International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

A Private Cloud Data Sharing Using Secured Group Key

Devarakonda Krishna , Ch.Vengaiah & M.Aharonu
[1]Assistant Professor,CSE Department,St.Martins Engineering College,JNTUH
[2]Assistant Professor,CSE Department,Malla Reddy College of Engineering,JNTUH
[3]Assistant Professor,CSE Department,Malla Reddy College of Engineering,JNTUH

Abstract:

The authenticated group key transfer protocol is a new protocol for creating a secure communication between the private cloud and the number of cloud users. The private clouds maintained by the IT organizations for their own security reasons to avoid the security attacks. The security attacks can be considered as external attacks and internal attacks. The external attacks will be a passive attacks and active attacks and we have many solutions to avoid external attacks by applying encryption algorithms to our sensitive data. The internal attacks came from the internal users in IT organizations. This paper describes the secured communication in between the private cloud and the users of the cloud to avoid internal attacks in the IT organizations.

Keywords

Security, Cloud Computing, Authenticated Group Key Transfer Protocol

1. Introduction

Confidentiality represents one of the main goals of secure communication. It assures that the data are only accessible to authorized parties and it is achieved by encryption. In case of symmetric cryptography, the plaintext is encrypted using a secret key that the sender shares with the qualified receiver(s). Under the assumption that the system is secure, an entity that does not own the private key is unable to decrypt and thus the data remain hidden to unauthorized parties. The necessity of a (session) key establishment phase before the encrypted communication starts is immediate: it allows the authorized parties to share a common secret key that will be used for encryption. Key establishment protocols divide into key transfer protocols - a mutually trusted key generation center (KGC) selects a key and securely distributes it to the authorized parties - and key agreement protocols - all qualified parties are involved in the establishment of the secret key.

Security Goals Group key transfer protocols permit multiple users to share a common private key by using pre-established secure communication channels with a trusted KGC, which is responsible to generate and distribute the key. Each user registers to KGC for subscribing to the key distribution service and receives a long-term secret, which he will later use to recover the session keys. We will briefly describe next the main security goals that a group key transfer protocol must achieve: key freshness, key confidentiality, key authentication, entity authentication, known key security and forward secrecy. Key freshness ensures the parties that KGC generates a random key that has not been used before. Unlike key agreement protocols, the users are not involved in the key generation phase, so the trust assumption is mandatory. Key confidentiality means that a session key is available to authorized parties only. Adversaries are categorized into two types: insiders - that are qualified to recover the session key - and outsiders - that are unqualified to determine the session key. A protocol is susceptible to insider attacks if an insider is able to compute secret keys for sessions he is unauthorized for. Similarly, it is vulnerable to outsider attacks if an outsider is capable to reveal any session key. Key authentication assures the group members that the key is distributed by the trusted KGC and not by an attacker. It may also stand against a replay attack: no adversary can use a previous message originated from KGC to impose an already compromised session key. Entity authentication confirms the identity of the users involved in the protocol, so that an attacker cannot impersonate a qualified principal to the KGC. Known key security imposes that a compromised session key has no impact on the confidentiality of other session keys: even if an adversary somehow manages to obtain a session key, all the other past and future session keys remain hidden. Forward secrecy guarantees that even if a long-term secret is compromised, this has no impact on the secrecy of the previous session keys.

A secret sharing scheme is a method to split a secret into multiple shares, which are then securely distributed to the participants. The secret can be recovered only when the members of an authorized subset of participants combine their shares together. The set of all authorized subsets is called the access structure. The access structure of a (k, n) threshold secret sharing scheme consists of all sets whose cardinality is at least k. The access structure of an all-or-nothing secret sharing scheme contains only one element: the set of all participants. Generally, a secret sharing scheme has 3 phases: sharing (a dealer splits the secret into multiple parts, called shares), distribution (the dealer securely transmits the shares to the parties) and reconstruction (an authorized group of parties put their shares together to recover the secret).

Private Cloud

A private cloud is a particular model of cloud computing that involves a distinct and secure cloud

based environment in which only the specified client can operate.

As with other cloud models, private clouds will provide computing power as a service within a virtualized environment using an underlying pool of physical computing resource. However, under the private cloud model, the cloud (the pool of resource) is only accessible by a single organization, therefore providing that organization with greater control and privacy.

Features and Benefits of Private Clouds

HIGHER SECURITY AND PRIVACY

While public cloud services offer a certain level of security, private clouds are the more secure option. This is achieved using distinct pools of resource with access restricted to connections made from one organization's firewall, dedicated leased lines and on-site internal hosting

MORE CONTROL

As a private cloud is only accessible by a single organization, that organization will have the ability to configure and manage it in line with their needs to achieve a tailored network solution

COST AND ENERGY EFFICIENCY

Implementing a private cloud model can improve the allocation of resources within an organization by ensuring that the availability of resources to individual departments/business functions can directly and flexibly respond to their demand. They make more efficient use of the computing resource than traditional LANs and can also reduce an organization's carbon footprint

