Research Article Impact Factor: 4.226 ISSN: 2319-507X
Pratibha R. Raut, IJPRET, 2015; Volume 3 (9): 1790-1797 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

KEY AGGREGATE CRYPTOSYSTEM FOR SCALABLE DATA SHARING IN CLOUD STORAGE

MISS. PRATIBHA R. RAUT, MISS. RESHMA N. SIDDIQUE, MISS. VAISHALI L. CHAVAN, MISS. PALLAVI S. VYAWAHARE, PROF. O. A. JAISINGHANI

Dept. Information technology, IBSS Collage of Engineering, Amravati.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Data sharing is an important functionality in cloud storage, how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible.

Keywords: Cryptography, Efficiently, ,Decryption, Encryption

Corresponding Author: MISS. PRATIBHA R. RAUT

Access Online On:

www.ijpret.com

How to Cite This Article:

Pratibha R. Raut, IJPRET, 2015; Volume 3 (9): 1790-1797

PAPER-QR CODE

INTRODUCTION

Cloud storage is gaining popularity recently. In enterprise settings, we see the rise in demand for data outsourcing, which assists in the strategic executive 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, and file sharing and/or remote access, with storage size more than 25GB.Togetherwith the current wireless technology; users can permit almost all of their files and emails by mobile phone in any area of the world.

In view of data privacy, a long-established way to ensure it is to rely on the server to enforce the access control after authentication, which means any unforeseen privilege growth will expose all data.

In a shared-tenancy cloud computing atmosphere, things become even of inferior quality. Data from different clients can be hosted on separate virtual machines but be inherent in on a single physical machine. Data in a intention VM could be stolen by instantiating another VM co-resident with the aim one.

As regards availability of files, there are a series of cryptographic schemes which go as far as allow a third-party inspector to check the availability, of files on behalf of the data owner without leaking anything about the data devoid of compromise the data owner's ambiguity. Likewise, cloud users perhaps will not hold the strong confidence that the cloud server is doing a good job in terms of confidentiality.

Literature review:

Cloud Computing

Cloud computing is a technology that uses the internet and central distant servers to maintain data applications. Cloud computing is the use of computing property that are delivered as service over a network. The name comes from the use of a cloud-shaped symbol as an abstraction for the multifaceted transportation it contains in a system diagram. Cloud computing entrust remote services with a user's data, software and computation.

Software as a Service:

Users access cloud computing using networked client devices, such as desktop computers, laptops, tablets and smart phones. Some of this devices-cloud client-rely on cloud computing

for all or a mainstream of their applications so as to be in actual fact inadequate without it. In computing client is a system that access service on another computer by some kind Of network

Features of Publically Auditable Service:

Multitenant:

Multitenant achievers to a principal in software architecture where a single instance of the software runs on a server, serving multiple client organization. Militant is contrasted with– instance architecture where detach software instances are set up for different client association With a militant architecture a software application is designed a virtually partition its data and configuration and each client organization works with a customized virtual application instance. Multitenancy is also regarded as one of the critical attributes of cloud computing.

High Return on Investment:

Cloud computing does not have any straight cost. It is completely based on usage. The user is build based on amount of affluence the use this helps the user to track their usage and in the end help to resources they use. This helps the user to track their usage and ultimately help to shrink cost. Cloud computing must provide means to capture, monitor, and control usage information for truthful billing. The information gathering should be transparent and readily available to the customer. This is compulsory to make the customer realize the cost benefits that a cloud computing bring.

Centralized Storage:

The use of central disk storage also makes more efficient use of disk storage. This can cut storage cost, liberation up capital to provide in more reliable, modern storage technologies, such as RAID array which support redundant operation and storage area networks which allow hot-adding of storage without any interruption. Future, it means that losses of disk drivers to mechanical or electrical failure which a large number of disk involved are often both less likely to happen and less likely to cause interruption.

System Implementation:-

System Architecture:

Multiunit application represents a natural evolution from this model, contribution additional customization to a group or user within the same client organization. Sometimes you may be sharing the same resources with another tenant. But of course, this is transparent to the

customer Cloud provides shall responsible the security aspect, ensuring that one tenant won't be able to access others data.

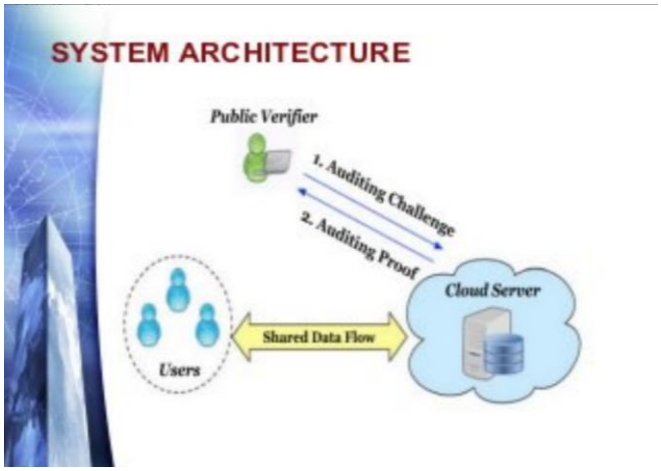

Fig 1. System Architecture

"To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the cipher texts is decrypt able by a constant-size decryption?" We solve this problem by introducing a special type of public-key encryption which we call key-aggregate cryptosystem. 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. 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.

