SECURE DATA SHARING IN CLOUD STORAGE USING PUBLIC-KEY CRYPTOSYSTEMS

M.Sundaresan, Prof. Jesila Mol.J

MCA final Year Sathyabama University
Asst Prof MCA, MTech. Sathyabama University
Department of Computer Application, Sathyabama University
Chennai, India.

ABSTRACT

Cloud computing refers to applications and services provides over the web. These services square measure offered from information centers everywhere the world. That conjointly square measure said because the cloud. In existing system the cloud storage show to securely, efficiently and flexibility share data with others. In existing system public-key cryptosystem produce that constant size of cipher text, Such that efficient delegation of decryption right for any set of cipher text are possible. But in the existing system limited number of public-key is used. In proposed system, need to overcome the limited number of public-key. Proposed system expand the bit level of public-key to access the number of users to share efficiently in cloud storage using the method called leakage-resilient cryptosystem.

Keywords: *Cloud Computing, Key-aggregate Encoding, Information sharing, leakage resilient cryptosystem.*

INTRODUCTION

The use of cloud computing has enhanced speedily in several organizations. Cloud-based services include Software-as-a- service (SaaS) and Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud computing offers various facilities for Information storage and information sharing. User generally deploys their information over cloud storage in terms of GB or TB. so cloud computing is advantageous in terms of low price and accessibility of knowledge. Making certain the safety of cloud storage could be a major think about the cloud computing atmosphere, as someday users store sensitive info with cloud storage. Where as information sharing in cloud computing atmosphere, information from totally different users will be keep on separate virtual machines (VMs) however belongs to one physical machine. However information during a target VM can be taken by instantiating another VM on same physical machine. so considering ancient ways in which of knowledge privacy, some depends on the server to enforce the access management when authentication [3] or some permits a third-party auditor to ascertain the supply of files on behalf of the information owner while not unseaworthy the information [2]. However cloud user cannot totally depend upon cloud server for his or her information security and confidentiality purpose. so users square measure motivated to write in code their information with own keys so providing access to solely desired Receivers. Allow us to think about AN example; user A uploads a group of photos over cloud. However he doesn't wish to share of these photos with everybody. Therefore he have to be compelled to place some security constraints. With the out there cloud security services user A isn't happy. Therefore he encrypts his photos victimization his own keys before uploading. Currently once user B asks user A to share his photos, user A can send him one constant size cryptography key via secure channel. With this cryptography key, user B is allowed to decipher solely those photos that square measure permissible by user A. so here we are able to offer drawback statement as, "Design a public key secret writing theme in such how that any set of the cipher text is decryptable by a continuing size cryptography key." the answer for this drawback is provided victimization Key combination Cryptosystem (KAC) [1]. With this answer, user A will merely send user B one combination key via a secure e-mail. Then user B will transfer the encrypted photos from A's cloud space for storing and so use this combination key to decipher these encrypted photos. The sizes of cipher text, public-key, master-secret key, and combination key during this KAC schemes square measure all of constant size.

RELATED WORK

In this section basic KAC theme is compared with various potential results on sharing in secure cloud storage

[1] S.G. Akl and P.D. Taylor are introduced, Cryptographic Keys for a Predefined Hierarchy cryptanalytic key assignment schemes works on the thought of minimize the expense in storing and maintaining secret keys for general Cryptographic use by employing a tree structure [1]. By victimization hierarchical tree structure, a key for a given branch are going to be accustomed derive the keys of its descendant nodes. This can solve the matter part if one intends to share all files underneath a precise branch within the hierarchy that instead means the amount of keys will increase with the amount of branches. Therefore it's tough to form a hierarchy that may save the amount of total keys to be granted for all people at the same time.

[2] J. Benaloh is proposed the Compact Key in Symmetric-Key secret writing this technique is employed to get a secret worth rather than a try of public/ secret keys [2]. It's designed for the symmetric-key setting during which the write in coder gets the corresponding secret keys to encrypt information. so it's unclear the way to apply this idea for public key secret writing theme.

