# EFFICIENT DATA MIGRATION MODEL USING ANONYMOUS IDENTITY IN MULTI CLOUD ENVIRONMENTS

**M.Naga Prahitha,** Student , Department of CSE, Narayana Engineering College (Autonomous) Gudur,.SPSR Nellore, AP, India
**Mr.U.Satyanarayana,** Assistant Professor, Department of CSE, Narayana Engineering College (Autonomous) Gudur,.SPSR Nellore, AP, India
**K.Pavithra,Student ,** Department of CSE, Narayana Engineering College (Autonomous) Gudur,.SPSR Nellore, AP, India
**D.Lakshmi Vinuthna,** Student Department of CSE, Narayana Engineering College (Autonomous) Gudur,.SPSR Nellore, AP, India

## Abstract

Cross-cloud information relocation is one of the common difficulties looked by portable clients, which is a fundamental interaction when clients change their cell phones to an alternate supplier. Be that as it may, because of the deficient neighborhood stockpiling and computational capacities of the advanced cells, it is regularly exceptionally hard for clients to reinforcement all information from the first cloud workers to their cell phones to additionally transfer the downloaded information to the new cloud supplier. To tackle this issue, we propose a proficient information relocation model between cloud suppliers and develop a shared confirmation and key understanding plan dependent on elliptic bend declaration free cryptography for distributed cloud. The proposed conspire assists with creating trust between various cloud suppliers and establishes a framework for the acknowledgment of cross-cloud information movement.

**Index terms** – elliptic curve, authentication, key agreement.

## Introduction

With the rapid development of the smart phone and mobile terminal industries, smart phones have become indispensable for people. China housed an estimation of 847 million mobile Internet users in December 2018, with 99.1 percent of them using mobile phones to surf the Internet [1]. Due to the weak storage and processing capabilities of the mobile terminals, smart phone users often prefer to store largescale data files (video and audio files and streaming media files) in the cloud server. This has accelerated research of various perspectives in the cloud computing paradigm [2], [3]. Smartphone manufacturers are increasingly launching and deploying their own cloud computing services to provide users with convenient data storage services [4], [5].

People are now increasingly relying on hand-held devices such as smart phones, tablet etc., in an unprecedented number. It is worthy of note that one individual may own and use multiple smart devices. It is also common for people to recycle their smart devices quite frequently, given the fact that new arrivals characterize more attractive inherent features from a variety of manufacturers.

When people opt to use a new smart device from a different manufacturer, the data stored in the cloud server of the previous smart device provider should be transferred to the cloud server of the new smart device provider. One of the common ways of accomplishing this transfer is to log onto the original cloud server, download the data onto the smart terminal devices, log onto the new cloud server, and finally upload the data to the new server. As shown in Fig. 1, this process is very inefficient and tedious. To this end, it is essential to develop a more efficient and secure way of data transfer from one cloud server to another. An ideal data migration model that can transfer user data directly between cloud servers is shown in Fig. 1.

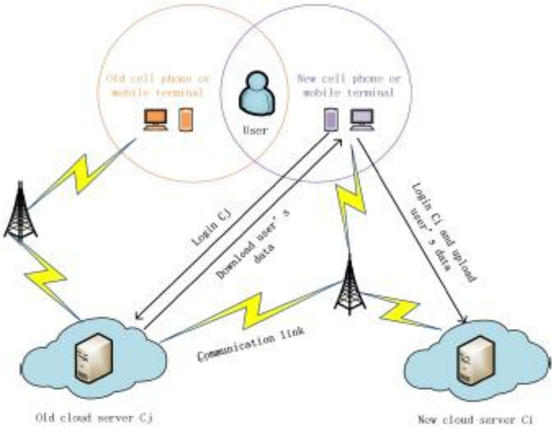

Old cell phone or mobile terminal
User
New cell phone or mobile terminal
Login Cj
Download user's data
Login Ci and upload user's data
Communication link
Old cloud server Cj
New cloud server Ci

**Fig. 1: Original Data migration Model**

Such a model often imposes compatibility issues, since different cloud service providers characterize diverse user functions, mutual distrust and security risks in the process of data transmission, which make this ideal data migration model difficult to implement.

A few researches have attempted to overcome such data migration issues in the recent past. For example, in 2011, Dana Petcu [6] argued that the biggest challenge in cloud computing is the interoperability between clouds, and proposed a new approach for cloud portability. Binz et al. [7] proposed a cloud motion framework that supports the migration of composite applications into or between clouds. Designed a scheme to support data portability between cloud databases[8].

