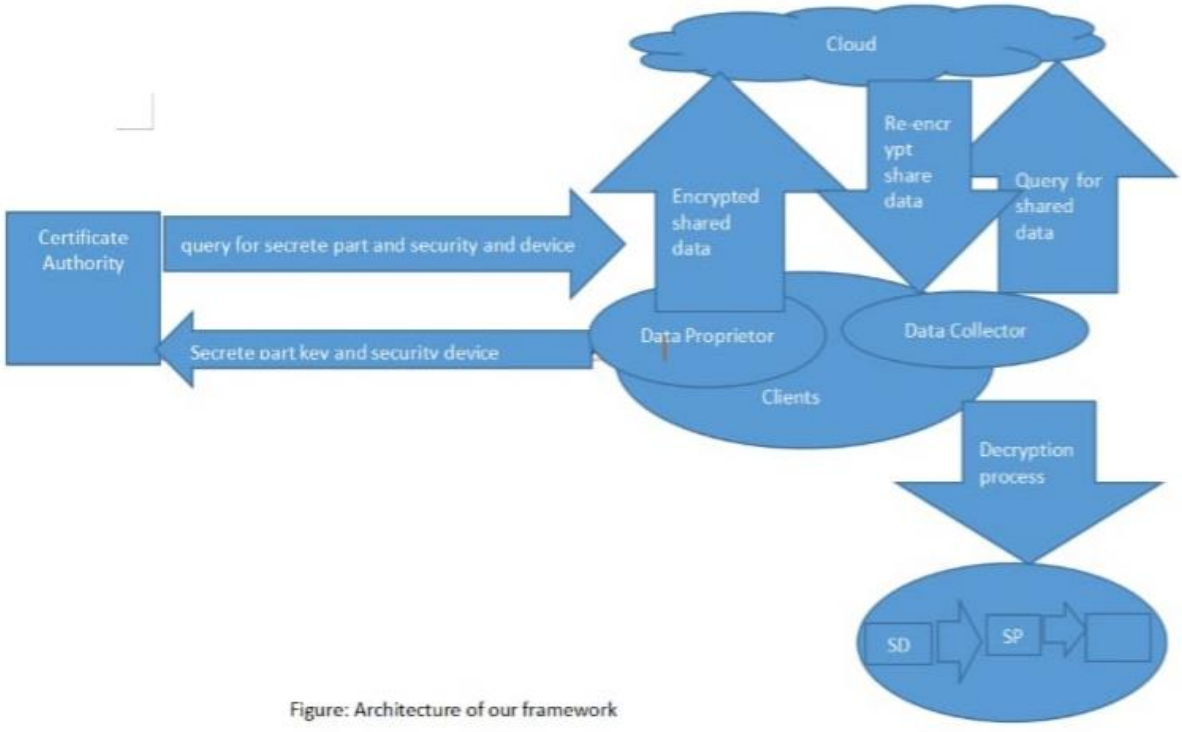

Figure: Architecture of our framework

CENTRAL AUTHORITY (CA)

The central authority is a trusted party that is in charge of issuing the cryptographic key for each client indicated by its set of attributes after it is divided into two sections: the first one called as a secret key of part that is stored in a potentially non trusted location. The other is named as a security device key that is stored in a physically secure future and the lead authority is also responsible for updating each client security device. especially in the key of the security device that is stored in a security device and the corresponding recipient key will be sent to the cloud. note that the recipient key is used to update the encrypted text so that the new security device key works, while the generation of the encryption key requires the data from the previous security device key. As mentioned above, one of the benefits of our proposal is that the central authority does not have to store any secrets for the client. In this case, the way in which the central authority essentially issues an update key to update the old key of the security device cannot work due to the lack of the old key of the security device to solve the problem, we use the key of secret part to recover the key of the security device.

