PROVIDING INTEGRITY VERIFICATION FOR DATA DYNAMICS IN CLOUD

[1]Janarthanan R
hod@tjsenggcollege.com
Head of the Department
[2]Karpagam T
karpagamthulasi@gmail.com
Assistant Professor
[3]Menaka S
menakas311@gmail.com
PG Student
[4]VanithaC
chanvani2009@gmail.com
Assistant Professor

Department of Computer Science and Engineering

T.J.S. Engineering

ABSTRACT

In this project we majorly focus that more clients would like to store their data to public cloud servers (PCSs). New security problems have to be solved in order to help more clients process their data in public cloud computing. In this project the users are allowed to store data in the cloud, using services provided by multiple cloud storage providers (CSPs) is a promising approach to increase the level of data availability and confidentiality, as it is unlikely that different CSPs are out of service at the same time or collude with each other to extract information of a user. We propose a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Also we propose the splitting and merging concepts during storage in cloud environment. During file access private keys are generated using pseudo key generator. The keys are transmitted in a cipher text format to the users using 3DES encryption algorithm. To provide data confidentiality we propose a secure data hiding and image compression technique in cloud storage. Our main contribution will be image compression with reversible data hiding technique while storing in the real cloud for image data hiding & image compression we propose Discrete Wavelet Transform (DWT) algorithm.

Index Terms—Cloud computing, identity-based cryptography, proxy public key cryptography, remote data integrity checking

1.INTRODUCTION:

A long with the rapid development of computing and communication technique, a great deal of data is generated. These massive data needs more strong computation resource and greater storage space. Over the last years, cloud computing satisfies the application requirements and grows very quickly [1]. Essentially, it takes the data processing as a service, such as storage, computing, data security, *etc*. By using the public cloud platform,

the clients are relieved of the burden for storage management, universal data access with independent geographical locations, *etc*. Thus, more and more clients would like to store and process their data by using the remote cloud computing system [2].In public cloud computing, the clients store their massive data in the remote public cloud servers. Since the stored data is outside of
the control of the clients, it entails the security risks in terms of confidentiality, integrity and availability of data and service. Remote data integrity checking is a primitive which can be used to convince the cloud clients that their data are kept intact. In some special cases, the data owner may be restricted to access the public cloud server, the data owner will delegate the task of data processing and uploading to the third party, for example the proxy. On the other side, the remote data integrity checking protocol must be efficient in order to make it suitable for capacity-limited end devices [3]. Thus, based on identity-based public cryptography and proxy public key cryptography, we will study ID-PUIC protocol. In public cloud environment, most clients upload their data to *PCS* and check their remote data's integrity by Internet. When the client is an individual manager, some practical problems will happen. If the manager is suspected of being involved into the commercial fraud, he will be taken away by the police. During the period of investigation, the manager will be restricted to access the network in order to guard against collusion. But, the manager's legal business will go on during the period of investigation. When a large of data is generated, who can help him process these data? If these data cannot be processed just in time, the manager will face the loss of economic interest. In order to prevent the case happening, the manager has to delegate the proxy to process its data, for example, his secretary. But, the manager will not hope others have the ability to perform the remote data integrity checking. Public checking will incur some danger of leaking the privacy [4]. For example, the stored data volume can be detected by the malicious verifiers. When the uploaded data volume is confidential, private remote data integrity checking is necessary. Although the secretary has the ability to process and upload the data for the manager, he still cannot check the manager's remote data integrity unless he is delegated by the manager. We call the secretary as the proxy of the manager. In PKI (public key infrastructure), remote data integrity checking protocol will perform the certificate management [5]. When the manager delegates some entities to perform the remote data integrity checking, it will incur considerable overheads since the verifier will check the certificate when it checks the remote data integrity. In PKI, the considerable overheads come from the heavy certificate verification, certificates generation, delivery, revocation, renewals, *etc*. In public cloud computing, the end devices may have low computation capacity, such as mobile phone, i-pad, *etc*. Identity-based public key cryptography can eliminate the complicated certificate management. In order to increase the efficiency, identity based proxy-oriented data uploading and remote data integrity checking is more attractive. Thus, it will be very necessary to study the ID-PUIC protocol.