## Literature survey

In order to realize data sharing in the cloud, a few schemes have used proxy re-encryption techniques [9]. For example, Liang and Cao [9] proposed a property-based proxy re-encryption scheme to enable users to achieve authorization in access control environments. However  pointed out that this scheme does not have Adaptive security and CCA security features[10]. Sun et al. introduced a new proxy broadcast repeat encryption (PBRE) scheme and proved its security against selective ciphertext attack (CCA) in a random oracle model under the decision n-BDHE hypothesis[11][12].

Ge and Liu proposed a broadcast agent encryption (RIBBPRE) security concept based on revocable identity to solve the key revocation problem. In this RIB-BPRE scheme, the agent can undo a set of delegates specified by the principal from the re-encryption key. They also pointed out that the identity-based broadcast agent re-encryption (RIB-BPRE) schemes do not take advantage of cloud computing, thus causes inconvenience to cloud users.

Liu et al. proposed a secure multi-owner data sharing scheme for dynamic groups in the cloud. Based on group signature and dynamic broadcast encryption technology, any cloud user can share their data anonymously with others. Yuan et al. proposed a cloud user data integrity check scheme based on polynomial authentication tag and agent tag update technology, which supports multi-user modification to resist collusive attack and other features. Ali et al. proposed a secure data sharing cloud (SeDaSC) method using a single encryption key to encrypt files. This scheme provides data confidentiality and integrity, forward and backward access control, data sharing and other functions. Li et al. proposed a new attribute-based data sharing scheme to assist mobile users with limited resources based on cloud computing.

Authentication and key agreement is a method that enables both parties to secretly calculate the session key on a public channel, which have been widely studies. As early as 1993, Maurer proposed that only a difference in the received signals helps achieving perfect cryptographic security, regardless of the enemy's computing power. But they have not considered the advantage of legitimate communicants. suffices for achieving perfect cryptographic security, regardless of the enemy's computing power. Lu and Linproposed a medical key negotiation scheme based on patient symptom matching. However, He et al. pointed out that Lu's scheme does not provide an identity tracking and resistance modification function and further proposed a cross-domain handshake scheme applicable to medical mobile social network and developed an android app for experimental analysis. Later, Liu and Ma found that He et al.'s scheme does not resist replay attack.

Mahmood et al. proposed an anonymous key negotiation protocol for smart grid infrastructure that enables smart meters to connect anonymously to utilities. But Wang and Wu pointed out that Amor et al.'s protocol cannot resist stolen verifier attacks and Mahmood et al.'s protocol cannot resist man-in-the-middle attacks and impersonation attacks.

**Proposed system**

Different from other traditional schemes, due to the particularity of our model, we replace the trusted authority (TA) with the users, for the generation of system parameters and partial key distribution. As shown in Fig. 2, our scheme contains three entities including a smart phone user U and two cloud server Ci;Cj .

U: The cell phone user, who publishes system parameters and distributes partial private keys to both the cloud servers.

Ci or Cloudi: The request data cloud server. This server verifies the validity of the user and performs mutual authentication and key negotiation with Cj.

Cj or Cloudj : The source data cloud server. This server verifies the validity of the user and performs mutual authentication and key negotiation with Ci.

In our model, users when changing their mobile devices, should first register and login to both the cloud server Ci (the new provider) and the cloud server Cj (the original mobile phone provider). The two cloud servers are now in a peer scenario. The user distributes part of the private key to both the cloud servers through a secure channel. Then, Ci and Cj exchanges related information, and Ci sends a request message to Cj to initiate the mutual authentication and key agreement process.

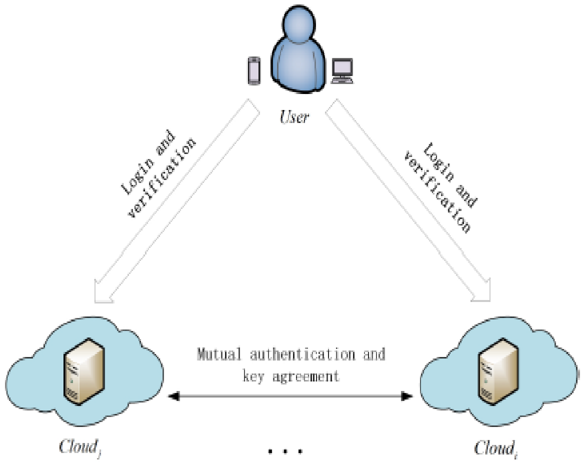


**Fig. 2: System Model**

## Implementation Modules

**User:**

- In this module, The cell phone user, who publishes system parameters and distributes partial private keys to both the cloud servers.
- In this upload the data into the cloud server before outsourcing data user has to encrypt the data.
- Once encrypt the data then he/she upload data to the cloud server.
- If he wants to change the cloud server the cloud server verifies the user validity.

