ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A Dynamic Secure Group Sharing Framework in Public Cloud Computing – A Survey

Omkar Patil, Ashish Tonde, Chinmay Sapkale, Smita Bansod

Student Final Year, Dept. of Information Technology, SAKEC, Mumbai, Maharashtra, India

Student Final Year, Dept. of Information Technology, SAKEC, Mumbai, Maharashtra, India

Student Final Year, Dept. of Information Technology, SAKEC, Mumbai, Maharashtra, India

Assistant Professor, SAKEC, Mumbai, Maharashtra, India

ABSTRACT: With the popularity of group data sharing in public cloud computing, the privacy and security of group sharing data have become two major issues. The cloud provider cannot be treated as a trusted third party because of its semi-trust nature, and thus the traditional security models cannot be straightforwardly generalized into cloud based group sharing frameworks.

The system is proposed as novel secure group sharing framework for public cloud, which can effectively take advantage of the Cloud Servers' help but have no sensitive data being exposed to attackers and the cloud provider. The framework combines proxy signature, enhanced Tree-based group Diffie Hellman (TGDH) and proxy re-encryption together into a protocol. By applying the proxy signature technique, the group leader can effectively grant the privilege of group management to one or more chosen group members. The enhanced TGDH scheme enables the group to negotiate and update the group key pairs with the help of Cloud Servers, which does not require all of the group members been online all the time. By adopting proxy re-encryption, most computationally intensive operations can be delegated to Cloud Servers without disclosing any private information. Extensive security and performance analysis shows that or proposed scheme is highly efficient and satisfies the security requirements for public cloud based secure group sharing.

KEYWORDS: Cloud computing, cloud services, re-encryption,

I. INTRODUCTION

With the popularity of group data sharing in public cloud computing, the privacy and security of group sharing data have become two major issues. The cloud provider cannot be treated as a trusted third party because of its semi-trust nature, and thus the traditional security models cannot be straightforwardly generalized into cloud based group sharing frameworks. In this paper, we propose a novel secure group sharing framework for public cloud, which can effectively take advantage of the Cloud Servers' help but have no sensitive data being exposed to attackers and the cloud provider. The framework combines proxy signature, enhanced TGDH and proxy re-encryption together into a protocol. By applying the proxy signature technique, the group leader can effectively grant the privilege of group management to one or more chosen group members. The enhanced TGDH scheme enables the group to negotiate and update the group key pairs with the help of Cloud Servers, which does not require all of the group members been online all the time. By adopting proxy re-encryption, most computationally intensive operations can be delegated to Cloud Servers without disclosing any private information. Extensive security and performance analysis shows that our proposed scheme is highly efficient and satisfies the security requirements for public cloud based secure group sharing.

The demand of outsourcing data has greatly increased in the last decade. To satisfy the need for data storage and high performance computation, many cloud computing service providers have appeared, such as Amazon Simple Storage Service (Amazon S3), Google App Engine, Microsoft Azure, Dropbox and so on. There are two obvious advantages to store data in Cloud Servers: 1) The data owners save themselves out from the trouble of buying extra storage servers and hiring server management engineers; 2) It is easier for the data owner to share their data with intended recipients when the data is stored in the cloud. Despite of the above advantages of cloud storage, there still remain various

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

challenging obstacles, among which, the privacy and security of users' data have become two major issues. Traditionally, the data owner stores his/her data in the rusted servers, which are generally controlled by a fully trusted administrator. However, the cloud is usually maintained and managed by a semi-trusted third party (Cloud provider). As a result, traditional security storage technologies cannot be directly applied in the cloud storage scenario. While it is desirable for the data owner to share his/her private data with intended recipients, it presents an even more challenging problem since we have to make sure that except the intended recipients, nobody, including the cloud providers, can obtain any useful information from the encrypted data. The conventional approach to address the above mentioned problem is to use cryptographic encryption mechanisms, and store the encrypted data in the cloud.

