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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Crypto-Graphical Approach for Secured Data Sharing in Cloud Storage

Dipak S. Kharpas[1], Yogesh S. Khandave[1], Omkar M. Dani[1], Sandesh D. Godase[1],

Bhagyashree Dhakulkar[2]

Dept. of Computer Engineering, SPPU, Pune University, Maharashtra, India[1]

Asst. Professor, Dr.D.Y.Patil School of Engineering Technology, Savitribai Phule Pune University, Mahrashtra, India[2]

ABSTRACT: Data sharing is an important functionality in cloud storage. In this paper, we show how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems that produce constant-size cipher-texts such that efficient delegation of decryption rights for any set of cipher-textsare possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher-text set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in smart card with very limited secure storage. We provide formal security analysis of our schemes in the standard model. We also describe other application of our schemes. In particular, our schemes give the first public-key patient-controlled encryption for flexible hierarchy, which was yet to be known.

KEYWORDS: AES, DES, HIBE, NIPE, Cloud, Encryption, Decryption, KAC.

I. INTRODUCTION

Cloud storage is gaining popularity recently. In enterprise settings, we see the rise in demand for data outsourcing, which assists in the strategic management of corporate data. It is also used as a core technology behind many online services for personal applications. Nowadays, it is easy to apply for free accounts for email, photo album, file sharing and/or remote access, with storage size more than 25GB (or a few dollars for more than 1TB). Together with the current wireless technology, users can access almost all of their files and emails by mobile phone in any corner of the world.

Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data. Ina shared-tenancy cloud computing environment, things become even worse. Data from different clients can be hosted on separate virtual machines (VMs) but reside on a single physical machine. Data in a target VM could be stolen by instantiating another VM co-resident with the target one. Regarding availability of files, there are a series of cryptographic schemes which go as far as allowing a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data owners anonymity.

Likewise, cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality. Acryptographic solution, with proven security relied on number-theoretic assumptions is more desirable, whenever the user is not perfectly happy with trusting the security of the VM or the honesty of the technical staff. These users are motivated to encrypt their data with their own keys before uploading them to the server.

Data sharing is an important functionality in cloud storage. For example, bloggers can let their friends viewa subset of their private pictures; an enterprise may grant her employees access to a portion of sensitive data. The challenging problem is how to effectively share encrypted data. Of course users can download the encrypted data from the storage, decrypt them, then send them to others for sharing, but it loses the value of cloud storage. Users should be able to

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

delegate the access rights of the sharing data to others so that they can access these data from the server directly. However, finding anefficient and secure way to share partial data in cloud storage is not trivial.

Assume that Alice puts all her private photos onDropbox, and she does not want to expose her photos toeveryone. Due to various data leakage possibility Alice cannot feel relieved by just relying on the privacy protection mechanisms provided by Dropbox, so she encrypts all the photos using her own keys before uploading. One day, Alice's friend, Bob, asks her to share the photos taken over all these years which Bob appeared in. Alice can then use the share function of Dropbox, but the problem now is how to delegate the decryption rights for these photos to Bob. A possible option Alice can choose is to securely send Bob the secret keys involved. Naturally, there are two extreme ways for her under the traditional encryption paradigm: Alice encrypts all files with a single encryption key and gives Bob the corresponding secret key directly. Alice encrypts files with distinct keys and sends Bob the corresponding secret keys

II. PROBLEM STATEMENT

Problem definition is to design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the cipher-texts (produced by the encryption scheme) is decrypt table by a constant-size decryption key (generated by the owner of the master-secret key).

III. LITERATURE SURVEY

A. Hierarchical Identity Based Encryption with Constant Size Cipher-text

We present a Hierarchical Identity Based Encryption (HIBE) system where the cipher-text consists of just three group elements and decryption requires only two bilinear map computations, regardless of the hierarchy depth. Encryption is as efficient as in other HIBE systems. We prove that the scheme is selective-ID secure in the standard model and fully secure in the random oracle model. Our system has a number of applications: it gives very efficient forward secure public key and identity based cryptosystems (with short cipher-texts), it converts the NNL broadcast encryption system into an efficient public key broadcast system, and it provides an efficient mechanism for encrypting to the future. The system also supports limited delegation where users can be given restricted private keys that only allow delegation to bounded depth. The HIBE system can be modified to support sub linear size private keys at the cost of some cipher-text expansion.

