International Conference on Advances in Materials, Computing and Communication Technologies
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Mutual Authentication and Key Agreement Scheme Based On Peer-To-Peer Cloud Computing

Mr. V S Siva Kumar, Mr. V Ramesh
Department of CSE , GIT College, Melvisaram, Tamil Nadu, India

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.

Index Terms—Cloud computing, data migration, elliptic curve, authentication, key agreement.

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. 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 Smartphone manufacturers are increasingly launching and deploying their own cloud computing services to provide users with convenient data storage services . 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 argued that the biggest challenge in cloud computing is the interoperability between clouds, and proposed a new approach for cloud portability. Binz et al. proposed a cloud motion framework that supports the migration of composite applications into or between clouds. In 2012, Shirazi et al designed a scheme to support data portability between cloud databases.

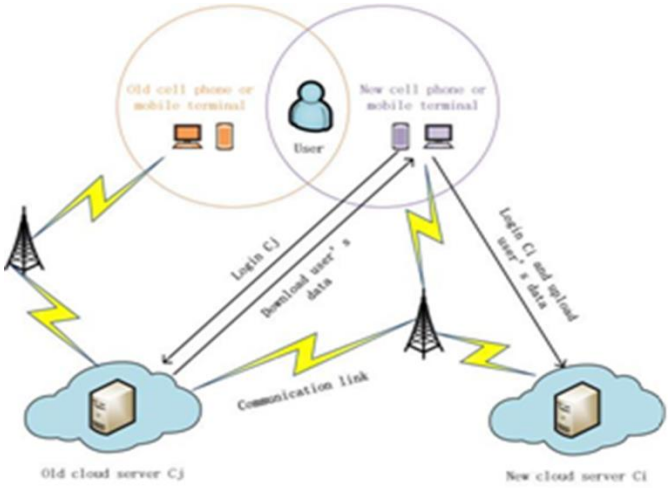


Fig. 1. Original data migration model

II. LITERATURE SURVEY

Title: OOABKS: Online/offline attribute-based encryption for keyword search in mobile cloud
Authors: Jie Cui, Yan Xu, Hong Zhong, Han Zhou
Year: 2019

Mobile cloud computing is a new computing method for mobile applications, which enables storage and computation migration from mobile users to resource-rich and powerful cloud server. More and more mobile phone users share their information through the mobile cloud. As the cloud server is not fully trusted, for security and privacy concerns, data owners usually encrypt their data before outsourcing them to the cloud server. In response to above questions, some attribute-based keyword search (ABKS) schemes have been proposed. However, the key generation, encryption and decryption for ABE take up a lot of computing resources in these schemes. In this paper, we propose an online/offline attribute-based keyword search scheme for mobile cloud (OOABKS). We use online/offline ABE technology and outsource ABE technology to reduce the online calculation cost and the local calculation cost of mobile users. And, we implement the fine-grained access control for the user. Security analysis demonstrates that our scheme can achieve trapdoor unlinkability, keyword security, data privacy security and search controllability. Efficiency analysis shows, in terms of functionalities and the computation overhead, OOABKS is more practical and efficient than existing approaches.

Title: AKSER: Attribute-based keyword search with efficient revocation in cloud computing
Authors: Jie Cui, Han Zhou, Hong Zhong , Yan Xu
Year: 2018

With the advent of cloud computing, it is becoming increasingly popular for data own- ers to outsource their data to public cloud servers while allowing indented data users to retrieve these data stored in the cloud. For security and privacy reasons, data owners

usu- ally encrypt their data prior to outsourcing to the cloud server. At the same time, users often need to find data related to specific keywords of interest, this motivates research on the searchable encryption technique. In this paper, we focus on a different, yet more challenging, scenario where the outsourced dataset can have contribution from multiple owners and are searchable by multiple users. Based on our research of attribute-based encryption (ABE), we propose an attribute-based keyword search with efficient revoca- tion scheme (AKSER). Our scheme is highly efficient in terms of user revocation and can achieve fine-grained authorization of the search under the distributed multiple-attribute authorized institution. Security analysis demonstrates that the proposed scheme AKSER can achieve keyword semantic security, keyword secrecy, trapdoor unlinkability, and collu- sion resistance.

