International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

A Data Security Scheme for Accessing Key In Cloud

Poreddy Malreddy[1] , K. Suresh[2], Alukunti Naresh[3], A. M. Rangaraj[4]
MCA Students[1,2 &3] , Associate Professor[4]
Department of Computer Application, Sri Venkateswara College of Engineering Technology Chittoor-India

Article Info

Publication Issue :
Volume 8, Issue 5
September-October-2022

Page Number : 229-234

Article History
Accepted: 02 Oct 2022
Published: 13 Oct 2022

ABSTRACT

In this work, we construct a key access management scheme that seamlessly transitions any hierarchical-like access policy to the digital medium. The proposed scheme allows any public cloud system to be used as a private cloud. We consider the data owner an entity consisting of several organization units. We provide a secure method for each user of this entity to access the public cloud from both inside and outside the company's network. The idea of our key access control scheme, which is based on Shamir's secret sharing algorithm and polynomial interpolation method, is suitable especially for hierarchical organizational structures. It offers a secure, flexible, and hierarchical key access mechanism for organizations utilizing mission-critical data. It also minimizes concerns about moving mission-critical data to the public cloud and ensures that only users with sufficient approvals from the same or higher privileged users can access the key by making use of the topological ordering of a directed graph, including self-loop. Main overheads such as public and private storage needs are reduced to a tolerable level, and the key derivation is computationally efficient. From a security perspective, our scheme is both resistant to collaboration attacks and provides key in distinguishability security. Since the key does not need to be held anywhere, the problem of a data breach based on key disclosure risk is also eliminated.

Keywords : RSA, DSaaS, CompaaS

I. INTRODUCTION

Digitizing several services increase demands on storage systems, large-scale computations, and hosting. In addition, advances in networking technology and administrative difficulties lead companies to outsource these services. A relatively new method called cloud computing enables users to access services from any location at any time [1]. In this work, we design a novel scheme to access a cloud storage system that runs on third parties' cloud infrastructure. The proposed method provides a secure scheme so that organizations requiring a higher level of security can use any public cloud infrastructure. Cloud computing also includes various service models [2] such as infrastructure as a service (IaaS), where a customer consumes a provider's computing, storage, and network resources; platform

as a service (PaaS) where a customer uses the provider's ready-made environments to develop, run, and manage specific applications; and software as a service (SaaS) where a customer runs software on the infrastructure of the providers. The work [3] adds a service model, which is called network as a service (NaaS), where the customers are provided transport connectivity and related network services. In addition, communication as a service (CaaS), compute as a service (CompaaS), data storage as a service (DSaaS) are defined in [4], and in this work, we focus on the DSaaS model. Cloud deployment models are categorized as private, public, community, and hybrid cloud [2]–[4]. The public cloud is defined to be a multi-tenant environment where the cloud computing environment is shared with several other users. The private cloud is a single-tenant environment where the hardware, storage, and network are dedicated to a single user. The community cloud is provided for private use by a specific consumer community and is owned, managed, and operated by the organizations in the community. In addition, the hybrid cloud is a composition of two or more distinct cloud deployment models. In a public cloud, generally, compliance, security, and privacy requirements can create an issue since the infrastructure. is managed and owned by a cloud storage provider that is located off-premise. The system can be accessed by any user who pays for the service. On the other hand, in the private cloud, these requirements do not generally create an issue since the infrastructure which is managed and owned by the customer is located on-premise. Many organizations are slowing down their overall public cloud adoption plans even though public cloud infrastructure ensures many advantages, especially in total cost [5]. In addition, they avoid public cloud due to concerns about reliability, availability, data integrity, and regulatory compliance [6], [7]. According to [8], the adoption obstacles for public cloud are availability, business continuity, data lock-in, data confidentiality, and auditability. The proposed scheme offers additional security layers to alleviate or minimize these concerns regarding transferring mission-critical data to a public cloud. The key features of our scheme designed for data owners desiring to consume DSaaS from the public cloud are extracted from the mathematical tool of Newton's interpolation. The proposed key access control scheme will be described for an organizational unit (OU) within a company which is basically one of the several organized groups that aim to accomplish a specific function in an organization. In other words, an organizational unit is one of the several vital business functions within an institution, and the key access control scheme works similarly for the others. There are various methods to design the organizational structure of an institution. However, it is common for all that all users within an institution do not have the same privileges. In other words, the users are grouped, and attributes are defined for each group so that users' accessibility to data is well maintained. The privileges and rights the users have and the unit or group they belong to are the most basic elements that determine whether the secret key K can be extracted or not. In this work, for simplicity, only one organization unit OU1 and groups Gi under this unit are considered. The group of the highest privileged users in this unit is denoted by G1, and the group of the second-highest privileged users is denoted by G2, and so on. The number of groups, Gi , is determined by the data owner according to the security policy. Due to the dynamic structure of an organization, the security policy of the company should be as flexible as possible. A user who is a member of a group Gi can also be a member of another group. The security policy and accessibility rights for users outside the network might not be the same for the users within the institution's network. The group structure for the organizational unit OU1 is similar to hierarchical, and the proposed key access control scheme is adapted accordingly. The proposed scheme provides a structure in which a user in the higher-level group has full rights to access the data to

