Volume 4, Issue 10, October 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Secure Data Sharing Application for Dynamic Groups in the Cloud

Ms. Shrayu P. Pachgade, Asso. Prof. K. G. Bagde
Department of Computer Science and Engineering, H.V.P.M's college of Engg. & Tech.
Amravati University, India

Abstract: ***Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. But sharing data in a multi-owner manner while preserving data and identity privacy from an un-trusted cloud is still a challenging issue, due to the frequent change of the membership. Designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task. This task includes identity privacy, multi-owner issue and maintaining dynamic groups.To overcome these problems, I propose a secure multi-owner attribute authorities based data sharing scheme for dynamic groups in the cloud. The aim of my project is secure data sharing in a dynamic group where the there is no fixed Attribute authorities where as multi – owner attribute authorities scheme is possible. Key policy attribute-based encryption (KP-ABE) method is used to select dynamic AA (Attribute authorities) . By leveraging group signature , signed receipts and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. As the result the computation cost is reduced and storage overhead and encryption computation cost of our scheme are independent with the number of revoked users so the encryption cost is also reduced.***

Keywords: Cloud computing, data sharing, privacy-preserving, access control, dynamic groups.

I. INTRODUCTION

Cloud computing will play a major role in the future Internet of Services, enabling on-demand provisioning of applications, platforms, and computing infrastructures. However, the cloud community must address several technology challenges to turn this vision into reality. Specific issues relate to deploying future infrastructure-as-a-service clouds and include efficiently managing such clouds to deliver scalable and elastic service platforms on demand, developing cloud aggregation architectures and technologies that let cloud providers collaborate and interoperate, and improving cloud infrastructures' security, reliability, and energy efficiency. service elasticity resulting from clouds' ability to automatically scale services and infrastructures; cost reduction when infrastructure and platform sizes are adapted to service demands; pay-per-use models that let users pay only for actual resource consumption; improved time-to-market for services owing to reduced development and infrastructure deployment times; increased service availability and reliability resulting from the replication of service components and rapid deployment of new service instances; and cloud interoperability, which lets users deploy a service on multiple clouds, thus providing unlimited scalability and optimized service performance.

cloud providers should be able to deliver scalable, on-demand infrastructures (including network, compute, and storage elements) that satisfy the requirements for different types of elastic services and workloads. In particular, single infrastructure providers must support dynamic service provisioning; quality-of-service (QoS) and service-level agreement (SLA) negotiation; service scalability; service monitoring, billing, and payment;6 and context-aware services. It is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner , where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/ her part of data in the entire data file shared by the company.

To provide efficient service virtualization, cloud platforms should decouple the service interface from the implementation in a way that enables service providers to map services dynamically to resources. Security, privacy, and trust form a cross discipline that must be included in all aspects of the future Internet's design. Although cloud platforms and providers incorporate different mechanisms and technologies to guarantee the security and privacy of users' data and resources, significant potential for improvement exists regarding the authentication, authorization, and auditing mechanisms. Reliability, High availability will be a key concern. IT departments will worry about a loss of service should outages occur. Mission critical applications may not run in the cloud without strong availability guarantees.

Data Security, Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure. Authentication and access technologies become increasingly important Security Management, Providers must supply easy, visual controls to manage firewall and security settings for applications and runtime environments in the cloud.

Signature verification is a common behavioral biometric to identify human beings for purposes of verifying their identity. Signatures are particularly useful for identification of a particular person because each person's signature is highly unique, especially if the dynamic properties of the signature are considered in addition to the static features of the signature. Even if skilled forgers can accurately reproduce the shape of signatures, but itis unlikely that they can simultaneously reproduce the dynamic properties as well. Offline (Static): The input of offline signature verification system is the image of a signature and is useful in automatic verification of signatures found on bank checks and documents. Online (Dynamic): Signatures that are captured by data acquisition devices like pressure-sensitive tablets and webcam that extract dynamic features of a signature in addition to its shape (static), and can be used in real time applications like credit card transactions, protection of small personal devices (e.g. PDA), authorization of computer users for accessing sensitive data or programs, and authentication of individuals for access to physical devices or buildings. Why Online (Dynamic): Off-line signatures systems usually may have noise, because of scanning hardware or paper background, and contain less discriminative information since only the image of the signature is the input to the system. While genuine signatures of the same person may slightly change, the differences between a forgery and a genuine signatures may be difficult, which make automatic off-line signature verification be a very challenging pattern recognition problem. In addition, the difference in pen widths and unpredictable change in signature's aspect ratio are other difficulties of the problem. It is worth to notice the fact that even professional forensic examiners perform at about 70% of correct signature classification rate (genuine or forgery).Unlike offline, On-line signatures are more unique and difficult to forge than their counterparts are, since in addition to the shape information, dynamic features like speed, pressure, and capture time of each point on the signature trajectory are available to be involved in the classification. As a result, on-line signature verification is more reliable than the off-line.

II. LITERATURE REVIEW & RELATED WORK

To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task. In the existing System data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively.

Naga Raju et al. [1] proposed two novel techniques for secure distribution of the group key. The techniques proposed in this paper makes use of the hybrid key trees which allow the complete elimination of the secure channels for the distribution of the key material unlike many of the earlier proposed schemes, minimum storage requirements at each member, elimination of the chances of generation of week keys, less number of rounds and minimum computational overhead. But hybrid cloud, may be missing three key pieces: security, connectivity and portability.