Title: Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure

Authors: Khalid Mahmood, Xiong Li, Shehzad Ashraf Chaudhry, Husnain Naqvi

Year: 2018

The most vital concern in the realization of the Internet of Things (IoT) is to encounter the disparate communication systems and technologies. Interoperability solutions such as standards can help us to integrate plenty of diverse devices and their applications in an interoperable framework. Since Smart Grid is a non-trivial prevalent application of Edge computing under the umbrella of IoT. The Smart Grid furnishes communication through Internet Protocol to enable interoperability. However, IP-Based communication makes it vulnerable to serious security threats. Therefore, the secure information sharing among diverse communicating agents in the smart grid environments has become a vital concern. Specifically, to enable secure communication between the smart meter and utility, key management prior to authentication is the most critical task to do. Nowadays, several mechanisms have been introduced to establish secure communication within the emerging smart grid environment. Although, these protocols do not support smart meter anonymity and fail to offer reasonable security. In this paper, we use the identity-based signature to present an anonymous key agreement protocol for the Smart Grid infrastructure. This protocol enables the smart meters to get connected with utility control anonymously to avail the services provided by them. The smart meters realize this objective with the private key in the absence of trusted authority. The trusted authority is involved only during the registration phase The proposed protocol is verified and validated through random oracle model and automated tool ProVerif. Moreover, performance analysis is also observed to consolidate the reliability and efficiency of the proposed protocol.

III. EXISTING SYSTEM

A property-based proxy re-encryption scheme to enable users to achieve authorization in access control environments. However, Liang and Au pointed out that this scheme does not have Adaptive security and CCA security features. Sun et al. 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.

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.

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.

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.

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.

IV. 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

V. SYSTEM ARCHITECTURE

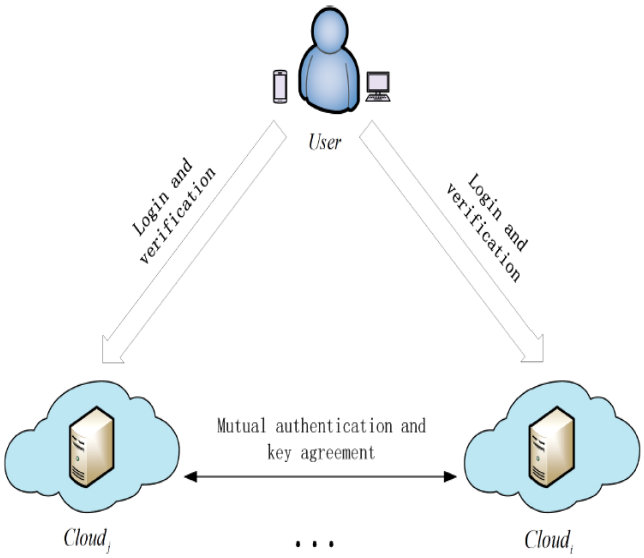


Fig. 2. System Architecture

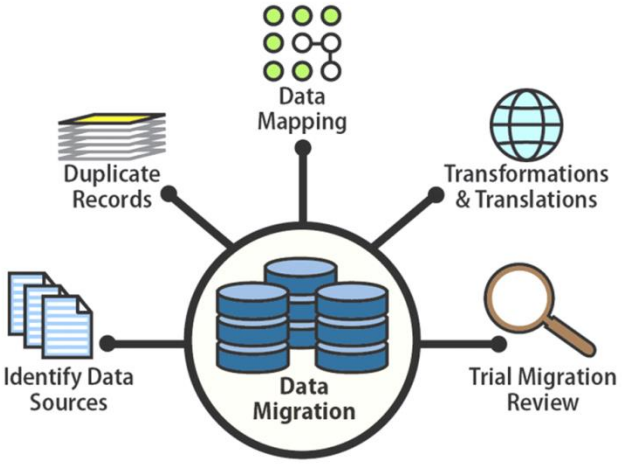
Migrating Applications. Application migration can mean moving data within an application, such as shifting from on-premises MS Office to Office 365 in the cloud. It can also mean replacing one application with a different one, such as moving from one accounting software to a new accounting platform from a different vendor.

