FLAW LESS CODING AND AUTHENTICATION OF USER DATA USING MULTIPLE CLOUDS

[1] J. Danny Anurisha and [2]A.Lalitha

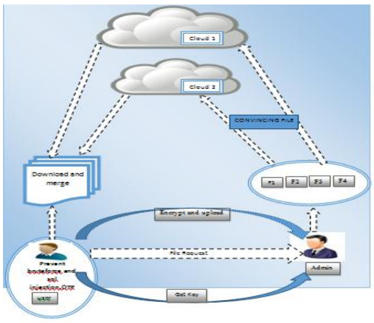
[1] Student, [2] Associate Professor
[1,2] Department of Computer Science and Engineering,
[1,2]Valliammai Engineering College SRM Nagar, Kattankulathur-603203, TamilNadu, India.

Abstract-*Nowadays more clients store their data in public cloud servers (PCSs).New security problems have to be solved in order to help more clients process their data in public cloud computing. The users are allowed to store data in the cloud, using services provided by multiple cloud storage providers (CSPs) which is a promising approach to increase the level of data availability and confidentiality. The data is stored by 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 use 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 use the Discrete Wavelet Transform (DWT) algorithm.*

Keywords-Public cloud servers, private key, data hiding, image compression, Data encryption etc.

1. INTRODUCTION

Cloud computing is an internet based computing that provides shared computer processing resources and data to computers and other devices on demand.Cloud providers typically use a pay service model. This will lead to unexpectedly high charges if administrators do not adapt to the pricing model in cloud. The availability of high-capacity networks, low-cost computers and storage devices which is the widespread adoption of hardware virtualization and its service-oriented architecture leads to autonomic and utility computing. Companies can scale up when computing needs increase rapidly and then scale down again as demands decrease. It was reported that cloud computing had become a highly demanded service or utility since it has the advantages as follows as such of high computing power, East to use, high performance, scalability, accessibility as well as availability. Cloud computing services can be private, public or hybrid clouds. This model offers versatility and convenience while preserving the management control and security allocated to common to local data centers.In the public cloud, a third party provider delivers the cloud service over the internet for the user. Public cloud services are sold on demand, typically by the minute or hour for the CPU cycles, storage and bandwidth they consume. Hybrid cloud is the combination of public cloud services and on-premises private cloud. Sensitive applications and confidential information are stored on the private cloud while using the public cloud. The hybrid cloud aims to create a unified network that automated in a scalable environment that takes advantage of all that a public cloud infrastructure. IaaS providers such as AWS supply a virtual server and storage instance as well as application program interfaces (API) that let users migrate workloads to a virtual machine. User filess have an allocated storage capacity that can start, stop, access and configure the VM and storage as desired. IaaS providers offer customised memory or optimized instances in addition to customized instances for various workload needs. In the PaaS model, providers host development tools on their infrastructures in which the user access these tools over the internet using APIs, web portals or gateway software. The PaaS deployed is used for general software development and many PaaS provider hosts the software after the development phase is completed. SaaS is a distribution model that delivers software applications over the internet are called web services. Microsoft Office 365 is a software that offers SaaS for software productivity and email services. Users will be able to access SaaS applications and services from any location using any device such as computer or mobile device that has internet access. The objective of image compression is to reduce irrelevance and redundancy of the data wherein the image in order to be able to store or transmit data in an efficient manner. Image compression is merely minimizing the size of a file either a text file or a graphics file without degrading the quality of the image to an unacceptable level. The reduction in the size of the file allows more number of images to be stored in a given amount of disk or memory space. It also reduces the uptime required for images to be sent over the Internet or downloaded from Web pages. A text or a program can be compressed without the introduction of errors, but only up to a certain extent of reduction which is called as lossless compression. Beyond this point, errors are introduced. In text files and program files, it is crucial that compression can be lossless because even a single error can seriously damage the meaning of a text file, or cause a program not to run. There is no point such as critical point up to which compression works perfectly, but beyond which it impossible. When there is some tolerance for loss is considered, the compression factor can be greater when there is no loss tolerance. For this reason, graphic images can be compressed more than text files or programs. Data hiding is a process to hide data into cover media. The relationship between these two sets of data characterizes different applications. In authentication phase embedded data are closely related to the cover media. Data hiding in images are selected as the cover media called as cover images. Cover images with the secret messages embedded in the images. Most of the hiding techniques is based on manipulating the least-significant-bit (LSB).Another technique introduced is to improve image quality by a local pixel adjustment process using an optimal substitution matrix for the embedding of the secret messages in the user data. It is a process planned to yield a compact representation of an image by reducing the image storage.