[3] F. Guo, Y. Mu, and Z. Chen are proposed Compact Key in Identity-Based secret writing (IBE) during this secret writing, there's a sure party referred to as personal key generator in IBE that holds a master-secret key and offers a secret key to every user with regard to the user identity. The write in code or will take the general public parameter and a user identity to encrypt a message [3]. The receiver will decipher this cipher text by his secret key. Some tried to make IBE with key aggregation. However their key-aggregation comes at the expense of O(n) sizes for

each cipher text and therefore the public parameter, wherever n is that the range of secret keys. This greatly will increase the prices to store and transmit cipher text.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters are introduced the Attribute-based secret writing (ABE) This theme maintains every cipher text to be related to AN attribute, and therefore the master-secret key holder will extract a secret key for a policy of those attributes so a cipher text will be decrypted by this key. however the dimensions of the key typically will increase linearly with the amount of attributes it encompasses, or the cipher text-size isn't constant [4].

S.S.M. Chow, Y. Dodis, S.S.M. Chow and] J. Benaloh et all published based on this concepts like Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions[5], Privacy-Preserving Public Auditing for Secure Cloud Storage[7], SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment[8] and Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records[9].

PROPOSED SYSTEM

Although KAC provides constant-size keys , once one carries the delegated keys during a mobile device while not victimization special sure hardware, the secret's prompt to outflow, so planning a leakage-resilient cryptosystem [9] is that the planned work for the system. Leakage-resilient cryptosystem tries to tackle attacks over its information. Leakage-resilient cryptosystem maintain their security even though attacker learn some partial data of their knowledge.

METHODOLOGIES

Various Algorithms square measure used for implementing the planned system. every section of this project involves one rule. initial section is uses public-key Cryptographic rule (AES) for encrypting files at file owner's want. In second section combination Secret secret's generated. combination secret key generation is completed in four steps , wherever several Cryptographic schemes square measure applied.

1 AES Algorithm

The AES encoding and cryptography processes for a 128-bit plain text block. The AES formula specifies 3 encoding modes: 128-bit, 192-bit, and 256-bit. every cipher mode has a corresponding variety of rounds Nr supported key length of Nk words. The state block size, termed Nb, is constant for all encoding modes. This 128-bit block is termed the state. every state is comprised of four words. A word is afterward outlined as four bytes. Table one shows the attainable key/state block/round combos.

Encoding method: The encoding and cryptography method consists of variety of various transformations applied consecutively over the information block bits, in an exceedingly mounted variety of iterations, referred to as rounds. the quantity of rounds depends on the length of the key used for the encoding method. For key length of 128 bits, the quantity of iteration needed are10. (Nr = 10). every of the primary Nr-1 rounds consists of four transformations: Sub Bytes(), Shift Rows(), combine Columns() &amp; Add spherical Key().