Migrating to the Cloud. Cloud migration moves data from on-premises to a cloud, or from one cloud to another. This type of data movement is not the same as backing up to the cloud: data migration is a distinct project that moves data from the source environment to populate the new one.

Data Migration. Moving data between storage devices, locations, or systems. Includes subsets like quality assurance, cleansing, validation, and profiling.

Data Conversion. Transforms data from a legacy application to an updated or new application. The process is ETL: extract, transform, load.

Data Integration. Combines stored data residing in different systems to create a unified view and global analytics.



VI. DATA MIGRATION CHALLENGES AND RISKS

Data migration has the reputation of being risky and difficult. It's certainly not an easy process. It is time-consuming with many planning and implementation steps, and there is always some risk involved in projects of this magnitude.

Data Loss

During the data migration process, data loss can occur. On a small scale, this may not be a problem – no one may ever miss the data, or IT can restore files with backup. However, catastrophic data loss is different. In the case of a short-term connection failure, IT may not even know that the short-lived failure abruptly terminated the migration process. The missing data goes unnoticed until a user or application calls for it – and it's not there.

Compatibility issues

There are also compatibility issues in data transfer, such as changed operating systems and unexpected file formats; or confusion over user access rights between the source and target systems. Although the data is not formally lost, the business cannot access it in the target system.

Poor execution impacts the business

Many IT departments decide to do a migration project in-house to save money, or the management team decides it for them. But do-it-yourself data migration is rarely a good strategy. Migration is a risky business with major business implications, and requires extensive expert attention. A poorly run data migration project causes extended downtime, loses data, overruns deadlines, exceeds budgets, and results in sub-par performance.

VII. MOTIVATIONS

First, we realized that the study of data migration across cloud platforms has very important practical significance. The data migration issues between clouds has many unresolved potential problems. Existing efforts in the context of cloud data migration has obvious pitfalls that restrains their efficiencies. This is to say, further research into the context of cloud data migration is an important and timely necessity, especially to facility quicker and ease data transfer between the cloud servers after users change their smartphones. Secondly, in reality,

Through the rigorous security analysis, we show that our scheme achieves SK-security and strong credentials' privacy and prevents all well-known attacks including the impersonation attack and ephemeral secrets leakage attack. Furthermore, we simulate our scheme for the formal security analysis using the widely-accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool, and show that our scheme is secure against passive and active attacks including the replay and man-in-the-middle attacks. More security functionalities along with reduced computational costs for the mobile users make our scheme more appropriate for the practical applications as compared to Tsai–Lo's scheme and other related schemes. Finally, to demonstrate the practicality of the scheme, we evaluate the proposed scheme using the broadly-accepted NS-2 network simulator.

VIII. ACKNOWLEDGMENT

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.

IX. REFERENCES

[1]. C. I. network information center, "The 44th china statistical report on in-ternet 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 key-word 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 attribute-based 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 Inter-national 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 re-encryption with delegating capabilities," in Proceedings of the 4th In-ternational 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 attribute-based 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 identity-based 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 cross-domain authenticated key agreement protocol with symptoms-matching in tmis," Journal of medical systems, vol. 42, no. 8, p. 135, 2018.

[21]. J.-L. Tsai and N.-W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," IEEE systems journal, vol. 9, no. 3, pp. 805–815, 2015.

[22]. J. Xu, D. Zhang, L. Liu, and X. Li, "Dynamic authentication for cross-realm soa-based business processes," IEEE Transactions on services computing, vol. 5, no. 1, pp. 20–32, 2010.

[23]. A. Irshad, M. Sher, H. F. Ahmad, B. A. Alzahrani, S. A. Chaudhry, and R. Kumar, "An improved multi-server authentication scheme for distributed mobile cloud computing services." TIIS, vol. 10, no. 12, pp.5529–5552, 2016.

[24]. A. B. Amor, M. Abid, and A. Meddeb, "A privacy-preserving au-thentication scheme in an edge-fog environment," in 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA). IEEE, 2017, pp. 1225–1231.

[25]. V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," Future Generation Computer Systems, vol. 68, pp. 74–88, 2017.