B. Collusion Resistant Broadcast Encryption with Short Cipher-texts and Private Keys

We describe two new public key broadcast encryption systems for stateless receivers. Both systems are fully secure against any number of colluders. In our first construction both cipher-texts and private keys are of constant size (only two group elements), for any subset of receivers. The public key size in this system is linear in the total number of receivers. Our second system is a generalization of the first that provides a trade-off between cipher-text size and public key size. For example, we achieve a collusion resistant broadcast system for n users where both cipher-texts and public keys are of size $O(\sqrt{n})$ for any subset of receivers. We discuss several applications of these systems.

C. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage.

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called *atomic proxy re-encryption*, in which a semi-trusted proxy converts a cipher-text for Alice into a cipher-text for Bob *without* seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Following recent work of Dodisand Ivan, we present new re-encryption schemes that realize a stronger notion of security, and we demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of our experimental file system demonstrate that proxy re-encryption can work effectively in practice.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

D. Achieving Short Cipher-texts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption

We present two *non-zero inner-product* encryption (NIPE) schemes that are *adaptively secure* under a standard assumption, the decisional linear (DLIN) assumption, in the standard model. One of the proposed NIPE schemes features *constant-size cipher-texts* and the other features *constant-size secret-keys*. Our NIPE schemes imply an identity-based revocation (IBR) system with constant-size cipher-texts or constant-size secret-keys that is adaptively secure under the DLIN assumption. Any previous IBR scheme with constant-size cipher-texts or constant-size secret-keys was *not adaptively secure* in the standard model. This paper also presents two zero inner-product encryption (ZIPE) schemes each of which has constant-size cipher-texts or constant-size secret-keys and is adaptively secure under the DLIN assumption in the standard model. They imply an identity-based broadcast encryption (IBBE) system with constant-size cipher-texts or constant-size secret-keys that is adaptively secure under the DLIN assumption.

IV. EXISTING SYSTEM

Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data. In a shared-tenancy cloud computing environment, things become even worse.Regarding availability of files, there are a series of cryptographic schemes which go as far as allowing a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data owners anonymity. Likewise, cloud users probably will not hold the strong belief that the cloud serveries doing a good job in terms of confidentiality.

A cryptographic solution, with proven security relied on number-theoretic assumptions is more desirable, whenever the user is not perfectly happy with trusting the security of the VM or the honesty of the technical staff.

- The costs and complexities involved generally increase with the number of the decryption keys to be shared.
- The encryption key and decryption key are different in public key encryption.
- There is no system to generate unique key to access multiple files.
- The costs and complexities involved generally increase with the number of the decryption keys to be shared.
- The encryption key and decryption key are different in public key encryption.
- Identity based encryption instead attributes based encryption.

V. PRAPOSED SYSTEM

How to make a decryption key more powerful in the sense that it allows decryption of multiple cipher-texts, without increasing its size. Specifically, our problem statement is “To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the cipher-texts (produced by the encryption scheme) is decryptable by a constant-size decryption key (generated by the owner of the master-secret key).” We solve this problem by introducing a special type of public-key encryption which we call key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of cipher-text called class. That means the cipher-texts are further categorized into different classes. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of cipher-text classes.

- The extracted key have can be an aggregate key which is as compact as a secret key for a single class.
- The delegation of decryption can be efficiently implemented with the aggregate key.
- System developed for generating an unique key for accessing multiple files in the aggregate server.
- The extracted key can be an aggregate key which is as compact as a secret key for accessing multiple files.
- There will be ABE (Attribute Based Encryption) to store file in the cloud server.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

VI. SYSTEM ARCHITECTURE

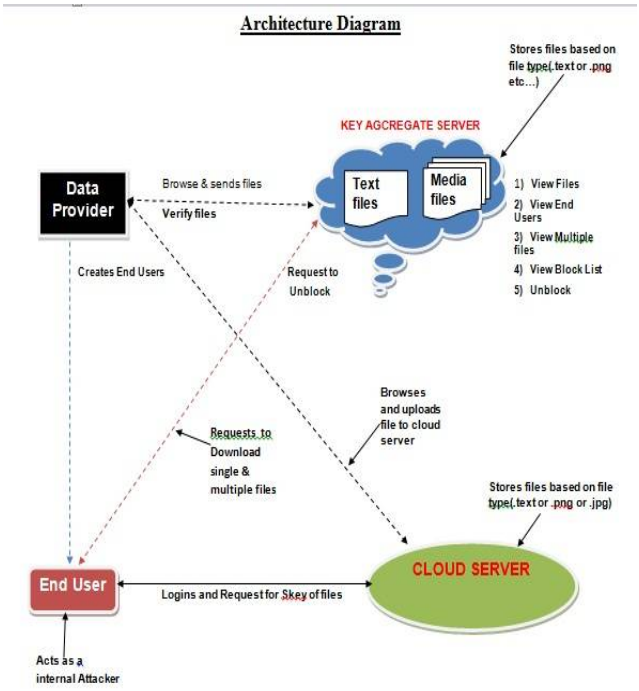

Fig: 1. System Architecture

A. SETUP PHASE

- The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

B. ENCRYPT PHASE

- Encrypt(PK,M, A). The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a cipher-texts CT such that only a user that possesses a set of attributes that satisfy the access structure will be able to decrypt the message. We will assume that the cipher-texts implicitly contains A.