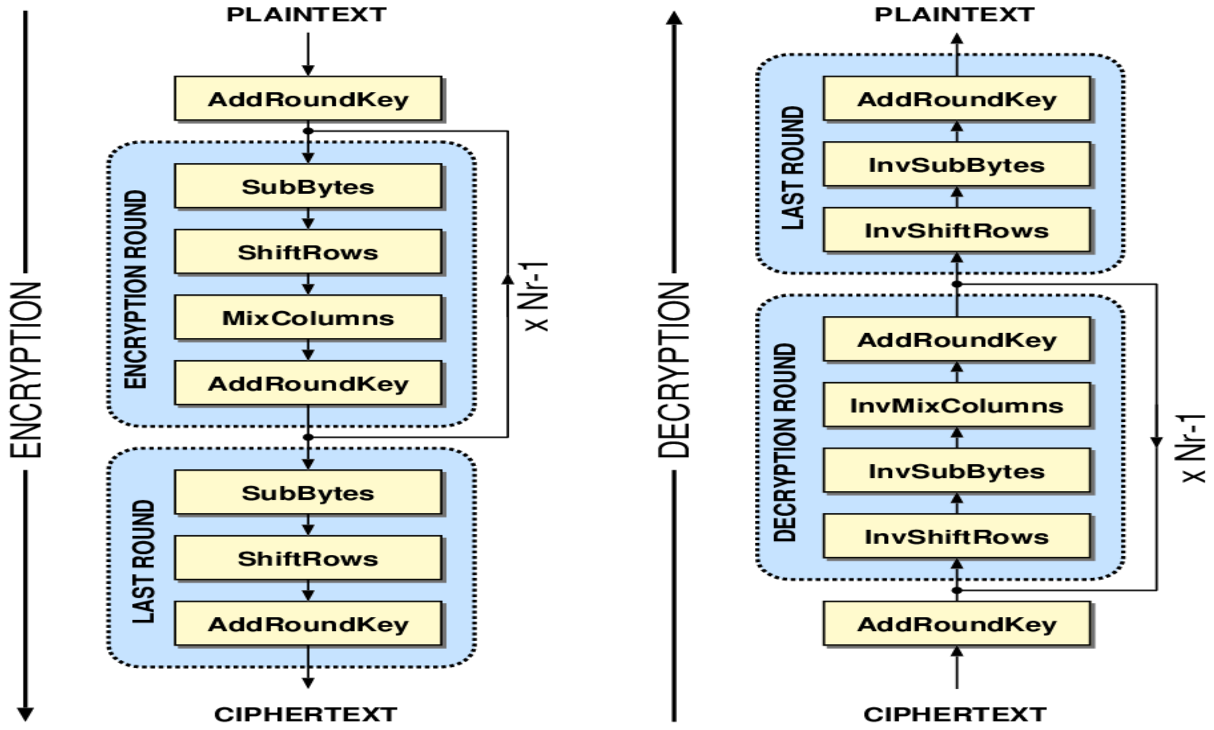

Fig 1: AES Encryption and Decryption Flow

KEY-AGGREGATE CRYPTOSYSTEM

A key-aggregate secret writing system essentially includes 5 algorithmic steps as follows- the information owner establishes the general public system parameter by victimization Setup and generates a public/master-secret key try by victimization Key Gen. Messages will be encrypted victimization write in code by anyone UN agency additionally decides what cipher text category is related to the plaintext message to be encrypted. The data owner will use the master-secret to get AN combination cryptography key for a set of cipher text categories by Extract. The generated keys will be passed to Receivers firmly via secure e-mails. Finally, Any user with an combination key will decipher any cipher text as long as the cipher texts category is contained within the combination key via

Decrypt: Setup(1? , n): information owner executes Setup to form AN account on AN untrusted server. With input as security level parameter 1? and therefore the range of cipher text categories n ,it outputs the general public system parameter pram.

KeyGen: Information owner executes Key Gen to at random generate a public/master-secret key try (pk ,msk)

Encrypt(pk, i, m): Anyone will execute this step UN agency needs to write in code information with input a public-key pk, AN index i denoting the cipher text category, and a message m, that outputs a cipher text C.

Extract(msk, S): Executed by the information owner to relinquishing the decrypting power for a precise set of cipher text categories to a Receiver . On input the master-secret key msk and a group S of indices reminiscent of totally different categories, it outputs the combination key for set S denoted by KS.

Decrypt(Ks, S, i, B): Executed by a Receiver UN agency received AN combination key KS generated by Extract. On input KS, the set S, AN index i denoting the encrypted text class the cipher text B belongs to, and B, it outputs the decrypted result m if i ? S.

