IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Key Aggregate Cryptosystem for Scalable Data Distribution in Cloud Storage

D. Suguna Kumari[1], B. Rajesh[2], P. Vamshi Krishna[3], Y. Ramakrishna[4]

Dept of Computer Science & Engineering in GRIET, Hyderabad, TLG, India[1]

Dept of Computer Science & Engineering in MTIET, Palamaner, AP, India[2]

Dept of Computer Science & Engineering in KMIT, Hyderabad, TLG, India[3]

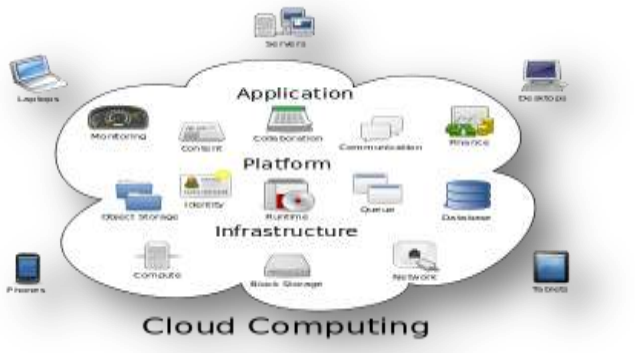
Dept of Computer Science & Engineering in HITS, Hyderabad, TLG, India[4]

Abstract: Data sharing being important functionality in cloud storage implements how to securely, efficiently, and flexibly share data with others. The public-key cryptosystems produce constant size cipher texts that efficiently delegate the decryption rights for any set of cipher texts. The significance is that one can total any arrangement of mystery keys and make them as conservative as a solitary key, yet including the energy of all the keys being accumulated. The mystery key holder can discharge a consistent size total key for adaptable decisions of figure content set in distributed storage; however the other encoded documents outside the set stay secret. The total key can be advantageously sent to others or be put away in a brilliant card with exceptionally restricted secure stockpiling.

Keywords: Cloud storage, public key encryption, cryptosystem, key aggregate encryption, and key aggregate cryptosystem.

I. INTRODUCTION

Cloud computing is the use of computing resources that are delivered as a service over a network. The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.
The objective of distributed computing is to apply conventional supercomputing, or superior processing power, regularly utilized by military and research offices, to perform several trillions of calculations for each second, in purchaser situated applications, for example, monetary portfolios, to convey customized data, to give information stockpiling or to control huge, immersive PC amusements. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.



Characteristics and Services Models:
The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:
On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a feeling of area freedom in that the client by and large has no control or information over the correct area of the gave assets however might have the capacity to indicate area at a more elevated amount of reflection.
Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service. Its flexible and cost optimizing characteristic motivates the end user as well as enterprises to store the data on cloud. The insider attack is one of security concern which's needs to be focused. Cloud Service provider need to make sure whether audits are held for users who have physical access to the server. As cloud service provider stores the data of different users on same server it is possible that user's private data is leaked to others. The public auditing system of data storage security in cloud computing provides a privacy-preserving auditing protocol. A new way for public-key encryption is used called as key aggregate cryptosystem. The encryption is done through an identifier of Cipher text known as class, with public key. The classes are formed by classifying the cipher text. The key owner has the master secret key which is helpful for extracting secret key. So in above scenario now the Alice can send an aggregate key to bob through an email and the encrypted data is downloaded from drop box through the aggregate key.

II. RELATED WORK

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 owner's anonymity. Likewise, cloud users probably will not hold the strong belief that the cloud server is 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.

Disadvantages of Existing System:
- 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.

Proposed System:
We study 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 decrypt table by a constant-size decryption 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.

Advantages of Proposed System:
- 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.

III. IMPLEMENTATION

The aggregation cryptosystem consists of efficient Key Aggregate Cryptosystem algorithm. The data owner set up the general public parameter using Setup and creates a public/private (master) key and combines using KeyGen. The secret