IMPROVED RELIABILITY

Even where resources (servers, networks etc.) are hosted internally, the creation of virtualized operating environments means that the network is more resilient to individual failures across the physical infrastructure. Virtual partitions can, for example, pull their resource from the remaining unaffected servers

CLOUD BURSTING

Some providers may offer the opportunity to employ cloud bursting, within a private cloud offering, in the event of spikes in demand. This service allows the provider to switch certain non-sensitive functions to a public cloud to free up more space in the private cloud for the sensitive functions that require it

Private Cloud Characteristics

Private cloud services can vary considerably and so it is hard to define what constitutes a private cloud from a technical aspect. Instead such services are usually categorized by the features that they offer to their client. Traits that characterize private clouds include:

Ring fencing of a cloud which has multiple clients accessing virtualized services, which all draw their resource from a distinct pool of physical computing. These may be hosted internally or externally and may be accessed across private leased lines or secure encrypted connections via public networks

Additional security, which is ideal for enterprises that need to store and process private data or carry out sensitive tasks. For example, a private cloud service could be utilized by a financial company that is required to store sensitive data internally and who will still want to benefit from some of the advantages of cloud computing, such as on-demand resource allocation.

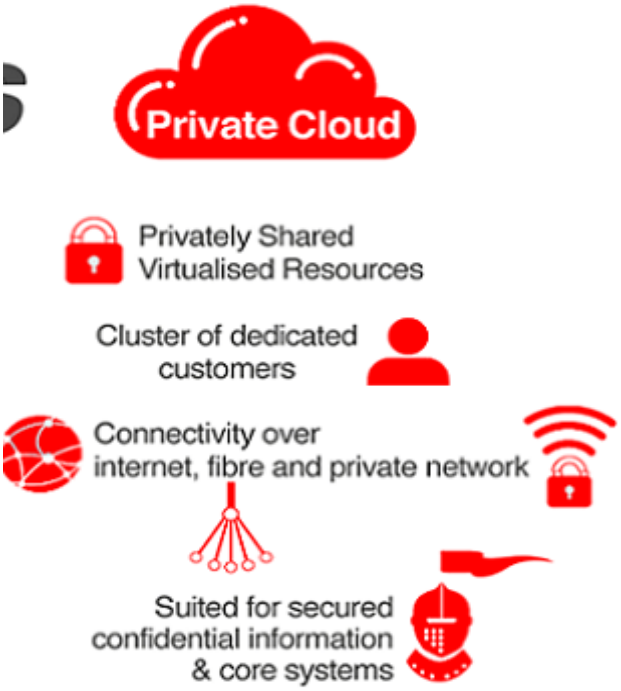


Figure 1: The architecture of a Private Cloud

2. Proposed System

Our authenticated group key transfer protocol consists of three processes: initialization of KGC, user registration, and group key generation and distribution. The detailed description is as follows: Initialization of KGC. The KGC randomly chooses two safe primes p and q (i.e., primes such that

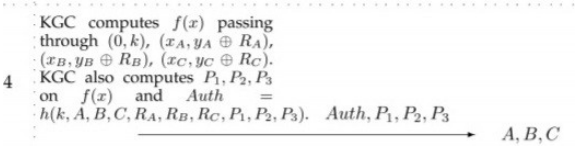
p1 =p-1/2 and q1=q-1/2 are also primes) and compute n=pq n is made publicly known.

User Registration: Each user is required to register at KGC for subscribing the key distribution service. The KGC keeps tracking all registered users and removing any unsubscribed users. During registration, KGC shares a secret (xi,yi) with each user Ui where xi , yi € Zn *

Group key generation and distribution: Upon receiving a group key generation request from any user, KGC needs to randomly selects a group key and access all shared secrets with group members. KGC needs to distribute this group key to all group members in a secure and authenticated manner. All communication between KGC and group members is in a broadcast channel. For example, we assume that a group consists of t members ,{U1,U2…….Ut}and shared secrets are (xi,yi) for i={1,2,3……..t} The key generation and distribution process contains five steps.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

Step 1: The initiator sends a key generation request to KGC with a list of group members as {U1,U2…….Ut}.
Step 2. KGC broadcasts the list of all participating members, {U1,U2…….Ut} as a response.
Step 3. Each participating group member needs to send a random challenge, Ri€ Zn * to KGC
Step 4 :



Step 5: Each participating user Ui Computes an interpolating polynomial f(x) passing through p1, p2, p3 and (xi, yi ≤Ri). Ui checks whether Auth= h(k, A, B,C, Ra,Rb,Rc,p1,p2,p3).