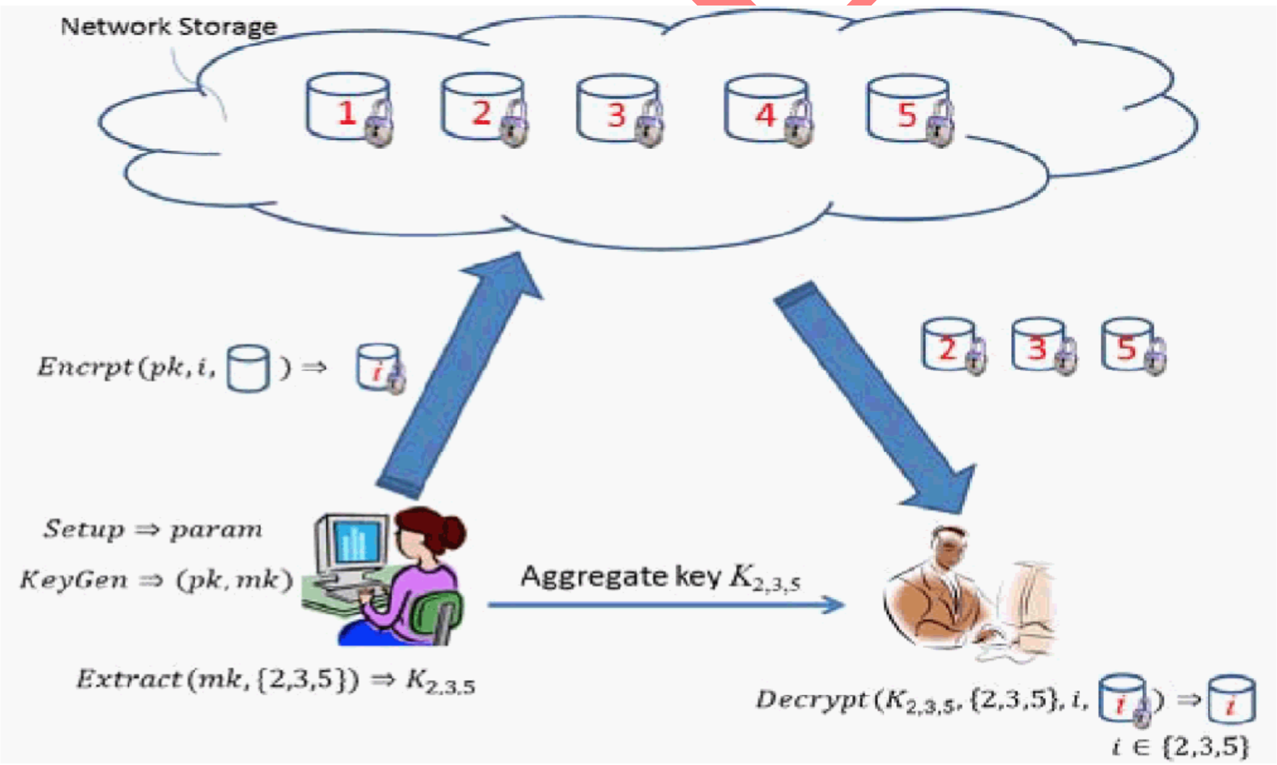
Network Storage
1
2
3
4
5
Encrpt(pk, i,) ⇒ i
2
3
5
Setup ⇒ param
KeyGen ⇒ (pk, mk)
Aggregate key $K_{2,3,5}$
Extract(mk, {2,3,5}) ⇒ $K_{2,3,5}$
Decrypt($K_{2,3,5}$, {2,3,5}, i, i) ⇒ i
i ∈ {2,3,5}

Fig 2: Using KAC for information sharing in cloud storage

2 Aggregate Secret Key Generation

The data owner produces public/master-secret key try during this section. combination key[1] generation section is split in 3 steps. Messages will be encrypted victimization Encrypt( ) operate by anyone UN agency additionally decides that cipher text category is related to the plain text message. the information owner will use master-secret to get AN combination cryptography key for cipher text categories victimization operate Extract( )

Encrypt(PK,i, m) : within the initial section public key PK is generated. On giving input a public key pk, AN index i(increment counter), that denotes the cipher text category, and a message m, it outputs a cipher text C.

Extract(Msk, S): information owner extracts the combination secret key. Here, On giving input as master-secret key Msk and a group of indices S that corresponds to totally different categories, it outputs the combination key KS for set S.

Decrypt(Ks, S, i, B) : cryptography of combination secret secret's performed by one UN agency received AN combination key KS generated in extract section. On input KS, the set S, Associate degree index i denoting the encrypted text class B belongs to, and B, it outputs the decrypted result m.

CONCLUSION

Thus information privacy and security is maintained by coming up with a public key cryptosystem known as Key Aggregate Cryptosystem (KAC). This KAC helps user to share their information part over cloud with constant size key combine of public-master keys and additionally receiver will decode this information with single constant size aggregate key. This helps Patient-Controlled encoding (PCE) system. There area unit some limitation to the present system like predefined sure of the quantity of most cipher text categories and system is prompt to outflow of key.

REFERENCES

[1] 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.

[2] J. Benaloh, “Key Compression and Its Application to Digital Fingerprinting,” technical report, Microsoft Research, 2009.

[3] F. Guo, Y. Mu, and Z. Chen, “Identity-Based Encryption: How to Decrypt Multiple Cipher texts Using a Single Decryption Key,” Proc. Pairing-Based Cryptography Conf. (Pairing ’07), vol. 4575,pp. 392-406, 2007.

[4] 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.

[5] 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.

[6] [Cheng Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng,,” Key Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage “,IEEE Transaction on Parellel and Distributed System, vol. 25, no. 2, February 2014 .

[7] 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.

[8] 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.

[9] 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.

AUTHOR

Sundaresan.M, MCA final Year student, Sathyabama University Chennai.

Co-author**:** Jesila Mol.J MCA, MTech, Asst Prof, Department of computer Application, Sathyabama University Chennai.