INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 9, Issue 2 - V9I2-1165)
Available online at: https://www.ijariit.com

Advanced key access security system on cloud computing

Choragudi Sasidhar
csasidhar.aits@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

Narreddy Pallavi
narreddypallavi@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

Sreeramdasu Pravalika
sriramdasupravalika@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

Palagiri Manoj Kumar Reddy
manojpalagiri0926@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

Yerragudi Sandeep
sandeepsandy64119@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

ABSTRACT

In this study, we create a system for managing key access that translates any access control policies with a hierarchical system to digital media. The given approach can be applied to any cloud infrastructure system as a private cloud. We consider the data owner to be a composite organizational entity. Every user of this organization has a secure way to connect to the public cloud within as well as outside the corporate servers. Our key access control mechanism, which is based upon Shamir's secret image-sharing method and the polynomials interpolation technique, is particularly well suited for tiered organizational structures. It offers a hierarchy, secure, and flexible key access solution for organizations handling mission-critical data. Moreover, it always concerns about moving quest information into the public cloud by using the topology order of shapes the way, including self-loop, and making sure that only individuals with The Keys can be accessible with enough permission from similarly privileged users or above. A significant overhead, such as the need for both public and private storage, is reduced to a manageable level by the computationally efficient key derivation. Our solution provides crucial security that can be distinguished from other systems as well as resistance to group attacks. In addition to removing the chance of a data breach caused by key exposure, the fact that the key is not required to be kept elsewhere also eliminates this necessity.

Keywords: *Cloud Security, Hierarchical, Interpolation, Key Access, Key Assignment, Secret Sharing*

1. INTRODUCTION

As more services get digitalized, there is a rise in the demand for hosting, massive compute, and storage systems. These services are also outsourced by businesses as a result of administrative difficulties and improvements in networking technology. Because to a relatively new method known as cloud computing [1], consumers may utilize services from every location at any time. In this paper, we develop a novel approach of access an online storage system that makes use of other people's cloud computing resources. The structured in the following of the proposed method dimension of organizational that require a higher level of security to use any publicly accessible cloud infrastructure. In addition, a number of service models fall under the category of cloud technology infrastructure as a service (IaaS), in which a customer uses a company's computing, storage, and shared network; platform as a service (PaaS), in which a customer makes use of the provider's pre-built climates to develop, run, and manage specific applications and software as a service (SaaS), in which a client uses the rail of the providers to run software.

The work introduces a new service model called Network as a Services (NaaS), which enables the provision of transportation networks and related network functions to customers. Moreover, describes data storage that is a service, computing as a service, and communications as a provider (CaaS) (DSaaS). We focus on the DSaaS model in this study. There are various cloud deployment models, including private, public, shared, and hybrid clouds [2]–[4]. Users who share a common cloud computing environment are referred to as being in the "public cloud," which is a multi-tenant environment. In a cloud infrastructure, which is a solitary environment, one user has the exclusive access to hardware, storage, and network. The community cloud is held, controlled, and operated by the member organizations and is made accessible to an exclusive consumer community for personal usage. Two or more diverse cloud deployment methodologies make up the hybrid cloud as well. Due to the fact that the infrastructure is managed and owned by a provider of cloud storage with an off-site location, conformance, safety, and privacy requirements may prove

difficult in a public cloud. Access to the system is available to anyone who pays for the service. Yet in the private cloud, these criteria are often not an issue so because customer oversees and owns the equipment, which is located on-premises. Several businesses are delaying their plans to use public cloud infrastructure, regardless of the fact that it has many benefits, especially in terms of overall cost. The reliability, accessibility, data protection, and regulatory compliance of public clouds are other concerns which discourage individuals form them. identifies the main barriers to the use of public clouds as availability, continuity planning, built security, data confidentiality, and auditability.