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

file is encrypted utilizing CP-ABE algorithm. The information owner will make use the master-secret to come up with aggregate decipher key for a collection of data files. The created keys might be passed to delegates safely. At last, any client with total key will unscramble information record and download it. An accepted utilization of KAC is information sharing. The key collection property is particularly helpful when we anticipate that assignment will be effective and adaptable. The KAC plans empower a substance supplier to share information in a private and specific route, with a settled and little figure content extension, by circulating to each approved client a solitary and little total key. We think about how to make a decoding key all the more intense as in it permits unscrambling of various figure writings, without expanding its size. In KAC, clients encode a message under an open key, as well as under an identifier of figure content called class. That implies the figure writings are additionally classified into various classes. The key proprietor holds a mystery called ace mystery key, which can be utilized to extricate mystery keys for various classes. All the more imperatively, the separated key have can be a total key which is as smaller as a mystery key for a solitary class, however totals the energy of numerous such keys, i.e., the unscrambling power for any subset of figure content classes. Information partaking in distributed storage utilizing KAC. Assume Alice needs to share her information m1, m2,...., mn on the server. The framework parameter and open key pk can be made open and ace mystery key msk ought to be kept mystery by Alice. Anyone can then encrypt each mi by Ci = Encrypt (pk, i, mi). The encrypted data are uploaded to the server. With parameter and pk, people who cooperate with Alice can update Alice's data on the server. Once Alice is willing to share a set S of her data with a friend Bob, she can compute the aggregate key KS for Bob by performing Extract (msk, S). Since KS is just a constant size key, it is easy to be sent to Bob through a secure e-mail. After obtaining the aggregate key, Bob can download the data he is authorized to access.

Modules:
1. Data Owner(Alice)
2. Network Storage
3. Aggregate Key Transfer
4. User(Bob)

Data Owner (Alice):
In this module we executed by the data owner to setup an account on an entrusted server. On input a security level parameter 1^{λ} and the number of cipher text class's n, it outputs the public system parameter param, which is omitted from the input of the other algorithms for brevity.

Network Storage (Drop box):
With our solution, Alice can simply send Bob a single aggregate key via a secure e-mail. Bob can download the encrypted photos from Alice's drop box space and then use this aggregate key to decrypt these encrypted photos. In this Network Storage is entrusted third party server or drop box.

Aggregate Key Transfer:
A key-aggregate encryption scheme consists of five polynomial-time algorithms as follows. The data owner establishes the public system parameter via Setup and generates a public/master-secret key pair via KeyGen. Messages can be encrypted via Encrypt by anyone who also decides what cipher text class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of cipher text classes via Extract. The generated keys can be passed to delegates securely finally; any user with an aggregate key can decrypt any cipher text provided that the cipher text's class is contained in the aggregate key via Decrypt

User (Bob):
The generated keys can be passed to delegates securely (via secure e-mails or secure devices) finally; any user with an aggregate key can decrypt any cipher text provided that the cipher text's class is contained in the aggregate key via Decrypt.

IV. RESULTS

Fig: Screen Shot For Home Page

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Fig: Screen Shot For Admin Login

Fig: Screen Shot to Upload Files

Fig: Screen Shot to Enter Public Key

Fig: Screen Shot to Enter Private Key

Fig: Screen Shot of Private Key

Fig: Screen Shot for Encrypted Data

Fig: Screen Shot of Uploaded Files Details

Fig: Screen Shot of Keys to be shared

DOI10.17148/IJARCCE.2017.6826

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Fig: Screen Shot of Entire Files Details

Fig: Screen Shot Of User Registration

Fig: Screen Shot of User Login

Fig: Screen Shot to Download Files

Fig: Screen Shot of Keys got in the Mail

Fig: Screen shot of files Location after Downloading

V. CONCLUSIONAND FUTURE ENHANCEMENT

The most effective method to secure client's information protection is a focal inquiry of distributed storage. With more numerical gadgets, cryptographic plans are getting more adaptable and often incorporate different keys for a single application. We consider how to "pack" riddle enters with no attempt at being subtle key cryptosystems which support task of secret keys for different figure content classes in appropriated capacity. Notwithstanding which one among the power set of classes, the delegate can basically get an aggregate key of steady size.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

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 text classes for the future extension.

Although the parameter can be downloaded with cipher texts, it would be better if its size is independent of the maximum number of cipher text classes. On the other hand, when one carries the delegated keys around in a mobile device without using special trusted hardware, the key is prompt to leakage, designing a leakage-resilient cryptosystem yet allows efficient and flexible key delegation is also an interesting direction.

