Authentication And Key Agreement Based On Anonymous Identity For Peer-To-Peer Cloud

Nagulapalli Mounika, Smt.K.R.Rajeswari, Sri.V.Bhaskara Murthy
Mca Student, Assistant Professor, Associate Professor
Dept Of Mca
B.V.Raju College, Bhimavaram

ABSTRACT
Cross-cloud data migration is one of the prevailing challenges faced by mobile users, which is an essential process when users change their mobile phones to a different provider. However, due to the insufficient local storage and computational capabilities of the smart phones, it is often very difficult for users to backup all data from the original cloud servers to their mobile phones in order to further upload the downloaded data to the new cloud provider. To solve this problem, we propose an efficient data migration model between cloud providers and construct a mutual authentication and key agreement scheme based on elliptic curve certificate-free cryptography for peer-to peer cloud. The proposed scheme helps to develop trust between different cloud providers and lays a foundation for the realization of cross-cloud data migration. Mathematical verification and security correctness of our scheme is evaluated against notable existing schemes of data migration, which demonstrate that our proposed scheme exhibits a better performance than other state of- the-art scheme in terms of the achieved reduction in both the computational and communication cost.

I. 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 large scale 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. 2. 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. In 2012, Shirazi et al. [8] designed a scheme to support data portability between cloud databases.

II. EXISTING SYSTEM

Liang and Cao [9] proposed a property-based proxy re-encryption scheme to enable users to achieve authorization in access control environments. However, Liang and Au [10] pointed out that this scheme does not have Adaptive security and CCA security features. Sun et al. [12] introduced a new proxy broadcast repeat encryption (PBRE) scheme and proved its security against selective cipher text attack (CCA) in a random oracle model under the decision n-BDHE hypothesis.

Ge and Liu [13] 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. [14] 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. [15] 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. [16] 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. [17] 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 [18]–[31]. As early as 1993, Maurer [18] 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 Lin [19] proposed a medical key negotiation scheme based on patient symptom matching.

However, He et al. [32] 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 [20] found that He et al.'s scheme does not resist replay attack.

Disadvantages

- In the existing work, the system doesn't have mote security due to lack of less security cryptography techniques.
- There is no authentication and key agreement for enhancing more security on data.

III. PROPOSED SYSTEM

The system proposes a peer-to-peer cloud authentication and key agreement (PCAKA) scheme based on anonymous identity to solve the problem of trust between cloud servers. Based on the elliptic curve certificate-free cryptography, our scheme can establish secure session keys between cloud service providers to ensure session security.

The novelty of the proposed scheme lies in the fact that it eliminates the need for trusted authority (TA) and simplifies operations while maintaining security. In our scheme, the cloud servers enable the data owners in need of the data migration services to act as trusted third authority, so that they can verify each other and establish trusted session keys after each of the involved users performs some computation independently.

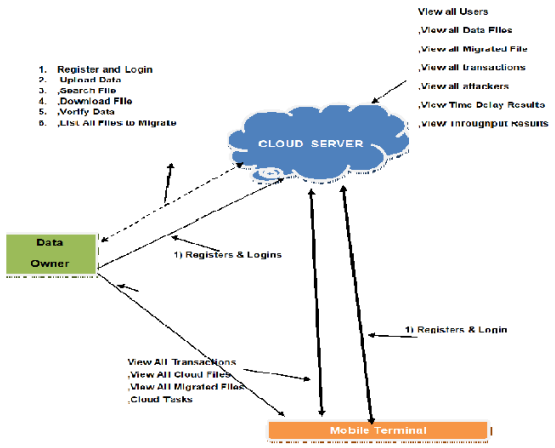
The proposed scheme uses server anonymity to protect the privacy of service providers and users. It is worthy of note that both the two cloud servers involved in the migration process use anonymous identities for mutual authentication and key agreement. This strategy not only protects the identity privacy of the cloud service providers, but also makes it impossible for the involved cloud service providers to gain unnecessary information such as the brand of the old and new mobile phones belonging to the users respectively. Thus, our methodology maintains the privacy of the users by not revealing his/her personal choice.

The proposed scheme provides identity traceability to trace malicious cloud servers. If the cloud service providers exhibit any errors or illegal operations in the service process, users can trace back to the real identity of the corresponding cloud server based on the anonymous identity.

Advantages

- The proposed achieves efficient revocation, efficient file access and immediate revocation simultaneously.
- The system stores encrypted data on the cloud, but never reveals the decryption keys to the cloud. This protects the confidentiality of the file data

IV. ARCHITECTURE DIAGRAM



V. IMPLEMENTATION

DATA OWNER

In this module, Data owner has to register to cloud and logs in, the data owner will do the following operations such Upload Data, Search File, Download File, Verify Data, List All Files to Migrate.

CLOUD SERVER

In this module, the cloud will authorize both the owner and the user and do the following operations such as View all Users, View all Data Files ,View all Migrated File, View all transactions, View all attackers, View Time Delay Results, View Throughput Results.

MOBILE TERMINAL

In this module, the terminal has to register to cloud and logs in. before the user can operate for the file details the terminal must do the following operations such as View All Transactions, View All Cloud Files, View All Migrated File, Cloud Tasks.

VI. CONCLUSION

This paper 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.

As a future work, we plan to explore and develop a protocol that allows multiple users to share data across different cloud servers, with the motivation of enhancing the efficiency of data sharing among multiple users.

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] M. N. Shirazi, H. C. Kuan, and H. Dolatabadi, "Design patterns to enable data portability between clouds' databases," in 2012 12th International Conference on Computational Science and Its Applications. IEEE, 2012, pp. 117–120.

[9] 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.

[10] 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.

[11] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, "Conditional identity-based broadcast proxy re-encryption and its application to cloud email," IEEE Transactions on Computers, vol. 65, no. 1, pp. 66–79, 2015.

[12] M. Sun, C. Ge, L. Fang, and J. Wang, "A proxy broadcast re-encryption for cloud data sharing," Multimedia Tools and Applications, vol. 77, no. 9, pp. 10 455–10 469, 2018.

[13] G. Chunpeng, Z. Liu, J. Xia, and F. Liming, "Revocable identitybased broadcast proxy re-encryption for data sharing in clouds," IEEE Transactions on Dependable and Secure Computing, 2019.

[14] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure multi-owner data sharing for dynamic groups in the cloud," IEEE transactions on parallel and distributed systems, vol. 24, no. 6, pp. 1182–1191, 2012.

[15] J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in IEEE INFOCOM 2014-IEEE Conference on Computer Communications. IEEE, 2014, pp. 2121– 2129.

[16] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, and A. Y. Zomaya, "Sedasc: secure data sharing in clouds," IEEE Systems Journal, vol. 11, no. 2, pp. 395–404, 2015.

[17] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Computers & Security, vol. 72, pp. 1–12, 2018.

[18] U. M. Maurer, "Secret key agreement by public discussion from common information," IEEE transactions on information theory, vol. 39, no. 3, pp. 733–742, 1993.

[19] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," Mobile Networks and Applications, vol. 16, no. 6, pp. 683–694, 2011.

[20] X. Liu and W. Ma, "Cdaka: a provably-secure heterogeneous crossdomain authenticated key agreement protocol with symptoms-matching in tmis," Journal of medical systems, vol. 42, no. 8, p. 135, 2018.