CLOUD

The cloud is a semi-fiduciary part that stores all the encrypted shared information and maintains a table T capable of containing the universal identity of the clients and the related recipient key when the data collector requests the shared data, the cloud functions as an intermediary to re-encrypt the encrypted shared data using the corresponding recipient key of the data collectors and return the data shared to encrypted data receiver.

DATA PROPRIETOR(DP)

A data proprietor is a client that needs to share data with different clients; all shared data is encrypted using CP-ABE according to the access policy

DATA COLLECTOR(DC)

The data collector is a client that can obtain the shared data from the cloud. At that point, the data collector needs to recover the shared data, the cloud first re-encrypts and then returns the encrypted text that is re-encrypted, the encrypted text that is re-encrypted can be decrypted by using the collector itself. SPK and SDK data if the data collector set of attributes complies with the access policy of the shared data. Note that the SDK is never revealed outside of the security device during decryption, while an incomplete decryption process with SDK will run on the security device once the security device has been lost or the data collector stolen can revoke it and get another new security device Through communication with the data collector.

Definition of TFDSP: Two-factor data security protection mechanism for the cloud storage system

The two-factor data security protection mechanism for the cloud storage system (TFDSP) consists of the following algorithms:

INIT → (param, msk): When entering a security parameter λ, the algorithm (executed by the CA) generates the public parameter param and the master secret msk.

KEYGEN (param, msk, Si) → (SPK, SDK): When entering the public parameters param, the secret master key msk and a user UID with the set of attributes Yes, the algorithm (executed by the CA) generates the secret key SPK and security device key SDK for user UID performed between the user who wishes to revoke their security device and the CA. TO At the end of this algorithm, the CA issues the new SDK security device key for the user and the corresponding rekey encryption key for the cloud.

DATAUPLOAD (param, policy, m) → CT: When entering the public parameters param, the access structure policy and the m message, the algorithm (executed by the DO) generates the CT encrypted text and loads it into the cloud.

DATA DOWNLOAD (CT, rk) → CT or CT: When entering the CT encryption text and the corresponding re-encryption key of DR UID, the algorithm (executed by the cloud) first verifies if there exists rk. If this is not the case (the DR security device has never been updated), the algorithm sends the CT to the DR. Otherwise, the algorithm returns the cipher text CT, to the DR.

DATAREVEAL (CT, SPK, SDK) → m: When entering CT, i2, the secret key SPK and the security device key SDK ,. The algorithm (executed by the DR) produces m. Note that SDK is never revealed outside of the security device in this algorithm.

4.CONCLUSION

In this document, we proposed a two-factor data security mechanism for cloud storage. The double factor is done by separating the secret key into two parts, one can be stored in a potentially unsafe location and the other is stored in a tamper-proof device. Only if one of them is kept secret, the proposal remains secure. In addition, with the help of CPABE and PRE, we obtained fine grain access control over encrypted data and the ability to revoke the tamper-proof device, respectively.

REFERENCES

[1] "Dropbox," www.dropbox.com.
[2] Jegadeesan,R.,Sankar Ram,N. "Energy Consumption Power Aware Data Delivery in Wireless Network", Circuits and Systems, Scientific Research Publisher,2016

[3] "Google drive," https://www.google.com/drive/.

[4] "Pcloud," www.pcloud.com/.
[5] Jegadeesan,R., Sankar Ram , and J.Abirmi "Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy" International journal of Advanced Research trends in Engineering and Technology (IJARTET) ISSN:2394-3785 (Volume-5, Issue-1, January 2018

[6] C.Wang, S. S. Chow, Q.Wang, K. Ren, andW. Lou, "Privacy-preserving public auditing [for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[7] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," Services Computing, IEEE Transactions on, vol. 5, no. 2, pp. 220–232, 2012.

[8] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," Services Computing, IEEE Transactions on, vol. 6, no. 2, pp. 227–238, 2013.