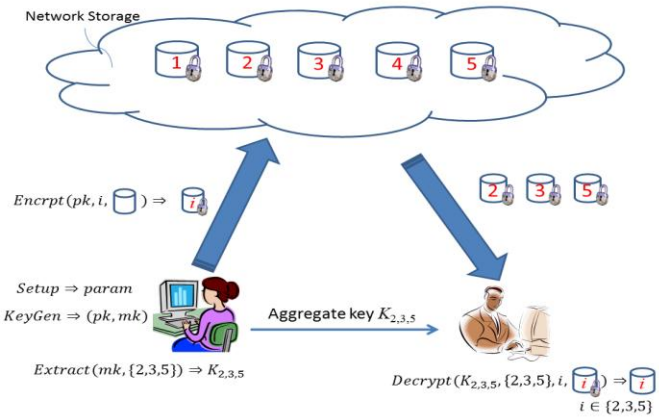

Fig 2. Transmission of the Data in the Encrypted Form

Minimize the expenditure in storing and managing secret keys for general cryptographic use. Utilize a tree structure; a key for a given branch can be used to derive the keys of its descendant nodes. Just granting the parent key implicitly grants all the keys of its descendant nodes. Sandhog proposed a method to generate a tree hierarchy of symmetric keys by using repeated evaluations of pseudorandom function/block-cipher on a fixed secret.

File Transfer and Storage Management:

Encrypted & Decryption:

While uploading users file be encrypted using AES algorithm and get stored on server. Decryption is conversion from cipher text to the plan text.

Secret Key Generation:

At the time of user registration, every user has to decide his/her unique secrets key. This key will be consider as a secrete key of his tall document. At the time of file upload actual secrete key for every document will be automatically generated and stored in database in encrypted format.

Encryption:

In Encryption process the original plain text is converted into the text which is in untidy form and that text is principally known to be as encryption practice.

The conversion of plaint text in to untidy form or the cipher text is known as the encryption.

Key-Aggregate Cryptosystem:

New public-key cryptosystems which produce constant-size cipher texts. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key. In other words, the secret key holder can release a constant-size aggregate key for bendy choices of cipher text.

Identity Encryption Techniques:

Identity based encryption is a type of public key encryption. System will automatically generate identity string of every user using set of different system generated algorithms. At the time of registration every user will get his/her identity key on email. While uploading and downloading documents on cloud, every user have to prove his/her identity using identity key.

Application:

- To keep the data secure from the third party while transferring the data from sender to the receiver
- Most of the times we see in bank ID no which is kept hidden and so on.
- Science in this project it provides the high quality of security.

CONCLUSIONS:

- Cryptographic algorithms provide the underlining tools to most security protocols used in today infrastructures.
- The algorithms work off of different mathematical functions and provide different types of functionality and different levels of security.
- A big leap was made when encryption went from symmetric key use to public key cryptography.
- Using cryptography user will get more security than plain data transmission over the network.
- Here RSA algorithm is used which asymmetric key encryption algorithm is having ability to encrypt and decrypt file using different keys.

Future Scope:

How to protect user 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 project, we consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text 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.

REFERENCES:

1. S. S. M. Chow, Y. J. He, L. C. K. Hue, and S.-M. You, "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. 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.

3. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proceedings of Advances in Cryptology - EUROCRYPT '03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416–432.

4. 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.

5. M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in ACM Conference on Computer and Communications Security, 2009, pp. 121–130.

6. R. Canetti and S. Hohenberger, "Chosen-Ciphertext Secure Proxy Re-Encryption," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07). ACM, 2007, pp. 185–194.

7. C.-K. Chu and W.-G. Tzeng, "Identity-Based Proxy Re-encryption without Random Oracles," in Information Security Conference (ISC '07), ser. LNCS, vol. 4779. Springer, 2007, pp. 189–202.

8. C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou,and R. H. Deng, "Conditional Proxy Broadcast Re-Encryption," in Australasian Conference on Information Security and Privacy (ACISP '09), ser. LNCS, vol. 5594. Springer, 2009, pp. 327–342.

9. S. S. M. Chow, J. Weng, Y. Yang, and R. H. Deng, "Efficient Unidirectional Proxy Re-Encryption," in Progress in Cryptology - AFRICACRYPT 2010, ser. LNCS, vol. 6055. Springer, 2010, pp. 316–332.10.

10. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "ImprovedProxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 1, pp. 1–30, 2006.11.