2. LITERATURE SURVEY

[1] In this paper, a secure data sharing scheme for dynamic members is developed. First, it uses a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager. Second, the scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Third, the scheme protects from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud. Finally it achieves fine efficiency, which means previous users need not update their private keys for the situation because either a new user joins in the group or a user is revoked from the group.[2] In this paper, a multi-authority CP-ABE scheme is proposed in which the authorities need not interact to generate public information during the system initialization phase. The scheme has constant ciphertext length and a constant number of pairing computations. The scheme can be proven CPA-secure in random oracle model under the decision q-BDHE assumption. It achieves the length of ciphertext in terms of optimization and enhances the efficiency of the encryption and decryption operation of uploading user data.[3]In this paper clouds uses a huge extra storage consumption, resulting in a huge storage cost for data-intensive applications in the Cloud in particular. In order to reduce the Cloud storage consumption while meeting the data reliability requirement, a cost-effective data reliability management mechanism named PRCR is presented based on a generalized data reliability model.The simulation indicates that when compared with the conventional three-replica strategy PRCR can reduce the Cloud storage space consumption, hence significantly lowering the storage cost in a Cloud. This mechanism is designed to be implemented by the Cloud storage providers in order to increase the profit and/or the competitiveness by cost saving, as well as serve as, a benchmark for storage consumption of different approaches. [4] This paper deals with the first range query processing scheme that achieves index indistinguishability under the indistinguishability against chosen keyword attack(IND-CKA). The key idea is to organize indexingelements in a complete binary tree called PBtree, which satisfies structure indistinguishability(i.e., two sets of data items have thesame PBtree structure if and only if the two sets have the same number of data items) and node

indistinguishability(i.e., the valuesof PBtree nodes are completely random and have no statistical meaning). The worst-case complexity of our query processing algorithm using PBtree is , where the total number of data items and the set of data items in the query result.[5] In this paper the ciphertext policy attribute based encryption (CP-ABE) schemes where the access policy is defined by AND-gate with wildcard. In particular, it shows a way to bridge Attribute based encryption techniques based on AND-gate with wildcard with inner product encryption It proves that the second scheme is secure under the standard decisional linear and decisional bilinear Diffie–Hellman assumptions. [6] In this paper it shows how the user stores data in the cloud, using services provided by multiple cloud storage providers (CSPs) which 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. This paper investigates the problem of storing data reliably and securely in multiple CSPs constrained by given budgets with minimum cost. First, CSPs may be unavailable temporarily or even permanently due to various reasons including disk failure, hacker attack, network disconnection, natural disaster, or even political influence. Second, from users' perspective, data stored in a CSP is not confidential, since the CSP has full access to its customers' data. [7] This paper works with Ciphertext Policy Attribute-Based Encryption (CP-ABE) which enforces expressive data access policies and each policy consists of a number of attributes On the other hand, existing privacy preserving schemes protect the anonymity of the ciphertext size. The proposed novel PP-CP-ABE construction, named Privacy Preserving Constant-size Ciphertext Policy Attribute Based Encryption (PP-CP-ABE) deals with wildcards and incurs constant-size conjunctive headers, regardless of the number of attributes. In our implementation, we use Type–D MNT curves with element compression. [8] In this paper new security problems have to be solved in order to help more clients process their data in public cloud. When the client is restricted to access PCS, he will delegate its proxy to process his data and upload themIt gives the formal definition, system model, and security model. The proposed ID-PUIC protocol is provably secure based on the hardness of computational Diffie-Hellman problem. In public cloud, this paper focuses on the identity-based proxy-oriented data uploading and remote data integrity checking. By using identity-based public key cryptology, the proposed ID-PUIC protocol is efficient since the certificate management is eliminated. [9] A novel scheme of reversible data hiding is proposed in encrypted images using distributed source coding. The selected bit series is Slepian–Wolf encoded using low-density parity check codes. On the receiver side, the secretbits can be extracted if the image receiver has the embedding key only .The proposed separable RDH method is applied for encrypted images using Slepian–Wolf source encoding. [10]In this paper, we propose a two-factor data security protection mechanism with factor revocability for cloud storage system. Our system allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the ciphertext. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the ciphertext without either piece. More importantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any ciphertext.

3. CONCLUSION

As per the literature survey done, there is a need to store the user data securely in multiple clouds. The users are allowed to store data in the cloud using services provided by multiple cloud storage providers (CSPs). The splitting and merging concepts are used 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.

4. FUTURE WORK

To provide data confidentiality, a secure data hiding and image compression technique is used in cloud storage. Our main contribution will be image compression with data hiding technique while storing in the real cloud. It is desired to make the progress to be implemented on the cloud and to enable the algorithms to work properly in the cloud environment. It can be continued, so as to produce a high quality image after the image compression technique are to be implemented.

5. REFERENCES

[1] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System", VOL. 65, NO. 5, MAY 2016

[2] Zhongma Zhu and Rui Jiang "Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", VOL. 27, NO. 1, JANUARY 2016.

[3] CHEN Yanlil, Lingling1, YANG Geng2 " Attribute-Based Access Control for Multi-Authority Computing", Feb 2016.

[4] Kan Yang, Zhen Liu, Xiaohua Jia and Xuemin Sherman Shen "Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing:A Cryptographic Approach" , VOL. 18, NO. 5, MAY 2016.

[5] R. Ostrovsky and B. Waters, "Attribute-based encryption with non monotonic access structures," JULY 2012.

[6] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges", VOL. 305, JUNE 2015.

[7] Q.Jing A.V. Vasilakos, J.Ubun, J.Lu and D.Qi " Security of the internet of things:Perspective and Challenges"Vol 20, NO. 4,NOVEMBER 2014.

[8] M.Van Dijik and A.Juds,"On the impossibility of cryptography alone for privacy preserving cloud computing",OCTOBER 2010.

[9] M.Ali et al" SeDaSC:Secure Data Sharing in Cloud", IEEE, JUNE 2014.

[10] X.Yang, S.Kandula, M.Zhang, "Cloud Computing: Comparing Public cloud Providers" in Proc. Melbourne, NOVEMBER 2010.