Further security measures are included in the suggested approach to assuage or lessen these concerns about shifting quest data to a cloud platform. The core ideas of our solution, which is designed for involved parties interested in employing DSaaS from a cloud platform, are derived from Newton's interpolation. The suggested key access control mechanism will be focused on a business's organizational unit (OU). In essence, an OU is just one of many regarding group that have been established within an organization to carry out certain tasks. In other terms, an organization is one of many important business processes carried out by a company, while the rest are all governed by the same essential access control system. A multitude of techniques can be used to create an institution's organizational structure. However, it is usual for different users to have different access levels within a same institution. Users are categorized, and attributes are set up for each group, to ensure that the administration of users access to data is done properly. The users' rights and privileges in addition to the unit or organization they are a part of are the most important variables that determine the possibility that the private key K can be recovered. Only one organization unit, OU1, as well as the groups Gi that fall under it are considered in this work in order to maintain simplicity.

The user group in this group with the greatest privileges is designated as G1, followed by the group with the next-highest privileges, G2, and so on. The data owner determines how several groups, Gi, there will be according on the security policy. A security strategy must be as adaptive as possible given the changing structure of the organization. Users who are a part of the group Gi are also permitted to be members of other groups. Users within the institution's network may not have the same accessibility or security policies as users outside of the network. The suggested key control system has indeed been modified because the organization OU1 has an organizational structure that is similar to a hierarchical one. The proposed scheme offers a framework where an users in the association. the association has absolute authority to retrieve the information to customers in the lesser group when the predetermined requirements are met. In the management structure which the data owner has designated, predetermined circumstances are shown in Figure 1.

2. LITERATURE SURVEY

This capability for users to store vast volumes of data on request and at a decent cost is shown to offer several benefits in this article. The confidentiality of information kept in the cloud is protected through the use of crypto role-based network access (RBAC) techniques, which ensure that the information can only be viewed by those who are authorized by access restrictions. However, trust-related problems aren't solved by these cryptographic methods. In this study, we provide trust models for assessing and boosting the safety of data stored on cloud storing systems that make use of cryptographic RBAC approaches. The trust models can be used by the owners and roles of the RBAC system to assess the dependability of certain roles or users, respectively. The proposed models consider role transmission and hierarchy when assessing the integrity of a position. We discuss the design of a confidence cloud storage system to show how trust concepts can be incorporated into a system that uses cryptographic RBAC techniques. As well, we considered real-world possible applications and showed how trust evaluations may be used to reduce risks and raise the standard of decision-making by involved parties and roles using cloud storage services.

In this article, Akl and Taylor developed a cryptographic method for limiting information availability among an user base organized in a hierarchical (1983). With just his own cryptographic key, a user can at some level in the system find out the keys of users who are below him inside the organizational hierarchy. With such a setup, two users could cooperate to calculate a key that they are not allowed to use. The authors outline all key assignments that satisfy the requirement as well as a condition that prohibits these coordinated attacks. The key generation algorithm of the cryptographic scheme becomes difficult if there is many users. The authors discuss the application of several algorithms.

This article, sometimes referred to as a data - flow policy, a key allocation scheme is a cryptographic technique for implementing hierarchical access control. Up to now, there has been no analysis of the features that have to be part of a key assignment scheme; instead, all research has focused on specific encryption techniques. We propose a family of general key assignment strategies to address this and compare the benefits of each scheme separately. We stress that each and every plan in the literature is really an example of a single of our general schemes. Eventually, after examining the Akl-Taylor method, we suggest numerous changes. We also show that a lot of the objections of this approach raised in regard to fundamental changes are unfounded. Finally, building on our improved understanding of significant assignment schemes, we present a way for utilizing the distinctive advantages of diverse schemes.