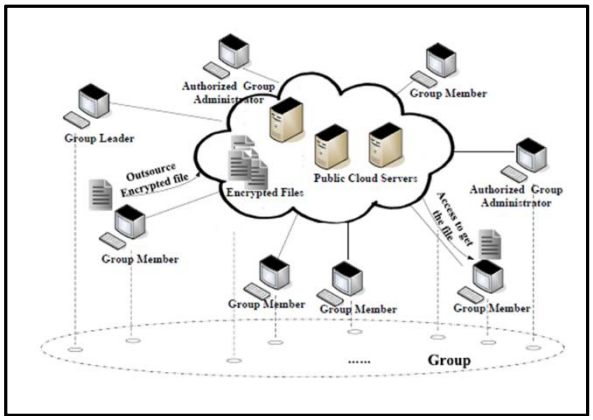

Figure 1: Cloud Scenario

As discussed with the increasing use of smart phones which leads to increasing use of vast varieties of applications. The developers of these applications will have the need to keep their particular applications up to date in order to keep their particular application in the top lists.

II. CLOUD COMPUTING

- Cloud computing comes in three forms: public clouds, private clouds, and hybrids clouds. Depending on the type of data you're working with, you'll want to compare public, private, and hybrid clouds in terms of the different levels of security and management required.

Public Clouds

A public cloud is one in which the services and infrastructure are provided off-site over the Internet. These clouds offer the greatest level of efficiency in shared resources; however, they are also more vulnerable than private clouds. A public cloud is the obvious choice when developing

- Workload for applications is used by lots of people, such as e-mail.
- To test and develop application code.
- SaaS (Software as a Service) applications from a vendor who has a well-implemented security strategy.
- Incremental capacity (the ability to add computer capacity for peak times).
- Collaborating projects.
- An ad-hoc software development project using a Platform as a Service (PaaS) offering cloud.

Private Clouds

A private cloud is one in which the services and infrastructure are maintained on a private network. These clouds offer the greatest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduces the cost savings. A private cloud is the obvious choice when developing

- Data and applications, to control and security are paramount.
- Applications for to conform strict security and data privacy issues.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

- Applications that has large enough data to run a next generation cloud data center efficiently and effectively on its own.

Hybrid Clouds

A hybrid cloud includes a variety of public and private options with multiple providers. By spreading things out over a hybrid cloud, you keep each aspect at your business in the most efficient environment possible. The downside is that you have to keep track of multiple different security platforms and ensure that all aspects of your business can communicate with each other. Hybrid environment is best to use when

- A SaaS application but is concerned about security. SaaS vendor can create a private cloud just for your company inside their firewall. They provide you with a virtual private network (VPN)for additional security.
- Services that are tailored for different vertical markets. A public cloud to interact with the clients but keep their data secured within a private cloud.

III.CLOUD STORAGE

Cloud storage is nowadays very popular storage system. Cloud storage is storing of data off-site to the physical storage which is maintained by third party. Cloud storage is saving of digital data in logical pool and physical storage spans multiple servers which are manage by third party. Third party is responsible for keeping data available and accessible and physical environment should be protected and running at all time. Instead of storing data to the hard drive or any other local storage, we save data to remote storage which is accessible from anywhere and anytime. It reduces efforts of carrying physical storage to everywhere. By using cloud storage we can access information from any computer through internet which omitted limitation of accessing information from same computer where it is stored. While considering data privacy, we cannot rely on traditional technique of authentication, because unexpected privilege escalation will expose all data. Solution is to encrypt data before uploading to the server with user's own key. Data sharing is again important functionality of cloud storage, because user can share data from anywhere and anytime to anyone. For example, organization may grant permission to access part of sensitive data to their employees. But challenging task is that how to share encrypted data. Traditional way is user can download the encrypted data from storage, decrypt that data and send it to share with others, but it loses the importance of cloud storage.