users in the lower-level groups when the pre-determined conditions are met. Figure 1 depicts an example of pre-determined conditions in the organizational structure defined by the data owner.

II. RELATED WORKS

L. Zhou, V. Varadharajan, and M. Hitchens: Cloud data storage has provided significant benefits by allowing users to store massive amount of data on demand in a cost-effective manner. To protect the privacy of data stored in the cloud, cryptographic role-based access control (RBAC) schemes have been developed to ensure that the data can only be accessed by those who are allowed by access policies. However, these cryptographic approaches do not address the issues of trust. In this paper, we propose trust models to reason about and to improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust models provide an approach for the owners and roles to determine the trustworthiness of individual roles and users, respectively, in the RBAC system. The proposed trust models consider role inheritance and hierarchy in the evaluation of trustworthiness of roles. We present a design of a trust-based cloud storage system, which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes. We have also considered practical application scenarios and illustrated how the trust evaluations can be used to reduce the risks and to enhance the quality of decision making by data owners and roles of cloud storage service.

J. Mackinnon, P. D. Taylor, H. Meijer, and S. G. Akl: A cryptographic scheme for controlling access to information within a group of users organized in a hierarchy was proposed by Akl and Taylor (1983). The scheme enables a user at some level to compute from his own cryptographic key the keys of the users below him in the organization. In such a system there exists the possibility of two users collaborating to compute a key to which they are not entitled. The authors formulate a condition which prevents such cooperative attacks and characterizes all key assignments which satisfy the condition. The key generation algorithm of the cryptographic scheme is infeasible when there is a large number of users. The authors discuss other algorithms and their feasibility.

C. Chang, R.-J. Hwang, and T.-C. Wu: A key assignment scheme is a cryptographic technique for implementing an information flow policy, sometimes known as hierarchical access control. All the research to date on key assignment schemes has focused on particular encryption techniques rather than an analysis of what features are required of such a scheme. To remedy this we propose a family of generic key assignment schemes and compare their respective advantages. We note that every scheme in the literature is simply an instance of one of our generic schemes. We then conduct an analysis of the Akl-Taylor scheme and propose a number of improvements. We also demonstrate that many of the criticisms that have been made of this scheme in respect of key udpates are unfounded. Finally, exploiting the deeper understanding we have acquired of key assignment schemes, we introduce a technique for exploiting the respective advantages of different schemes.

P. D'Arco, A. De Santis, A. L. Ferrara, and B. Masucci: In 1983, Akl and Taylor [Cryptographic solution to a problem of access control in a hierarchy, ACM Transactions on Computer Systems 1 (3) (1983) 239–248] first suggested the use of cryptographic techniques to enforce access control in hierarchical structures. Due to its simplicity and versatility, the scheme has been used, for more than twenty years, to implement access control in several different domains, including mobile agent environments and XML documents. However, despite its use over time, the scheme has never been fully analyzed with respect to security and efficiency requirements. In this paper we provide new results on the Akl–Taylor scheme and its variants. More precisely:

- We provide a rigorous analysis of the Akl–Taylor scheme. We consider different key assignment strategies and prove that the corresponding schemes are secure against key recovery.
- We show how to obtain different tradeoffs between the amount of public information and the number of steps required to perform key derivation in the proposed schemes. • We also look at the MacKinnon et al. and Harn and Lin schemes and prove they are secure against key recovery.
- We describe an Akl–Taylor based key assignment scheme with time-dependent constraints and prove the scheme efficient, flexible and secure.
- We propose a general construction, which is of independent interest, yielding a key assignment scheme offering security w.r.t. key indistinguishability, given any key assignment scheme which guarantees security against key recovery.
- Finally, we show how to use our construction, along with our assignment strategies and tradeoffs, to obtain an Akl–Taylor scheme, secure w.r.t. key indistinguishability, requiring a constant amount of public information.