In this essay, Akl and Taylor made the initial recommendation to use cryptographic methods to impose network access in hierarchical structures in 1983 [Data encryption solution to problems of network access in a power structure, ACM Transfers on Computer Networks 1 (3) (1983) 239-248]. Due to the method's adaptability and simplicity, access control has been created using it for and over twenty years in a variety of domains, including XML documents and mobile agent environments. Although the plan has been in operation for a long, it has never been fully investigated in terms of safety and efficiency requirements. In this paper, we provide recent results on the Akl-Taylor framework and associated systems. To put it more precise

I provide a thorough assessment of the Akl-Taylor concept. Several more key assignment techniques are taken into consideration,

and we show that the corresponding computers are resistant to secret recovery.

In the proposed approach, they show various tradeoff between the quantity of information that is publicly accessible and the amount of steps needed for completing key derivation in the proposed approaches. We also look at and show how the public key encryption security of the system was developed by Mack & al and Harn and Lin.

We describe a moment key assignment methodology based on Akl-Taylor and show how fast, flexible, and secure it is.

We offer a generic structure that is of autonomous interest and produces a key assignment scheme that delivers security with regard to key indistinguishability for any key allocation scheme that guarantees security against key recovery.

In our final part, we show how to integrate our architecture with our allocation strategies and tradeoff to provide an Akl-Taylor method that is safe with regard for important of in while only needing a constant quantity of publicly available knowledge.

In this essay, Access privileges in distributed systems can be working groups as a tree structure made up of numerous classes. A hierarchical moment key allocation scheme assigns unique cryptographic keys to unique classes in line with their rights to prevent users from higher classes from being used their class key to deduce the key of lower classes. Key derivation is restricted to the class relationship and the time period so because keys differ for each time period. We suggest an improved moment key assignment scheme based on a futz device, which significantly improves computing speed and reduces implementation costs.

In the present study, we show how to divide data D in n parts such that D can be readily rebuilt from any k parts, but even exact understanding of k - 1 bits offer no knowledge at all about D. This technique allows designers to design robust key management methods for cryptosystems that can function securely and consistently even if half of the parts are damaged and all that but a single remaining one have security faults.

3. EXSISTING SYSTEM

The public cloud is what we are using just now. Because of infrastructure is managed and owned by an off-site cloud storage provider, compliance, security, or privacy laws can often be an issue in a public cloud. The system is accessible to any user who pays for the service. The customer controls and maintains the equipment, which is located on-premises, thus these requirements normally do not present a problem in the cloud infrastructure.

Disadvantages
Security concerns
Privacy difficulties with data
Data from all users can be kept in the same cloud location.

Block Diagram

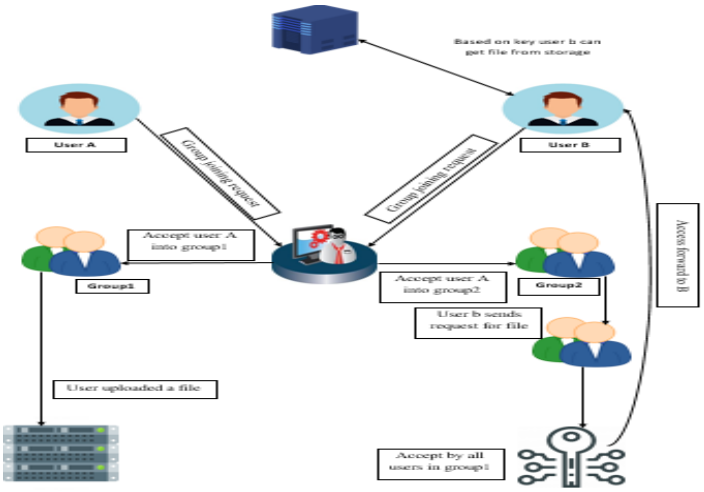


Figure 1. Block Diagram

4. PROPOSED SYSTEM

With proposed solution, we are using a private cloud. In a cloud infrastructure, which is a solitary environment, one user has the exclusive use of the equipment, storage, and network. A specific consumer community can access the cloud environment, which is

controlled, managed, and operated by the organizations involved.

