ISSN 2319 – 7595
Volume 8, No.2, March - April 2019
International Journal of Information Systems and Computer Sciences
Available Online at http://warse.org/IJISCS/static/pdf/file/ijiscs27822019.pdf
https://doi.org/10.30534/ijiscs/2019/27822019

SHARED OWNERSHIP IN THE CLOUD FOR BUSINESS COLLABORATION

Parvathy Radhakrishnan[1], Ranjima P.S[2], Renju Renjith[3], Shifamol P.H[4], Sruthy Emmanuel[5]
[1]Student, Mangalam College of Engineering, INDIA, sreelkmirdkn@gmail.com
[2] Student, Mangalam College of Engineering, INDIA, ranjimaps@gmail.com
[3] Student, Mangalam College of Engineering, INDIA, renju8421@gmail.com
[4] Student, Mangalam College of Engineering, INDIA, shifamolph@gmail.com
[5]Assistant Professor, Mangalam College of Engineering, INDIA, sruthy.emmanuel@mangalam.in

ABSTRACT

With expanding execution and scope of offering, an ever increasing number of endeavors are picking to take their administrations in the cloud. The general population who can share the documents and partake in conspiracy, so far they required all records or information to have an individual proprietor who can lineally make changes without the consent of others. This can be one of the main disadvantage in many co-operation. Here arise the perception of shared ownership.I n this paper, we are introducing the concept of shared ownership within a file or data access control model. Here we ensure the cloud security by the shared ownership model. All things considered, the model guarantee that all entrance grant in the cloud require the consent of a portion of the proprietors except if the client can't almost certainly do any alteration or access a document.

Key words: Cloud security, Distributed enforcement, Key generation, Shared ownership.

1.INTRODUCTION

Cloud computing-storing data and applications remotely rather than on your own premises-can cut IT costs dramatically and speed up your operations. The future of the cloud seems bright 59% of cloud workloads will be created from Software As A Service(SaaS).While these statistics are optimistic, we cannot ignore a few concerns that stifle cloud adoption efforts ,such as data ownership. Most people would be inclined to say that they still own data in the cloud. While they may be right in some sense, this is not always the case. Truthfully data ownership in the cloud is a complicated issue determined by both government and company policies data ownership in the cloud is not always retained.

In this paper we addressed the problems of single ownership of the cloud in a business project team. If all partners contribute their research efforts to the project ,then they may want to share the ownership over the collusion files so that all access decisions are agreed upon among the owners. A Single owner can modify or access the data or file without the concern of others. By distributed shared ownership, we means that, where access to files in a shared repository is granted if and only if t out of n owners separately support the grant decision. We are applying some criteria and formulate an algorithm to find the t data owners. Therefore, we introduce the Shared Ownership file access control Model(SOM) [1] in a business project. By introducing this in a project team system we can ensure security of data and in each file system can have more than one data owners and they collaboratively make decisions and accessing of data or files. Here we divide the business project team in to different modules, Admin, data owners, employees where data owners who can buy the cloud. Employees who get the key from the data owner can be the part of the project. If one of them want to access the data atleast out n data owners granted the permission, otherwise the person cannot read or write on that file. This is the main advantage of the shared ownership in business project team, by this we can ensure the security of the file system.

2.RELATED WORKS

The security and ownership in cloud storage is fairly termed in many papers. We concentrate more on works closely related to this paper. The term shared ownership is coined in [1]. Existing many systems use the scenario of individual file ownership, each file we stored in the cloud owner by an individual owner. Main limitation of individual ownership is a single owner can mishandle his privileges by lineally making changes. This paper addresses the problem of distributed implementation of shared ownership in general, not pointing any particular application based. For this, proposed a solution named commune by using shared ownership file access control model (SOM) [1]. It ensures that all access permits in the cloud require the support of co-owners. Another solution named comrade [1], grasps the block chain technology to get a general agreement on access control decisions. Comrade requires that the cloud should be able to transcribe access control decisions into storage access control rules. The idiom "shared ownership" was first defined in [2]. It formalize the shared ownership in a file access control model and propose the solution named commune which ensures that the files are accessible only when the n users grant permission.

The distributed models like web services involve frequent collaborations between elements with no previously established time relations. Each has their own authorization policies. To maintain such web applications, all the authorization decisions must be automated with respect to some human readable policies. Hence proposed a new authorization language secPAL [3] which improves the scalability, maintenance and availability.

The authorization problem in large-scale distributed system is addressed in [4]. The privacy protection, electronic commerce fields needs authorization decisions in a trust-management approach. This paper uses a logic-based language called Delegation Logic [4], to depict policies, requests in distributed authorization. This paper describes D1LP [4], a monotonic version of DL, which is declarative, expressive and implementable. The approach to implementing D1LP is based on compiling the D1LP program into ordinary logic programs (OLP). The transformation based approach make the OLP results easily accessible.

