Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.364 – 370

RESEARCH ARTICLE

SECURITY ANALYSIS OF DYNAMIC GROUPS IN CLOUD

Ms. Shrayu P. Pachgade[1], Prof .K.G. Bagde[2]

[1]Second year student M.E

(Computer Science & Engineering)

[2]Associate Professor, Department of Computer Science & Engineering

H.V.P.M's College of Engineering & Technology Amravati, India

Email: - shrayup@gmail.com

Email: - karunabagde@rediffmail.com

ABSTRACT

The technology of distributed data processing in which some scalable information resources and capacities are provided as a service to multiple external customers through Internet technology. Cloud computing can and does mean different things to different people. The common characteristics most share are on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and dislocation of data from inside to outside the organization. While aspects of these characteristics have been realized to a certain extent, cloud computing remains a work in progress. This publication provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment. Recent advances have given rise to the popularity and success of cloud computing. However, when outsourcing the data and business application to a third party causes the security and privacy issues to become a critical concern. In this paper I proposed a secure data sharing scheme for the dynamic groups in the cloud. Also we analyze the security and privacy of our scheme with the proofs, algorithms and techniques.

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

© 2014, IJCSMC All Rights Reserved

I. INTRODUCTION

Cloud computing is not a technology but a model of provision and marketing IT services that meet certain characteristics. Cloud is all about computer services, not products: The infrastructure is shared. Multiple clients share a common technology platform and even a single application instance. The services are accessed on demand in units that vary by service**.** Units can be, for example, user, capacity, transaction or any combination thereof. Services are scalable**.** From the user's point of view, services are flexible; there are no limits to growth. The pricing model is by consumption. Instead of paying the fixed costs of a service sized to handle peak usage, you pay a variable cost per unit consumption (users, transactions, capacity, etc.) that is measured in time periods that can vary, such as hour or month.

Services can be accessed from anywhere in the world by multiple devices. The cloud model leads to basically two different kinds of clouds: private and public. The public clouds are those that offer IT services to any customer over the Internet. Private clouds offer IT services to a predefined group of customers, with access through Internet or private networks. You might have also heard about internal and external clouds. The former are a subgroup of the private clouds, and provide services within the same company or corporate group. The latter may be public or private and provide services to other companies.

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. 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

© 2014, IJCSMC All Rights Reserved

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.

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 it is unlikely that they can simultaneously reproduce the dynamic properties as well.

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.

© 2014, IJCSMC All Rights Reserved

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; supports 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

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.

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.

© 2014, IJCSMC All Rights Reserved

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 systems 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 systems try to provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

© 2014, IJCSMC All Rights Reserved

REFERENCES

[1] 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)

[2] 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)

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

[4] Fu-Kuo Tseng, and Rong-Jaye Chen, " Enabling Searchable Dynamic Data Management for Group Collaboration in Cloud Storages" (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)

© 2014, IJCSMC All Rights Reserved

[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)

© 2014, IJCSMC All Rights Reserved