SECURE DATA MIGRATION FOR PEER-TO-PEER CLOUD SYSTEM

Mrs. SUSI. A[1], Mrs. SAKTHIYAVATHI.K[2] , ASHIFA.T[3], SANGEETHA.S[4], SWENITHA.S[5]

[1,2]Assistant Professors, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry – 605107
[3,4,5]UG Students, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry - 605107

---***---

Abstract *With the development of cloud computing, another path for data sharing is being shaped profiting each and every other individual or association related with it. However, there exists a characteristic obstruction for clients to directly transfer the data to the cloud server since the information frequently contain significant data. In this manner, it is important to put cryptographically improved admittance control on the data that is being shared and data must be accessed only by authorized users. A revocable identity based encryption (RS-IBE) is utilized which can give the forward/backward security of ciphertext by presenting the functionalities of client revocation and ciphertext update all the while. . Here the state-of-the-art authentication mechanisms reported for the secure cloud transfer, we have identified the weak points and the strengths of the different mechanisms studied in order to better establish our solution.*

Key Words: **Data Migration, Authentication, Confidentiality, Security, Cloud Computing**

1.INTRODUCTION

Cloud computing services has become an important paradigm as it is reliable and provides a cost-effective way of storing and hosting applications. Cloud storage is developing dramatically there is a need to oversee and screen the data in a protected way . Data migration is moving data starting with one cloud then onto the next Cloud storage system. Data Migration in cloud is done because of different reasons like less expensive expense for user of cloud i.e., pay per utilization. Data migration need to be securely transferred for maintaining confidentiality such migration can strongly or effectively done even some active attacks are occurred. So, some encryption techniques should be effectively done during migration of data which can ensures integrity , confidentiality and data loss prevention. Our goal is to analyze the cloud migration techniques, which is useful in specifying the security requirements and to determine the limitations of current cloud migration mechanism.

1)Data confidentiality: Unauthorized clients ought to be stop from getting to the plaintext of the shared information which is put away in the cloud server. Moreover, the cloud server, which should be certifiable however curious, ought to likewise be turn away from knowing plaintext of the shared data.

2)Backward secrecy: Backward secrecy implies when a client's approval is being stopped, or a client's secret key is undermined, he/she ought to be kept from getting to the plaintext of the in this manner shared information that are as yet being decrypted under their identity.

3) Forward secrecy: Forward secrecy implies when a client's position is stopped, or a client's secret key is undermined, he/she ought to be kept from getting to the plaintext of the shared data that can be recently gotten to by him/her.

The particular issue addressed in this paper is the means by which to develop a major identity based cryptographical mechanism to accomplish the above security objectives. We likewise note that there stay alive other security gives that are similarly significant for a viable arrangement of data sharing, like the authenticity and accessibility of the shared data.

2. RECENT WORK

The work proposed in [1],address the low computational overhead during data sharing in mobile cloud environment through a light-weight data sharing scheme. It uses a CP-ABE, a technology utilized within the traditional cloud environment for access control, by making changes in the structure of access control tree to make it suitable for mobile cloud environment. Here the normal CP-ABE algorithm is modified and LDSS-(CP-ABE) algorithm is built to make sure the privacy of data when outsourcing computational tasks to users mobile and service providers decryption.

In the idea focused in [2], the author has proposed a Two Factor Authenticated key exchange (TF-AKE) protocol which may be a dynamic Idensity based anonymous two factor security model which ensures user anonymity and extra mechanism of desynchronization to resist lost smart card attack and prevents leakage of data by introducing a nonces within the message flows.

The idea implemented in[3], the author has proposed a model that concentrates on data confidentiality and integrity. They use Multi-factor Authentication for user authentication through static username and password and OTP generation using new tokens or default tokens . The Ciphertext Policy Attribute Based Encryption(CP-ABE) algorithm used as encryption technique for achieving data confidentially and access control.

In the novel method in [4], which focuses on a secure data migration mechanism to migrate the data's between different cloud storage system. It comprises of mutual authentication, blended with key splitting and sharing methods that ensure pre-migration authentication. It is performed by symmetric keys encryption, which are shared using RSA Cryptosystem. The safety factors like confidentiality, authentication, integrity , authorization, are ensured by this system .

In the thought centred in [5], the creator has proposed a methodology for secure and consistent movement of legacy mechanical control frameworks to the cloud . It works as fitting and play and makes no or insignificant interference modern tasks during the cloud relocation measure. The plan and approval for synchro phasor innovation in smart grid utilizing the Amazon AWS cloud is taken as a utilization case.

The work proposed in [6], investigates the intercloud information movement component and distinguish security issues as far as Hadoop Distributed File System (HDFS) . This methodology ensures better security and quicker response time during move of enormous information records in distributed storage frameworks.

In [7] , a novel strategy has been proposed to protect data transfer with irregular enhanced cryptographic method. It involves three stages, for example, is validation is finished by the Trusted Third Party (TTP) utilizing the Luhn calculation , data encryption is performed with the Randomized Optimal Cryptographic Technique (ROCT) utilizing Efficient Probabilistic Public Key Encryption (EPPKE) plan and information recovery through CSP dependent on client verification. Furthermore, BLAKE 2b calculation likewise used to guarantee the information trustworthiness. It is carried out in Open Stack with Java Language.