**Mobile Terminal**

- In this module, user login to the system and view all cloud files, managed files, and view cloud tasks.
- He/ she can access the cloud data from the cloud server.

**Old Cloud Server**

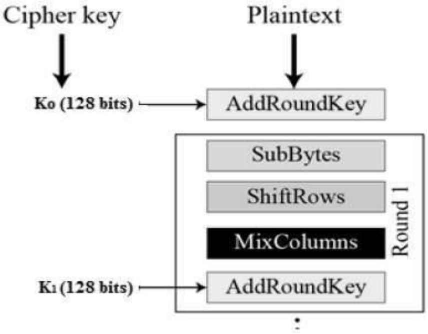
- The source data cloud server. This server verifies the validity of the user and performs mutual authentication and key negotiation with new Cloud Server.
- In this the cloud server view the users and authorize them, view all cloud files, view user transaction information, and view the user requests and check the validity, and send request to new cloud server.

### New Cloud Server:

- In this module, The request data cloud server. This server verifies the validity of the user and performs mutual authentication and key negotiation with old Cloud Server.
- In which, the cloud receives the request from the old cloud server, view all cloud files, view users details, view transactions, and validate the requests of the cloud server then accept or reject the request.

### Implementation Algorithm

- In this project to protect the personal documents we adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES).
- AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).



## Conclusion

This project proposed a novel scheme to transfer user data between different cloud servers based on a key agreement protocol. Through the mathematical analysis and comparative evaluation presented in this paper, the advantages of our scheme are proved from three aspects: security performance, calculation costs and communication costs. Our proposed scheme can efficiently solve the primary problem of trust during data migration between cloud servers and further can provide anonymity for the identity of cloud servers. On the premise of protecting the privacy of cloud service providers, our proposed scheme indirectly protects the privacy of users. In addition, the identity traceability provided by our proposed scheme also enables users to effectively constrain the cloud service providers.

## References

[1] C. I. network information center, “The 44th china statistical report on internet development,” http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201908/-P020190830356787490958.pdf, 2019.

[2] B. Li, J. Li, and L. Liu, “Cloudmon: a resource-efficient iaas cloud monitoring system based on networked intrusion detection system virtual appliances,” Concurrency and Computation: Practice and Experience, vol. 27, no. 8, pp. 1861–1885, 2015.

[3] J. Cui, H. Zhou, H. Zhong, and Y. Xu, “Akser: attribute-based keyword search with efficient revocation in cloud computing,” Information Sciences, vol. 423, pp. 343–352, 2018.

[4] J. Cui, H. Zhong, W. Luo, and J. Zhang, “Area-based mobile multicast group key management scheme for secure mobile cooperative sensing,” Science China Information Sciences, vol. 60, no. 9, p. 098104, 2017.

[5] J. Cui, H. Zhou, Y. Xu, and H. Zhong, “Ooabks: Online/offline attributebased encryption for keyword search in mobile cloud,” Information Sciences, vol. 489, pp. 63–77, 2019.

[6] D. Petcu, “Portability and interoperability between clouds: challenges and case study,” in European Conference on a Service-Based Internet. Springer, 2011, pp. 62–74.

[7] T. Binz, F. Leymann, and D. Schumm, “Cmotion: A framework for migration of applications into and between clouds,” in 2011 IEEE International Conference on Service-Oriented Computing and Applications (SOCA). IEEE, 2011, pp. 1–4.

[8] P Ravinder Rao,Dr. V.Sucharita,A Framework to Automate Cloud based Service Attacks Detection and Prevention, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 2, 2019.

[9] PM, Dr. P. Venkateswara Rao, Dr.V.Sucharita ,Data Security Using Multi-Authority Data Access Control for Cloud Storage SystemJournal of Emerging Technologies and Innovative Research 6 (6), 103-107

[10] X. Liang, Z. Cao, H. Lin, and J. Shao, “Attribute based proxy reencryption with delegating capabilities,” in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, 2009, pp. 276–286.

[11] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, “A secure and efficient ciphertext-policy attributebased proxy re-encryption for cloud data sharing,” Future Generation Computer Systems, vol. 52, pp. 95–108, 2015.