The language DKAL [5] which is a declarative language is used in distributed system. It is based on fixed-point and is more expressive than other languages. It has a targeted communication which ensures more security.For making a distributed system more secure, the concept of security language is introduced by John DeTreville [6] and is known as Binder [6]. It is a logic based language which encodes security statements as elements of logic programs in distributed system. Here operations such as certificates and delegation are simplified.

IPsec is the protocol suite for network layer security. It doesn't address how to control the traffic in security endpoints. This paper produces an effective policy management scheme for IPsec [7]. It is based on trust management principles.

A new mode of encryption is applied to block ciphers, called all-or-nothing encryption [8] where one must decrypt the entire cipher text before anyone can find even a single block of message. A packet transform [8] is used to encrypt.

3.PROPOSED SYSTEM

In this section, we are introducing the concept of distributed ownership in a business collaboration. The main modules that involved in the system are (a) shared data owners,(b) employees and (c) admin where data owners are the persons who buy the cloud from existing cloud platforms like Amazon S3, drop box etc and share the generated key to n different data owners. Employees who request for access the data file and get permission from at least t data owners, where t is the threshold owners less than n. Admin of the system take care of the authentication process of the user and data owner registration.

Overview of the proposed system is depicted in Figure 1 and Figure 2 and working of the modules are given.

(a) **Shared owners**

1. Data owners buy a new cloud and get key for the cloud.

2. Share the key with n data owners and request to other n data owners to be shared owner.

3. Shared owners accept or reject the ownership.

4. On acceptance of ownership,new a data owners get a key.

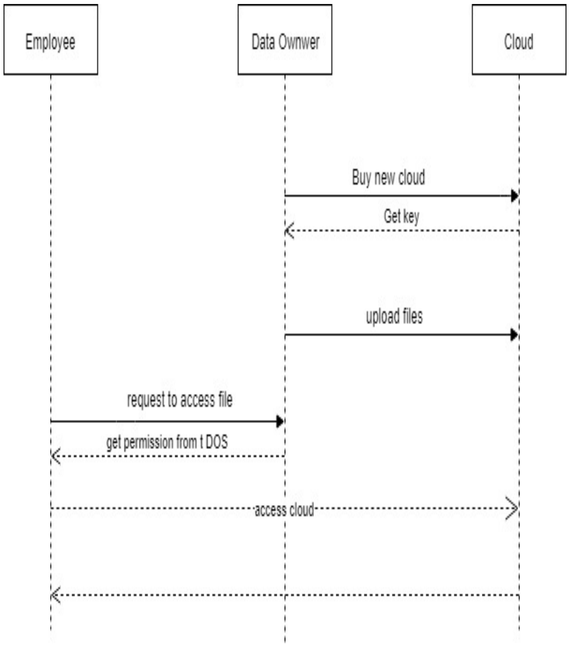

Figure 1: Sequential flow of system

(b) **Data access of employee**

1. Employee (who is part of a project) can view the name of files uploaded to the cloud. They request read/write permission of file.

2. All shared owners get notification on employee's request.

3. We set a threshold value t on the acceptance of t or more shared owners, the employee get read/write permission of file.