The work submitted in [8] ,the author proposes a plan which guarantees secure data transfer from the customer's framework to the Cloud Service Providers. It's anything but a consolidated methodology of cryptography and steganography for information transmission as it provide a two way security. The information is changed over into a coded design through encryption calculation and afterward this coded design information is changed over again into a harsh picture utilizing steganography. As steganography shrouds the presence of the message, accordingly odds of information being taken are less.

In the thought centred in [9] , the author has proposed secure revaluated information move plot which permits customer's to relocate their information starting with one cloud then onto the next cloud without recovering the information from the previous cloud to accomplish the information secrecy and confidentiality can be accomplished during this cycle. The cloud can perform secure information guarantee after the information are relocated by using the intermediary re-encryption method which guarantees secure information movement in distributed storage.

In [10], the paper surveys various cloud migration techniques where its findings and contribution are analysed, it aims to identify some limitations of current cloud computing migration techniques.

3. PROPOSED WORK

The main entities involved in our proposed methodology are: cloud user, the person who is the member of the cloud as well the owner of data; Cloud Service Provider one who has large storage space to store enough information, computing resources, and offer remote data storage services to users in a pay-as-you-use manner and the trusted third party, trusted by both the Cloud Service Provider as well as the cloud user. When a user wants to transfer data, the trusted third party [data providers] who encrypts the data under the identities of authorized users and uploads the encrypted form of the shared data to the cloud storage. When an authorized user wants to get the shared data, they can download and decrypt the corresponding data. However, for an unauthorized user and the cloud server, the original message of the shared data is not available. In some cases, user's authorization gets expired, data provider can download the ciphertext of the shared data, and then decrypt-then-re-encrypt the shared data such that user is prevented from accessing the shared data, and then reupload the encrypted data to the cloud server.

3.1 STEPS INVOLVED IN PROPOSED WORK:

User Registration Page

User register with their username and password to connect with cloud server .Server will create the account for the user to maintain , upload file and download/sharing file to another user. If the user is new user, user must record their details such as username, password, renter password, gender and Email id etc. or already existing user directly can login into the server.

Access Key

In this module, once registration process completed the user can login to the server, the server sent the dynamic Trial/secret key for uploading the file. Using that key user can upload many files at a time.

Upload File

After receiving key from Data owner via E-Mail cloud users upload many documents with using same key.

Key Validation

In this module, implemented Forward secrecy. i.e., if the user's authority is expired or secret key is compromised should be prevented to accessing the plaintext of the shared data that can be previously accessed from the server. New key will be generated as per existing user request.

File store to cloud server

Cloud file sharing, also called cloud is allotted storage space or an online file sharing on a server used for file authorized user to upload documents with file name , type and modified time.

4. Security Analysis

Authorization: It is a security that checks the character of an individual or an association. Login id and passwords of the clients are like the dashboard login page address. Authentication is done to check the source cloud, objective cloud, and clients before data movement happen.

Confidentiality: The data which is being moved from source cloud to objective cloud ought not be uncovered to third individual. This is guaranteed by encrypting at the source cloud and decrypting at the objective cloud utilizing private key. This process empowers confidentiality of the data involved Regardless of whether an attacker gains admittance to any of the messages passed, as in Man-In-the Middle Attack, he/she can't extricate the messages since they are encrypted.

Integrity: The hashing procedures used to ensure the integrity of the data shared. The data with its hash esteem is sent from the source to objective and integrity protects the information of the data. The data ought not be missed or changed by unapproved clients. Data trustworthiness is the principal cycle of checking the information and significant among other cloud difficulties.

5. CONCLUSIONS

Cloud computing is widely used nowadays because of its reduced cost, shared resources, ubiquitous access, higher efficiency etc. Hence, it is paramount to have mechanisms to migrate the data stored in one cloud storage system to another cloud storage system. Secure data migration is an important as a successful cloud migration reduces cost efficiency, improves scalability , easy access and achieves data loss preventions. We addressed main security attributes of data migration such as confidentiality, authenticity, authorization and data integrity. Thus, identifies state-of-the-art of cloud computing migration techniques and their security requirements.

REFERENCES

[1] R. LI, C. Shen, H. He, X. Gu, Z. Xu and C. Xu, "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing," 2018

[2] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen and L. Fang, "Provably Secure Dynamic ID-Based Anonymous Two-Factor Authenticated Key Exchange Protocol with Extended Security Model,"

[3] R. Nikam and M. Potey, "Cloud storage security using Multi-Factor Authentication," *2016*

[4] C. Gudisagar, B. R. Sahoo, M. Sushma and C. D. Jaidhar, "Secure data migration between cloud storage systems," *2017*

[5] R. Khan, K. McLaughlin, B. Kang, D. Laverty and S. Sezer, "A Seamless Cloud Migration Approach to Secure Distributed Legacy Industrial SCADA Systems," *2020*

[6] I. Khalil, I. Hababeh and A. Khreishah, "Secure inter cloud data migration," *2016*

[7] M. G. Aruna and K. G. Mohan, "Secured cloud data migration technique by competent probabilistic public key encryption," 2020

[8] A. Dhamija and V. Dhaka, "A novel cryptographic and steganographic approach for secure cloud data migration," 2015

[9] J. Ni, X. Lin, K. Zhang, Y. Yu and X. S. Shen, "Secure outsourced data transfer with integrity verification in cloud storage," in 2016

[10] A. Balobaid and D. Debnath, "An Empirical Study of Different Cloud Migration Techniques," in *2017*