Advantages

Boosting security

Increasing data privacy by allowing for separate data storage for each user

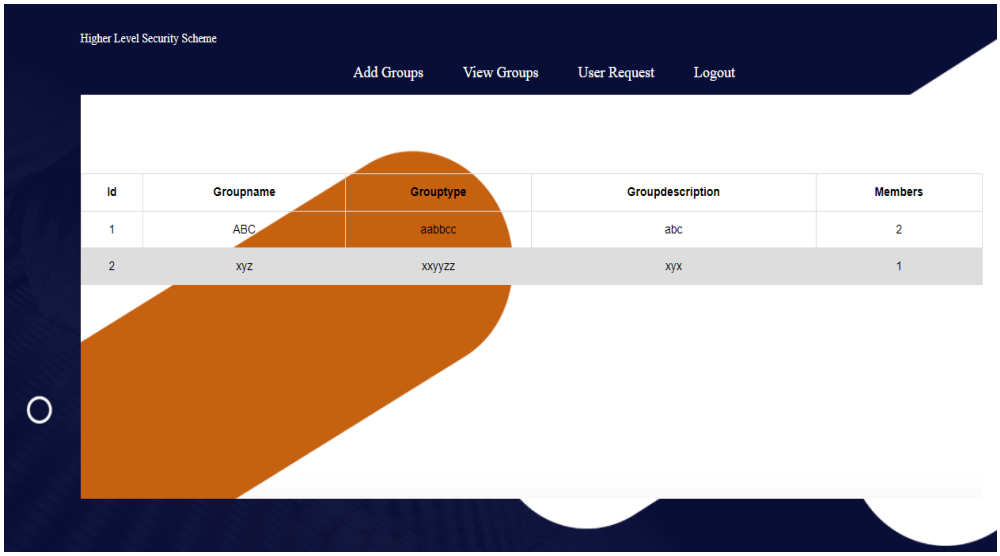
Algorithm

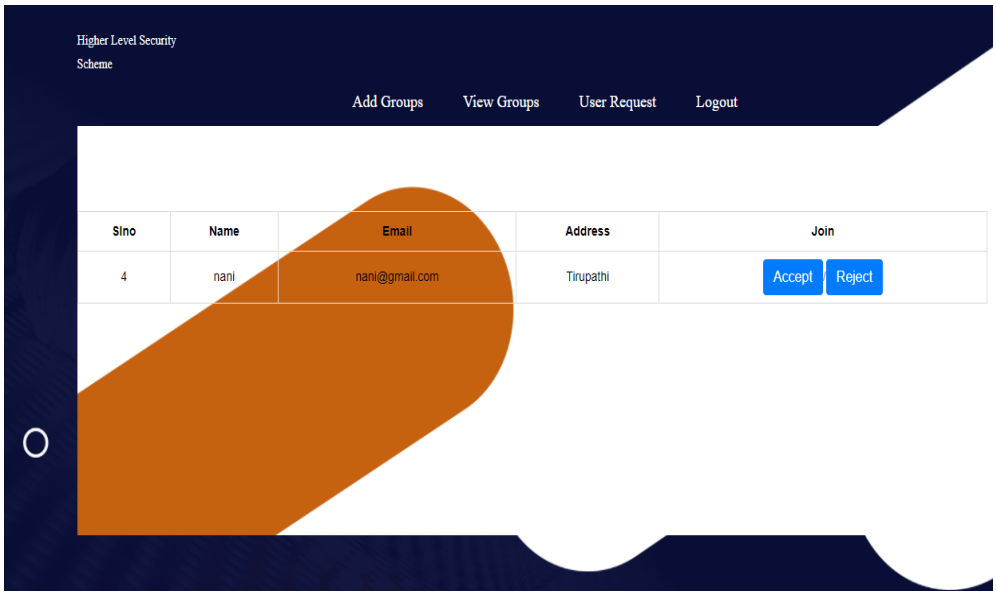
Shamir's Secret Sharing Algorithm: An algorithm for distributing keys is called Shamir's Secret Sharing (SSS). The Rivest-Shamir-Adleman (RSA) algorithm was co-invented by the well-known Israeli cryptographer Adi Shamir, after whom it is called.
SSS divides a secret into pieces called shares, like a cryptographic key. Participants in the discussion receive shares of the business. A most important feature of Shamir's secret sharing is that the secret can be rebuilt using only a part of the shares rather than the entire number.