2.LITERATURE REVIEW:

Reema Gupta and Tanisha implemented a concept of hybrid encryption scheme to address the security needs. In this they proposed 2 encryption algorithms like blowfish and recent version of RSA. For test bed, they have utilised cloud environment [6].

Elham Abdet al., proposed multiple cloud storage architecture. They have address various security protocols invoking multiple cloud servers. Also it addresses the security and privacy preserving needs of the data owners [7].

S. Subbiah et al., have addressed security issue in cloud storage using vertical partitioning algorithm. This protects the user data from intrusion and security breach. Thus this algorithm is being implemented in java and compared with other partitioning algorithm to identify the accuracy and efficiency [8].

S. Selva Muthukumaran and T. Ramkumar represented an Approach for Enhancing Secure Cloud Storage Using Vertical Partitioning

Algorithm. The vertical partitioning algorithm is used to protect the data in an efficient manner. The algorithm has been executed in a java platform and results are compared with the other algorithms [9].

Priyanka et al, proposed multi-cloud storage system using distributed file system. In this research article, encryption, splitting of user data and storing in multiple cloud servers are been addressed. Also comparison of storage between single cloud and multiple clouds are been elaborated [10].

3.EXISTING SYSTEM:

Due to cloud system migration, many clients move their data to public cloud servers (PCSs). Many security problems are resolved to gain the confidentiality of the client. Thus when the clients are authorized and restricted, they try to access the data using proxy and upload the data. Thus security problems also play a major role in the public cloud systems. Also the admin should make sure the client outsourced data is secure [6]. Thus there is no complete solution for security and reliability. Example: If the third party user knows the key of a registered users file or data, the third party user will get the file easily.

4.PROPOSED SYSTEM:

We propose a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Also we propose the splitting and merging concepts during storage in cloud environment. During file access private keys are generated using pseudo key generator. The keys are transmitted in a cipher text format to the users using 3DES encryption algorithm. This proposed system will solve the problem of storing data with reliability and security in multiple clouds in accordance to user budgets. To provide data confidentiality we propose a secure data hiding and image compression technique in cloud storage. Our main contribution will be image compression with reversible data hiding technique while storing in the real cloud. As extensive literature survey states storage and security are the important factors in the cloud storage so focus on project on both reversible data hiding and image compression techniques. For image data hiding & image compression we propose Discrete Wavelet Transform (DWT) algorithm.

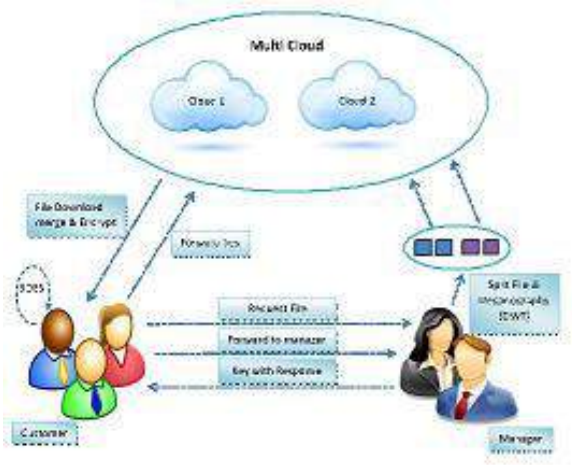

Fig 1: System Architecture

5.PRELIMINARIES:

Identity Management:

At first Initial stage all users must create own username and password. After the Registration the user can login to their own space. This application verifies the username and password which is either matched or not with the user registration form which is already created by the user while user registration process. If the valid user did not remember the username or password correctly the user can generate own password by using this application.

Time-based Group Key Management

Time-based Group Key Management algorithm for cryptographic cloud storage applications, which uses the proxy re-encryption algorithm to transfer major computing task of thegroup key management to the cloud server. So, the proposed TGKM scheme greatly reduces the user's computation and storage overhead and makes full use of cloud server to achieve an efficient group key management for the cryptographic cloud storage applications. Moreover, we introduce a key seed mechanism to generate a time-based dynamic group key which effectively strengthens the cloud data security. Our security analysis and performance evaluations both show that the proposed TGKM scheme is a secure and efficient group key management protocol for the cloud storage applications with low overheads of computation and communication.