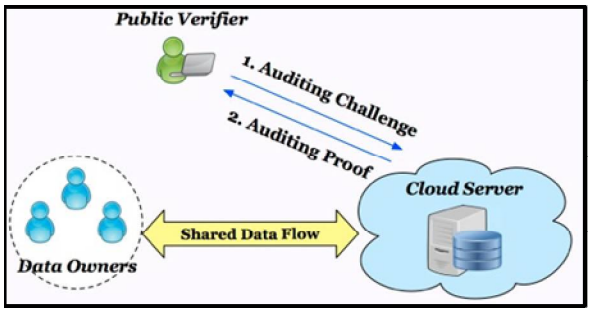

Figure 2: Cloud Storage Structure

Cryptography technique can be applied in a two major ways- one is symmetric key encryption and other is asymmetric key encryption. In symmetric key encryption, same keys are used for encryption and decryption. By contrast, in asymmetric key encryption different keys are used, public key for encryption and private key for decryption. Using asymmetric key encryption is more flexible for our approach. This can be illustrated by following example. Suppose Alice put all data on Box.com and she does not want to expose her data to everyone. Due to data leakage possibilities she does not trust on privacy mechanism provided by Box.com, so she encrypt all data before uploading to the server. If Bob ask her to share some data then Alice use share function of Box.com. But problem now is that how to share encrypted data. There are two severe ways: 1. Alice encrypt data with single secret key and share that secret key directly with the Bob. 2. Alice can encrypt data with distinct keys and send Bob corresponding keys to Bob via secure channel. In first approach, unwanted data also get expose to the Bob, which is inadequate. In second approach, no. of keys is as many as no. of shared

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

IV. CASE STUDY

The proposed system mainly consists of five phases: Group Initialization, Group Administration Privilege Management, Group Member Leaving and Joining (including Group Member Leaving, Group Member Joining and Group Administrator Leaving), Key Synchronizing, and Data Sharing Management. Obtaining storage and computing resource from the cloud provider, the group leader GL implements the phase of Group Initialization to initialize a binary tree and some related security information of the group. Then GL can unicast the private key of each leaf node to the associated group member under the protectionof encryption and signature. With the help of Cloud Servers' storage, each member can compute the group private key PrKG.
Relying on the proxy signature, the phase of Group Administration Privilege Management can help GL grant the group administration privilege to some specific group members.
Furthermore, we divide the phase of Group Member Leaving and Joining into three possible sub-phases:

i. Group Member Joining,
ii. Group Member Leaving
iii. Group Administrator

Leaving. Through the sub-phase of Group Member Joining, a group administrator and the new joining group member interact with each other to update security information of the group, including the group key pair PrKG and PuKG.
Forward Secrecy should be guaranteed when a group member joins, which ensures that the newly joined user can also access and decrypt the previously published data. Therefore, all the old digital envelopes used to protect session keys, which are generated to encrypted previously published data don't need to beupdated. When a group member leaves, his/her associated node is mandated by a group administrator. In the sub-phase of Group Member Leaving, the group administrator GA launches enhanced TGDH based group key updating and then generates a proxy re-encryption key from the version of group public key used in the existing digital envelopes to the new updated version.
Different from a general group member, a group administratorusually mandates more than one leaf node, and he/she knows all the secret keys of these leaf nodes. Therefore, when a group administrator leaves, another GA or GL should mandate all these leaf nodes, change the security keys, and update security information of the groupincluding the group private key. The proxy re-encryption implementation is like that used in the sub-phase of Group Member Leaving. With the algorithm of proxy re-encryption, Cloud Servers can update all existing digital envelopes to be encrypted under the new updated group public key.
Key Synchronizing is a key part of enhanced TGDH in our scheme. With the help of Cloud Servers, it makes temporarily offline group members can compute the current agreed group private key and other security information which needs to be synchronized. The phase of Data Sharing Management describes the method how to securely upload and download file in the group.

V. THE STRUCTURE

The application will provide all of the above that will help the developers to provide an effective and efficient application to the application users and will reduce their efforts otherwise which will help them improve the quality and overall product which will be served to the fellow users.
Cloud Computing is a vast topic and the above report does not give a high level introduction to it. It is certainly not possible in the limited space of a report to do justice to these technologies. What is in store for this technology in the near future? Well, Cloud Computing is leading the industry's endeavor to bank on this revolutionary technology.
The person using the cloud services is the actual user who will either create or join the group .Either he acts as a admin and controls the data transfer within the group as the size of the group increases he assigns a group leader on behalf of him to carry the same functions. The developer allows the user to send request to different groups and
Carries out encryption and decryption to the data uploaded and downloaded by the user.
Cloud Computing Brings Possibilities

i. Increases business responsiveness
ii. Accelerates creation of new services via rapid prototyping capabilities
iii. Reduces acquisition complexity via service oriented approach
iv. Uses IT resources efficiently via sharing and higher system utilization
v. Reduces energy consumption

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

vi. Handles new and emerging workloads
vii. Scales to extreme workloads quickly and easily
viii. Simplifies IT management
ix. Platform for collaboration and innovation
x. Cultivates skills for next generation workforce.