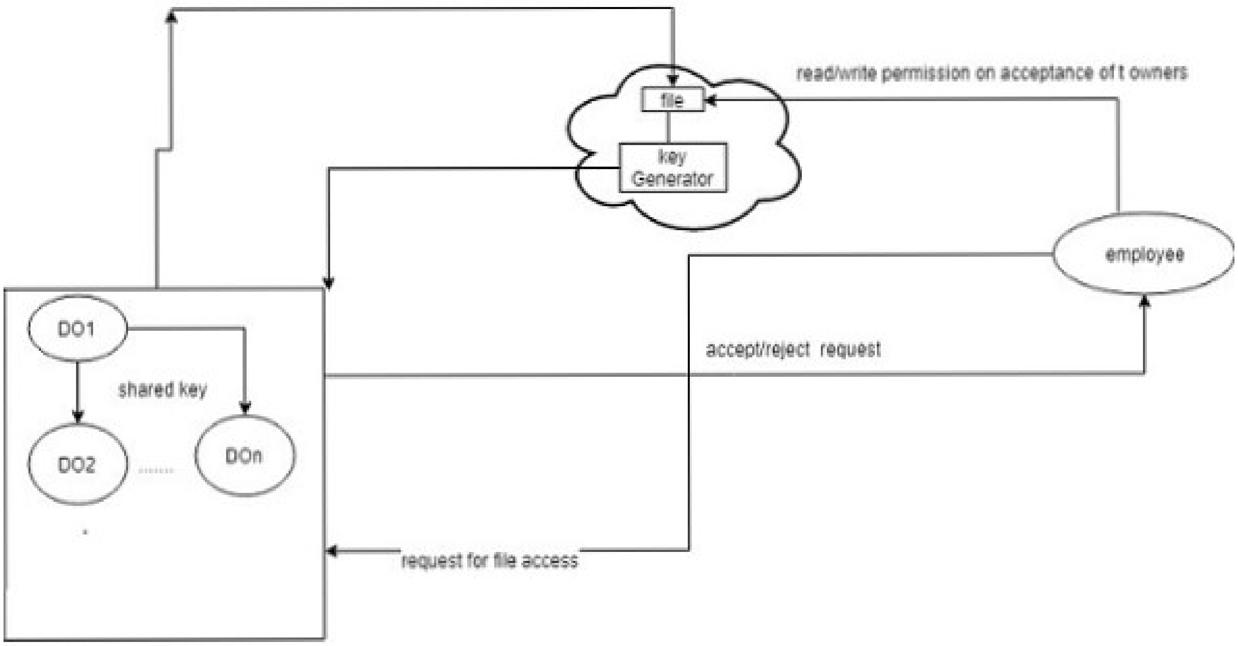

Figure 2: Architecture of Shared ownership in cloud

4.EXPERIMENTAL RESULTS

As cloud platform provide only individual ownership, here we implements the system which performs the idea of shared ownership. The person who owns the cloud platform shares the ownership with the people under the business collaboration. Those people together owns the cloud platform are the data owners. As per the system the access permission of a guest to the system is handled by t data owners. When a guest approaches for access permission the t data owners together make the decision whether to reject or accept. If rejected by data owners the guest is not able to access the cloud storage. After acceptance by the t data owners the guest employee get the right to modify the data. Employees works under a particular data owner and he has a dashboard containing list of data owners whom he shares his cloud and list of employees accessing the cloud.

5.CONCLUSION

Despite the fact that current cloud stages are utilized as shared stores, they don't bolster any thought of shared proprietorship. We think about this as an extreme constraint on the grounds that contributing gatherings cannot mutually choose how their assets are utilized. In this paper, we presented a novel idea of shared proprietorship and we depicted it through a formal access control model called SOM.

We at that point propose one conceivable instantiations of our proposed shared possession demonstrate. Our answer, depends on secure document dispersal and plot safe mystery sharing to guarantee that all entrance concedes in the cloud require the help of a concurred limit of owners. As such ,this can be utilized in existing skeptic mists without alterations to the platforms. And we are applying this mutual proprietorship thought into a business coordinated effort where the colleagues can similarly shares the cloud possession thus there won't be any acts of neglect thus security increments.

REFERENCES

[1] H. Ritzdorf, C. Soriente, G.O.Karame, S. Marinovic, D. Gruber and S.Capkun, "**Towards Shared Ownership in theCloud**,"in*Information Forensics and Security, IEEE transactions on*, 2018. https://doi.org/10.1109/TIFS.2018.2837648

[2] C. Soriente, G. O. Karame, H. Ritzdorf, S. Marinovic, and S. Capkun, "**Commune: Shared ownership in an agnostic cloud**," ser.SACMAT'15,2015. https://doi.org/10.1145/2752952.2752972

[3] M. Y. Becker, C. Fournet, and A. D. Gordon, "**SecPAL: Design and Semantics of a Decentralized Authorization Language**," in *Journal of Computer Security (JCS)*, 2010, pp. 597–643. https://doi.org/10.3233/JCS-2009-0364

[4] N. Li, B. N. Grosof, and J. Feigenbaum, "**Delegation logic: A Logic-based Approach to Distributed Authorization**," in *TISSEC*, 2003. https://doi.org/10.1145/605434.605438

[5] Y. Gurevich and I. Neeman, "**DKAL: Distributed-Knowledge Authorization Language**," in *CSF*'08.

[6] J. DeTreville, "**Binder, a Logic-based Security Language**," in *Proceedings of IEEE Symposium on Security and Privacy*, 2002, pp. 105–113.

[7] M. Blaze, J. Ioannidis, and A. D. Keromytis, "**Trust Management for IPsec**," in *ACM Transactions on Information and System Security (TISSEC)*, 2002. https://doi.org/10.1145/505586.505587

[8] R. L. Rivest, "**All-or-Nothing Encryption and the Package Transform**," in *International Workshop on Fast Software Encryption (FSE)*, 1997. https://doi.org/10.1007/BFb0052348