Split and Merge:

Cloud Storage usually contains business-critical data and processes, hence high security is the only solution to retain strong trust relationship between the cloud users and cloud service providers. Thus to overcome the security threats, this paper proposes multiple cloud storage. Thus the common forms of data storage such as files and databases of a specific user is split and stored in the various cloud storages (e.g. Cloud A and Cloud B). Databases consists of tables, rows and columns. Databases are easy to store in multiple cloud storages. Our application will act as a combiner and store different parts of the table such as rows and columns in multiple clouds using Vertical fragmentation and horizontal fragmentation. These rows and columns will be encrypted using 3DES encryption algorithm. During response our application combines the data and sends to the verifier. Files are stored in multiple clouds using cryptographic data splitting. The file is split into fragments and stored in distinct cloud servers with encrypted key. Thus once the authorized token for the specific file is requested, searchable encryption allows keyword search on encrypted data and combines the fragments. This is sent to the verifier.

3DES:

3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56). TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt-Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3.

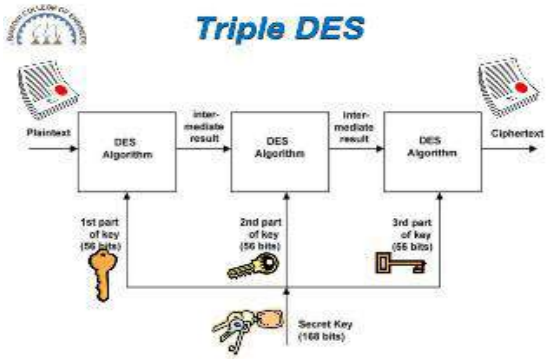

Fig 2: ALGORTHM DESIGN

Steganography

Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. More commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the

hidden message is not seen. The aim of these techniques is to hide secret data (steganograms) in the innocent looking carrier e.g. in normal transmissions of users. In ideal situation hidden data exchange cannot be detected by third parties. For image hiding and compression we have implemented DWT algorithm for efficient data hiding and extraction.

CONCLUSION:

This research project model focus on security. Thus secure key generation and transmission is performed by integrating virtual machines.

REFERENCE:

[1] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans. Commun., vol. E98-B, no. 1, pp. 190–200, 2015.

[2] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," J. Internet Technol., vol. 16, no. 2, pp. 317–323, 2015.

[3] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in Proc. CCS, 1996, pp. 48–57.

[4] E.-J. Yoon, Y. Choi, and C. Kim, "New ID-based proxy signature scheme with message recovery," in Grid and Pervasive Computing (Lecture Notes in Computer Science), vol. 7861. Berlin, Germany: SpringerVerlag, 2013, pp. 945–951.

[5] B.-C. Chen and H.-T. Yeh, "Secure proxy signature schemes from the weil pairing," J. Supercomput., vol. 65, no. 2, pp. 496–506, 2013.

[6] Neha, Mandeep Kaur, Enhanced Security using Hybrid Encryption Algorithm, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 7, July 2016

[7] Elham Abd Al Latif Al Badawi & Ahmed Kayed, SURVEY ON ENHANCING THE DATA SECURITY OF THE CLOUD COMPUTING ENVIRONMENT BY USING DATA SEGREGATION TECHNIQUE, IJRRAS, 2015.

[8] S. Subbiah, S. Selva Muthukumaran and T. Ramkumar, An Approach for Enhancing Secure Cloud Storage Using Vertical Partitioning Algorithm, Middle-East Journal of Scientific Research, 2015.

[9] Miss. Priyanka.R.Raut, Prof. Vaidehi Baporikar, DESIGN AND IMPLEMENTATION OF ENHANCED SECURITY IN MULTICLOUD STORAGE SYSTEM USING DISTRIBUTED FILE SYSTEM, IJSETR, 2015.

[10] X. Liu, J. Ma, J. Xiong, T. Zhang, and Q. Li, "Personal health records integrity verification using attribute based proxy signature in cloud computing," in Internet and Distributed Computing Systems (Lecture Notes in Computer Science), vol. 8223. Berlin, Germany: SpringerVerlag, 2013, pp. 238–251.