H.-Y. Chen: The access privileges in distributed systems can be effectively organized as a hierarchical tree that consists of distinct classes. A hierarchical time-bound key assignment scheme is to assign distinct cryptographic keys to distinct classes according to their privileges so that users from a higher class can use their class key to derive the keys of lower classes, and the keys are different for each time period; therefore, key derivation is constrained by both the class relation and the time period. We propose, based on a tamper-resistant device, a new time-bound key assignment scheme that greatly improves the computational performance and reduces the implementation cost.

A. Shamir: In this paper we show how to divide data D into n pieces in such a way that D is easily reconstruct able from any k pieces, but even complete knowledge of k - 1 pieces reveals absolutely no information about D. This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces.

III. METHODOLOGY

Proposed system:

In proposed system we are using private cloud. The private cloud is a single-tenant environment where the hardware, storage, and network are dedicated to a single user. The community cloud is provided for private use by a specific consumer community and is owned, managed, and operated by the organizations in the community.

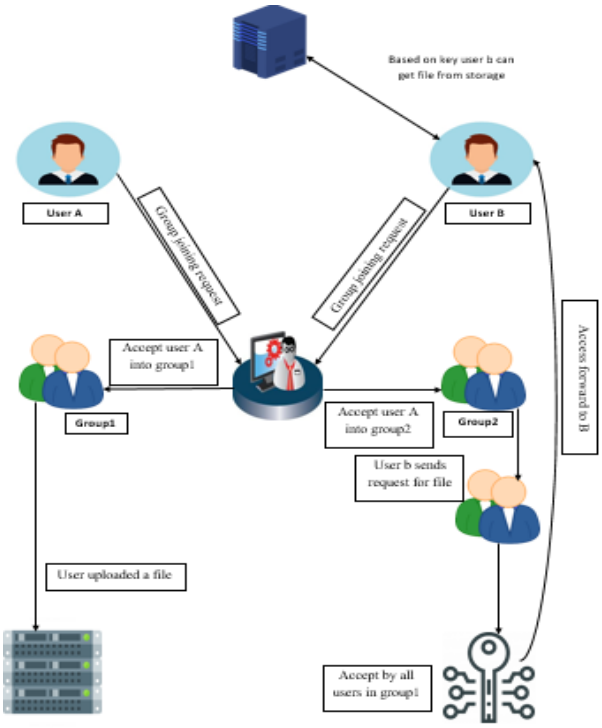


Figure 1 : Fake reviews dataset block diagram

IV. IMPLEMENTATION

Shamir's Secret Sharing Algorithm:

Shamir's Secret Sharing (SSS) is a key distribution algorithm. It is named for the well-known Israeli cryptographer Adi Shamir who co-invented the Rivest–Shamir–Adleman (RSA) algorithm.

SSS divides a secret, such as a crypto key, into parts called shares. The shares are distributed to a group of people who are parties to the conversation. The parts of the secret are brought together to reconstruct the secret, but an important feature of Shamir's Secret Sharing is that the total number of shares is not needed to reconstruct the secret. A number less than the total number, called the threshold, is required. This helps avoid failures in decrypting the closely-held information should just one or a few parties be unavailable.

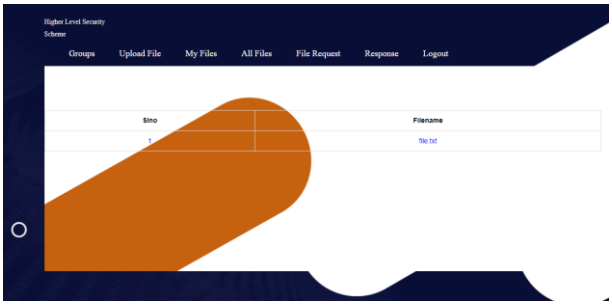
SSS is practical in its solution to the key-sharing problems many arrangements face, and is therefore usually used to secure the keys to something that is encrypted or secure using other tools or algorithms. A simple illustration of SSS is that of a vault that only a corporate board may access. The passcode is encrypted by SSS, so a quorum (threshold) of board members is needed to authorize the display or release of the vault passcode. If a board member is traveling, but the threshold is met, SSS still allows for a reasonable assurance that the vault is secure.

V. RESULTS AND DISCUSSION

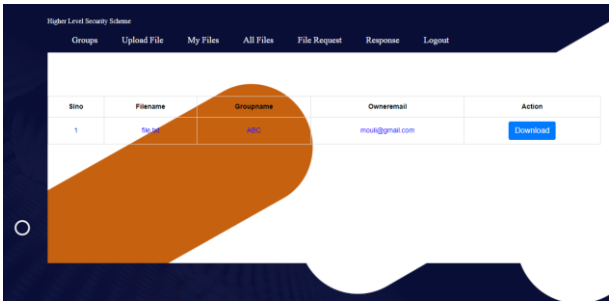
The following images will visually depict the process of our project.