Caronni et al. [2] proposed a series of novel approaches for achieving scalable security in IP multicast, providing privacy and authentication on a group-wide basis. They can be employed to efficiently secure multi-party applications where members of highly dynamic groups of arbitrary size may participate. Supporting dynamic groups implies that newly joining members must not be able to understand past group communications, and that leaving members may not follow future communications. Key changes are required for all group members when a leave or join occurs, which poses a problem if groups are large. The algorithms presented here require no trust in third parties, support either centralized or fully distributed management of keying material, and have low complexity. In the dynamic groups new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users

Tseng et al. [3] proposed one novel cloud storage construction enabling the management of searchable dynamic data for dynamic group collaboration. They make use of the attribute based encryption scheme (ABE) and public-key encryption with conjunctive keyword search (PECK) They also provide one practical example to demonstrate how our construction enables dynamic group collaboration by providing search-based retrieval and fine grained access control of dynamic data for enterprises. The main goal for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, this can be achieved only when user and server are in a trusted domain. But what if their domains are not trusted or not same? So, the new access control scheme that is 'Attribute Based Encryption (ABE)' scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided fine grained access control.

Re_k Molva et al. [4] proposed a new framework for multicast security based on distributed computation of security transforms by intermediate nodes. The involvement of intermediate nodes in the security process causes a new type of dependency between group membership and the topology of the multicast network. The containment of security exposures in large multicast groups is assured. The framework also assures both the scalability for large dynamic groups and the security of individual members. Two different key distribution protocols complying with the framework are introduced.

III. ANALYSIS OF PROBLEM

In the existing Systems, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems

because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Only the group manager can store and modify data in the cloud. The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed The proposed system, try to propose the security and performance of application. In this system, only authorized group members can,

1) Search/retrieve the group data and

2) Decrypt the retrieved group data stored in cloud storages. The employee who leaves the group or is revoked cannot retrieve or decrypt the stored data in cloud storages. Moreover, we evaluate the computation and communication costs in our design and conclude our design is effective and efficient for the enterprise users to share.

IV. CONCLUSION

The proposed system try to introduce the approach to achieve anonymity in storing data to the cloud with publicly-verifiable data-integrity in mind. System's approach decouples the anonymous protection mechanism from the provable data possession mechanism via the use of security mediator. The solution is not only minimizes the computation and bandwidth requirement of this mediator, but also minimizes the trust placed on it in terms of data privacy and identity privacy. The system try to provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

REFERENCES

[1] D. V. Naga Raju, Dr. V. Valli Kumari and Dr. K. V.S.V.N. Raju," Efficient Distribution of Conference Key for Dynamic Groups", International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010 1793-8201 (Access on dated:13-sep-2013)

[2] Germano Caronni , Marcel Waldvogel_ , Dan Sun_ , Bernhard Plattner_, "Efficient Security for Large and Dynamic Multicast Groups" First publ. in: Proceedings / Seventh IEEE Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '98), June 1998, Stanford, California, USA, pp. 376-383 (Access on dated:13-sep-2013)

[3] Fu-Kuo Tseng, and Rong-Jaye Chen, " Enabling Searchable Dynamic Data Management for Group Collaboration in Cloud Storages" (Access on dated:13-sep-2013)

[4] Re_k Molva, Alain Pannetrat, "Scalable Multicast Security in Dynamic Groups" (Access on dated:13-sep-2013)

[5] Boyang Wang †,‡, Sherman S.M. Chow §, Ming Li ‡, and Hui Li † † State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China ‡ "Storing Shared Data on the Cloud via Security-Mediator", 2013 IEEE 33rd International Conference on Distributed Computing Systems (Access on dated:13-sep-2013)

[6] M. Kavitha Margret, "Secure Policy Based Data Sharing for Dynamic Groups in the Cloud" ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) Volume 2, Issue 6, June 2013 (Access on dated:13-sep-2013)

[7] Zhang, J, Varadharajan, V and Mu, Y, "A novel dynamic key management scheme for secure Multicasting", ICON2003. The 11th IEEE International Conference on Networks, 28 September - 1 October 2003, 391-395. Copyright IEEE 2003. Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au (Access on dated:13-sep-2013)

[8] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan," Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013

[9] Zurich Christian Cachin, "Protocols for Secure Cloud Computing", IBM Research, April 2011(Access on dated:17-sep-2013)

[10] Mr. Anup R. Nimje , Prof. V. T. Gaikwad ,Prof. H. N. Datir, "Attribute-Based Encryption Techniques in Cloud Computing Security" International Journal of Computer Trends and Technology- volume4Issue3- 2013 ISSN:2231-2803 http://www.internationaljournalssrg.org Page 419 (Access on dated:17-sep-2013)

[11] Chunxuan Ye and Alex Reznik," Group Secret Key Generation Algorithms"

[12] Rafael Moreno-Vozmediano, Rubén S. Montero, and Ignacio M. Llorente, "Key Challenges in Cloud Computing Enabling the Future Internet of Services**"** (Access on dated:17-sep-2013)