[9] H. C. Chen, Y. Hu, P. P. Lee, and Y. Tang, "Nccloud: a networkcoding- based storage system in a cloud-of-clouds," Computers, IEEE Transactions on, vol. 63, no. 1, pp. 31–44, 2014.
[10] Jegadeesan,R.,T.Karpagam, Dr.N.Sankar Ram , "Defending Wireless Network using Randomized Routing Process" International journal of Emerging Research in management and Technology ISSN: 2278-9359 (Volume-3, Issue-3) . March 2014

[11] "Encryption key virus threat," http://searchsecurity.techtarget.com/tip/ Encryption-key-virus-threat.
[12] Jegadeesan,R., Sankar Ram,N. "Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling", Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016

[13] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems," in Advances in Cryptology–EUROCRYPT 2002. Springer, 2002, pp. 65–82.

[14] "Strong key-insulated signature schemes," in Public Key Cryptography–PKC 2003. Springer, 2002, pp. 130–144.
[15] Vijayalakshmi, Balika J Chelliah and Jegadeesan,R., February-2014"SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups" Global journal of Engineering,Design & Technology. G.J. E.D.T.,Vol.3(1):43-47 (January-February, 2014) ISSN: 2319 –7293

[16] G. Hanaoka, Y. Hanaoka, and H. Imai, "Parallel key-insulated public key encryption," in Public Key Cryptography-PKC 2006. Springer, 2006, pp. 105–122.

[17] B. Libert, J.-J. Quisquater, and M. Yung, "Parallel key-insulated public key encryption without random oracles," in Public Key Cryptography– PKC 2007. Springer, 2007, pp. 298–314.
[18] J. Liu, K. Liang, W. Susilo, J. Liu, and Y. Xiang, "Two-factor data security protection mechanism for cloud storage system," Computers, IEEE Transactions on, vol. 65, no. 6, pp. 1992–2004, 2016.

[19] V. J. Winkler, "Cloud computing: Privacy, confidentiality and the cloud," https://technet.microsoft.com/en-us/magazine/dn235775.aspx.

[20] Jegadeesan,R., Sankar Ram "Defending Wireless Sensor Network using Randomized Routing "International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938
[21] J. K. Liu and D. S. Wong, "Solutions to key exposure problem in ring signature." IJ Network Security, vol. 6, no. 2, pp. 170–180, 2008.

[22] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–EUROCRYPT 2005. Springer, 2005, pp. 457–473.
[23] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attributebased systems," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 99–112.
[24] Jegadeesan,R., Sankar Ram, M.S.Tharani (September-October, 2013) "Enhancing File Security by Integrating Steganography Technique in Linux Kernel" Global journal of Engineering,Design & Technology G.J. E.D.T., Vol. 2(5): Page No:9-14 ISSN: 2319 – 7293

[25] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006, pp. 89–98.

[26] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM pp. 195–203.

[27] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Security and Privacy, 2007. SP'07. IEEE Symposium conference on Computer and communications security. ACM, 2007, on. IEEE, 2007, pp. 321–334.

[28] L. Cheung and C. Newport, "Provably secure ciphertext policy abe," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 456–465.
[29] Jegadeesan,R., Sankar Ram October -2013 "ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS" International Journal of Asia Pacific Journal of Research Ph.D Research Scholar 1, Supervisor2, VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

[30] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography PKC 2011. Springer, 2011, pp. 53– 70.

[31] J. Herranz, F. Laguillaumie, and C. R`afols, "Constant size ciphertexts in threshold attribute-based encryption," in Public Key Cryptography–PKC 2010. Springer, 2010, pp. 19–34.

[32] N. Attrapadung, B. Libert, and E. De Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in Public Key Cryptography–PKC 2011. Springer, 2011, pp. 90–108.

[33] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 463–474.

[34] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained twofactor access control for web-based cloud computing services," IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 484–497, 2016.

[35] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 417–426.
[36] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," in Pairing-Based Cryptography–Pairing 2009. Springer, 2009, pp. 248–265
[36],"Attribute-based encryption supporting direct/indirect revocation modes," in Cryptography and Coding. Springer, 2009, pp. 278–300