C. KEY GEN PHASE

- Key Generation(MK,S). The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

D. DECRYPT PHASE

- Decrypt(PK, CT, SK). The decryption algorithm takes as input the public parameters PK, a cipher-texts CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the cipher-texts and return a message M.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

VII. RESULT

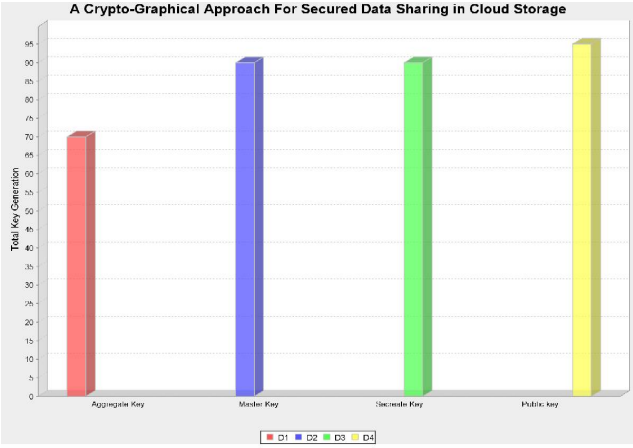

Fig : 2. Result

VIII. EXPERIMENT RESULT

- In this the System consist of technology like JAVA,HTML,CSS, and JavaScript. For back end MySQL is used. Also, To used real time cloud called as Dropbox. Hence before experimental set up Software like Eclipse, Tomcat is projected to be installed on server. User should have basic windows family, good browser to view the results. Un-Supervised dataset is used for testing.

IX. CONCLUSION

- How to protect users' data privacy is a central question of cloud storage. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. In this article, we consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different cipher-texts classes in cloud storage. No matter which one among the power set of classes, the delegate can always get an aggregate key of constant size. Our approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges. A limitation in our work is the predefined bound of the number of maximum cipher text classes. In cloud storage, the number of cipher-texts usually grows rapidly. So we have to reserve enough cipher-texts classes for the future extension. Otherwise, we need to expand the public-key as we described in this system.

REFERENCES

[1] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M.Yiu, "SPICE Simple Privacy-Preserving Identity-Management for Cloud Environment,"in Applied Cryptography and Network Security – ACNS2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.
[2] L. Hardesty, "Secure computers aren't so secure," MIT press, 2009,http://www.physorg.com/news176107396.html.
[3] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362–375, 2013.
[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conferenceon Distributed Computing Systems - ICDCS 2013. IEEE, 2013.
[5] MD AsifMushtaque , Harsh Dhiman , ShahnawazHussain , ShivangiMaheshwari "Evaluation of DES, TDES, AES, Blowfish and Two fish Encryption Algorithm: Based on Space Complexity," International

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

[6] DiaaSalama Abdul. Elminaam1, Hatem Mohamed Abdul Kader2 and Mohie Mohamed Hadhoud3"Performance Evaluation of Symmetric EncryptionAlgorithms"
[7] NarenderTyagi Anita Ganpati "International Journal of Advanced Research in Computer Science and Software Engineering"
[8] Mrs. Komal Kate, Prof. S. D. Potdukhe" Data sharing in cloud storage with key-aggregate cryposystem."
[9] Ramakrishna Jadhav1 ,Snehal Nargundi2 "a review on key-aggregate cryptosystem for scalable data sharing in cloud storage"ijret: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308
[10] S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng,"Dynamic Secure Cloud Storage with Provenance," in Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.
[11] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," inProceedings of Advances in Cryptology - EUROCRYPT '03, ser. LNCS,vol. 2656. Springer, 2003, pp. 416–432.
[12] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamicand Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.
[13] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.
[14] F. Guo, Y. Mu, Z. Chen, and L.Xu, "Multi-Identity Single-Key Decryption without Random Oracles," in Proceedings of Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990.Springer, 2007, pp. 384–398.
[15] 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 (CCS '06). ACM, 2006, pp. 89–98.