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," Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS), vol. 7341, pp. 526-543, 2012.
[2] L. Hardesty, Secure Computers Aren't so secure. MIT press, http://www.physorg.com/news176107396.html, 2009.
[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, Feb. 2013.
[4] B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems (ICDCS), 2013.
[5] S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng, "Dynamic Secure Cloud Storage with Provenance," Cryptography and Security, pp. 442-464, Springer, 2012.
[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '03), pp. 416-432, 2003.
[7] M.J. Atallah, M. Blanton, N. Fazio, and K.B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Trans. Information and System Security, vol. 12, no. 3, pp. 18:1-18:43, 2009.
[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.
[9] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," Proc. Information Security and Cryptology (Inscrypt '07), vol. 4990, pp. 384-398, 2007.
[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.
[11] S.G. Akl and P.D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Trans. Computer Systems, vol. 1, no. 3, pp. 239-248, 1983.
[12] G.C. Chick and S.E. Tavares, "Flexible Access Control with Master Keys," Proc. Advances in Cryptology (CRYPTO '89), vol. 435, pp. 316-322, 1989.
[13] W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Trans. Knowledge and Data Eng., vol. 14, no. 1, pp. 182-188, Jan./Feb. 2002.
[14] G. Ateniese, A.D. Santis, A.L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," J. Cryptology, vol. 25, no. 2, pp. 243-270, 2012.
[15] R.S. Sandhu, "Cryptographic Implementation of a Tree Hierarchy for Access Control," Information Processing Letters, vol. 27, no. 2, pp. 95-98, 1988.
[16] Y. Sun and K.J.R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," Proc. IEEE INFOCOM '04, 2004.
[17] Q. Zhang and Y. Wang, "A Centralized Key Management Scheme for Hierarchical Access Control," Proc. IEEE Global Telecomm. Conf. (GLOBECOM '04), pp. 2067-2071, 2004.
[18] J. Benaloh, "Key Compression and Its Application to Digital Fingerprinting," technical report, Microsoft Research, 2009.
[19] B. Alomair and R. Poovendran, "Information Theoretically Secure Encryption with Almost Free Authentication," J. Universal Computer Science, vol. 15, no. 15, pp. 2937-2956, 2009.
[20] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Advances in Cryptology (CRYPTO '01), vol. 2139, pp. 213-229, 2001.
[21] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), vol. 3494, pp. 457-473, 2005.
[22] S.S.M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions," Proc. ACM Conf. Computer and Comm. Security, pp. 152-161, 2010.
[23] F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key," Proc. Pairing-Based Cryptography Conf. (Pairing '07), vol. 4575, pp. 392-406, 2007.
[24] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130.

BIOGRAPHIES

Mrs. D. Suguna Kumari, Post Graduated in Computer Science and Engineering (M.Tech) From **ANU, Guntur in Jul - 2010** and Graduated in Information Technology (B.Tech) from **Hi-Point College of Engineering and Technology, JNTUH in 2006**. She is working as an Assistant Professor in Department of Computer Science and Engineering in **Gokaraju Rangaraju Institute of Engineering and Technology**, R.R Dist, TLG and India. She has 10+ years of Teaching Experience. Her Research Interest includes networking, mining, and security.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Mr. B.RAJESH, Post Graduated in Computer Science & Engineering (**M.Tech**) From **ANNA University**, Chennai in 2015 and Graduated in Computer Science & Engineering (B.Tech) form JNTU, Ananthapur, 2013. He is working as an Assistant Professor in Department of Computer Science & Engineering in **Mother Theresa Institute of Engineering and Technology**, Palamaner, and Chittoor. He has 2+ years of Teaching Experience. His Research Interests Include Network Security, Cloud Computing & Data Warehousing and Data Mining.

Mr. P.VAMSHI KRISHNA, Post Graduated in Computer Science & Engineering (**M.Tech**) From **SVS group of Institutions** affliated to JNT University, Hyderabad in 2015 and Graduated in Computer Science & engineering (**B.Tech**) form **Balaji Institute of Technology and Science** affliated JNTU, Hyderabad, 2012. He is presently working as Assistant Professor in **Keshav Memorial Institute of Technology**, narayanaguda, Hyderabad.. His Research Interests Include mainly Cloud Computing & Data Warehousing and Data Mining, Network Security. He is a member of CSI.

Mr. Y. Ramakrishna, Pursuing Ph.D in Computer Science from Rayalaseema University, His completed Post Graduated in Computer Science & Engineering (**M.Tech**) From, **HMITS COE**, JNTUH in 2013 and Post Graduated in Master of Computer Applications(MCA) from **Dr. N.N. College of Engineering**, Anna University in 2005. He is working as an Associate Professor in Department of Computer Science & Engineering in **HITS, Hyderabad**. He has 9+ years of Teaching Experience. His Research Interests Include Image Processing, Network Security, Cloud Computing & Data Warehousing and Data Mining.