User login: In this login page, User will login into the system using registered details.

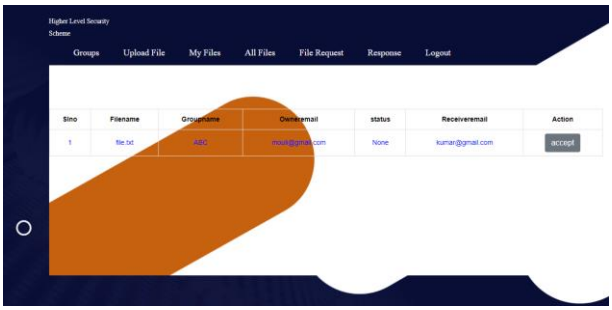
Upload file: In this page, User can upload files in the group.



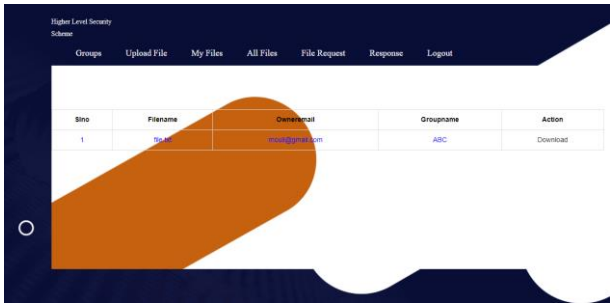
My files: In this page, the user can see his/her uploaded file after uploading the file into group.



All files: This page contains all the files uploaded by users and CSP in the group.



File request: In this page, the user can send a request to CSP to download the file was uploaded by CSP.



Response file: This is the file we can see, after a person added in the group.

VI. Conclusion

The proposed key access control scheme provides a computationally efficient method for key derivation. The proposed scheme provides both the private cloud security and the functionality, accessibility, and cost savings of the public cloud. With the use of the public cloud by companies, other advantages such as the reliability of the public cloud and the minimum maintenance and management requirements are obtained.

VII. REFERENCES

[1]. S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," ACM Trans. Comput. Syst., vol. 1, no. 3, pp. 239–248, 1983.

[2]. S. J. Mackinnon, P. D. Taylor, H. Meijer, and S. G. Akl, "An optimal algorithm for assigning cryptographic keys to control access in a hierarchy," IEEE Trans. Comput., vol. C-34, no. 9, pp. 797–802, Sep. 1985.

[3]. R. S. Sandhu, "Cryptographic implementation of a tree hierarchy for access control," Inf. Process. Lett., vol. 27, no. 2, pp. 95–98, 1988.

[4]. L. Harn and H.-Y. Lin, "A cryptographic key generation scheme for multilevel data security," Comput. Secur., vol. 9, no. 6, pp. 539–546, Oct. 1990.

[5]. C.-C. Chang, R.-J. Hwang, and T.-C. Wu, "Cryptographic key assignment scheme for access control in a hierarchy," Inf. Syst., vol. 17, no. 3, pp. 243–247, May 1992.

[6]. H. T. Liaw, S. J. Wang, and C. L. Lei, "A dynamic cryptographic key assignment scheme in a tree structure," Comput. Math. Appl., vol. 25, no. 6, pp. 109–114, Mar. 1993.

[7]. M. S. Hwang, C. C. Chang, and W. P. Yang, "Modified Chang-Hwang-Wu access control scheme," Electron. Lett., vol. 29, no. 24, pp. 2095–2096, 1993.

[8]. H.-T. Liaw and C.-L. Lei, "An optimal algorithm to assign cryptographic keys in a tree structure for access control," BIT, vol. 33, no. 1, pp. 46–56, Mar. 1993.

[9]. H. Min-Shiang, "A cryptographic key assignment scheme in a hierarchy for access control," Math. Comput. Model., vol. 26, no. 2, pp. 27–31, Jul. 1997.

[10]. P. D'Arco, A. De Santis, A. L. Ferrara, and B. Masucci, "Variations on a theme by Akl and Taylor: Security and tradeoffs," Theron. Comput. Sci., vol. 411, no. 1, pp. 213–227, 2010.

[11]. W.-G. Tzeng, "A time-bound cryptographic key assignment scheme for access control in a hierarchy," IEEE Trans. Knowl. Data Eng., vol. 14,no. 1, pp. 182–188, Aug. 2002.

Cite this article as :

Poreddy Malreddy, K. Suresh, Alukunti Naresh, A. M. Rangaraj, "A Data Security Scheme for Accessing Key In Cloud ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 5, pp. 229-234, September-October 2022.

Journal URL : https://ijsrcseit.com/CSEIT228544