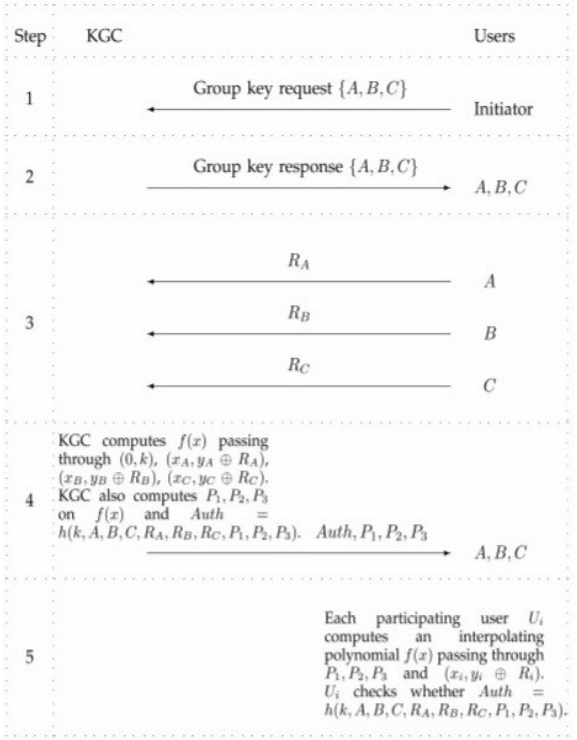


Figure 2: Group Key Transfer Protocol and steps

FileCloud:
FileCloud allows you to run your own private cloud storage and sync solution for your employees, customers and clients.
FileCloud offers the same features of public cloud services such as access from any device, file sync and easy sharing without moving your data or changing your IT infrastructure.
The unique selling proposition of FileCloud is Complete Control, Total Security, Unparalleled Branding, Easy Integration and Incredible ROI.

SECURE ACCESS, FILE SHARING, SYNC AND BACKUP

Access your files from anywhere. Share large files and folders with family, friends and colleagues. Setup public direct links so anyone can access the content or create a secure private share that only authorized people are allowed to access them. Backup and sync any number of folders.

WORKS UNIVERSALLY

Works on Windows, Linux, Mac and all major mobile phones and tablets including iPhone, iPad, Android and Windows Phone. Works on Raspberry Pi.

AUTOMATICALLY BACKUP PHOTOS FROM YOUR PHONE

Automatically backup photos/video from Android/iPhone to your Personal Cloud without user intervention.

HAVE YOUR OWN LOGO, BRANDING, IDENTITY

You can customize the branding to what you want to make the Tonido space your own. You can even run the service using your own custom domain name.

PRIVATE AND SECURE

By providing direct access to your files on your computer, you can rest assured that your data stays with you, providing complete privacy and control.

3. Conclusion

This paper represents the security in the private cloud by using filecloud. We have proposed an efficient group key transfer protocol based on secret sharing in the private clouds. Every user needs to register at a trusted KGC for using the clouds initially and pre-share a secret with KGC. KGC broadcasts group key information to all group members of clouds at once. The confidentiality of our group key distribution is information theoretically secure in the cloud. We provide group key authentication. Security analysis for possible attacks is included.

4. References

[1] S. Pearson, “Privacy, security and trust in cloud computing,” in Privacy and Security for Cloud Computing (S. Pearson and G. Yee, eds.), Computer Communications and Networks, pp. 3–42, Springer London, 2013.

[2] E. U. Directive, “95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data,” Official Journal of the EC, vol. 23, 1995.

[3] U. States., “Health insurance portability and accountability act of 1996 [micro form] : conference

report (to accompany h.r. 3103).” http://nla.gov.au/nla.catvn4117366, 1996.

[4] “Hypervisors, virtualization, and the cloud: Learn about hypervisors, system virtualization, and how it works in a cloud environment.” Retrieved June 2015.

[5] M. Portnoy, Virtualization Essentials. 1st ed., 2012.Alameda, CA, USA: SYBEX Inc.,

[6] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” tech. rep., July 2009.

[7] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology (Special Publication 500-292). USA: CreateSpace Independent Publishing Platform, 2012.

[8] R. Dua, A. Raja, and D. Kakadia, “Virtualization vs containerization to support paas,” in Cloud Engineering (IC2E), 2014 IEEE International Conference on, pp. 610–614, March 2014.

[9] M.O. Rabin, “Digitized Signatures and Public-Key Functions As Intractable As Factorization,” Technical Report LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[10] R.L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems,” Comm. ACM, vol. 21, pp. 120- 126, 1978.

[11] G. Saze, “Generation of Key Predistribution Schemes Using Secret Sharing Schemes,” Discrete Applied Math., vol. 128, pp. 239-249, 2003.

[12] A. Shamir, “How to Share a Secret,” Comm. ACM, vol. 22, no. 11, pp. 612- 613, 1979. [27] A.T. Sherman and D.A. McGrew, “Key Establishment in Large Dynamic Groups Using One-Way Function Trees,” IEEE Trans. Software Eng., vol. 29, no. 5, pp. 444-458, May 2003.

[13] D.G. Steer, L. Strawczynski, W. Diffie, and M.J. Wiener, “A Secure Audio Teleconference System,” Proc. Eighth Ann. Int’l Cryptology Conf. Advances in Cryptology (Crypto ’88), pp. 520-528, 1988.

[14] M. Steiner, G. Tsudik, and M. Waidner, “Diffie-Hellman Key Distribution Extended to Group Communication,” Proc. Third ACM Conf. Computer and Comm. Security (CCS ’96), pp. 31-37, 1996.