The proposed systems creates a group for sharing file on cloud. The security is providedto the sensitive data therefore the file sharing with the help of encryption and decryption is done on the cloud. The group leader can assign one or two admins for particular groupand can grant privileges. Invalid users and access are blocked because of third party authentication. The further scope of study is to make cloud provider itself as a trusted third party.

VI. CONCLUSION

Today, with such cloud-based interconnection seldom in evidence, cloud computing might be more accurately described as "sky computing," with many isolated clouds of services which IT customers must plug into individually. On the other hand, as virtualization and SOA permeate the enterprise, the idea of loosely coupled services running on an agile, scalable infrastructure should eventually make every enterprise a node in the cloud. It's a long-running trend with a far-out horizon. But among big metatrends, cloud computing is the hardest one to argue with in the long term.
Cloud Computing is a technology which took the software and business world by storm. The much deserved hype over it will continue for years to come.

REFERENCES

[1] Xiaohui Yu, Member, IEEE, Yang Liu, Member, IEEE, Jimmy Xiangji Huang, Member, IEEE, and Aijun An, Member, “Mining Online Reviews for Predicting Sales Performance: A Case Study in the Movie Domain” IEEE, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 24, NO. 4, APRIL 2012 pp 720-735
[2] https://en.wikipedia.org/wiki/Sentiment_analysis Source=Available.
[3] Chien-Liang Liu, Wen-Hoar Hsaio, Chia-Hoang Lee, Gen-Chi Lu, and Emery Jou, “Movie Rating and Review Summarization in Mobile Environment” IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 42, NO. 3, pp 397-408
[4] Shulong Tan, Yang Li, Huan Sun, Ziyu Guan, Xifeng Yan, Member “Interpreting the Public Sentiment Variations on Twitter”, IEEE, Jiajun Bu, Member, IEEE, Chun Chen, Member, IEEE, and Xiaofei He, Member, IEEE, pp 1158-1171
[5] Chien-Liang Liu, Wen-Hoar Hsaio, Chia-Hoang Lee, Gen-Chi Lu, and Emery Jou, “Movie Rating and Review Summarizationin Mobile Environment” IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 42, NO. 3, pp 397-408
[6] Shulong Tan, Yang Li, Huan Sun, Ziyu Guan, Xifeng Yan, Member “Interpreting the Public Sentiment Variations on Twitter”, IEEE, Jiajun Bu, Member, IEEE, Chun Chen, Member, IEEE, and Xiaofei He, Member, IEEE, pp 1158-1171.
[7] Shulong Tan, Yang Li, Huan Sun, Ziyu Guan, Xifeng Yan, Member“Interpreting the Public Sentiment Variations on Twitter”, IEEE, Jiajun Bu, Member, IEEE, Chun Chen, Member, IEEE, and Xiaofei He, Member, IEEE, pp 1158-1171
[8] AlenaNeviarouskaya and Masaki Aono “Sentiment Word Relations with Affect, Judgment, and Appreciation”, IEEE TRANSACTIONS ON AFFECTIVE COMPUTING, VOL. 4, NO. 4, pp 425-439
[9] Desheng Dash Wu, LijuanZheng, and David L. Olson “A Decision Support Approach for Online Stock Forum Sentiment Analysis”, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, VOL. 44, NO. 8, pp 1077-1088
[10] MyriamMunezero, CalkinSuero Montero, Member, IEEE, ErkkiSutinen, and John Pajunen, “Are They Different? Affect, Feeling, Emotion, Sentiment, and Opinion Detection in Text” pp 101-112
[11] AnindyaGhose and Panagiotis G. Ipeirotis, Member, IEEE, “Estimating the Helpfulness and Economic Impact of Product Reviews: Mining Text and Reviewer Characteristics” IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 23, NO. 10, pp 1498-1514