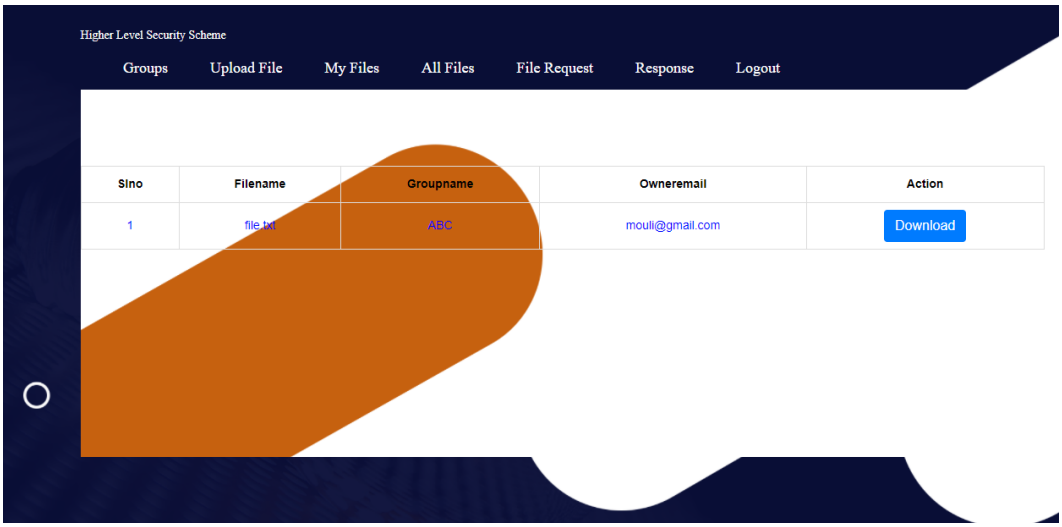
The barrier is the quantity that has to be less than the total quantity. This helps avoid failures in the encryption of the critical information in the event if only one or few of parties are absent.

SSS is widely used to safeguard the key to data which has been encoded or made private to use other tools and algorithms since it gives a feasible solution to the core problems that many arrangements face. The simplest example of SSS is a vaults that only the company board has access to. Because the vault password is encrypted by SSS, a majority (threshold) of members of the board must approve that it may be seen or released. SSS also permits a reasonable certainty that the vaults is secure regardless of whether a board is out of town provided the criteria is still met.

5. RESULT AND ANALYSIS







6. CONCLUSION

A computationally effective technique of key creation is provided by the recommended key access control mechanism. The suggested strategy gives the security of a private cloud coupled with the usability, cost, and accessibility of a public cloud. The stability and low upkeep and administration requirements of the public cloud are further benefits for businesses.

7. REFERENCES

[1] D. Tiwari and G. R. Gangadharan, ‘‘SecCloudSharing: Secure data sharing in public cloud using ciphertext-policy attribute-based proxy re-encryption with revocation,’’ Int. J. Commun. Syst., vol. 31, no. 5, p. e3494, Mar. 2018.
[2] M. Abadi et al., ‘‘TensorFlow: A system for large-scale machine learning,’’ in Proc. 12th USENIX Symp. Oper. Syst. Design Implement. (OSDI), Savannah, GA, USA, 2016, pp. 265 283.
[3] S. Tang, X. Li, X. Huang, Y. Xiang, and L. Xu, ‘‘Achieving simple, secure and efcient hierarchical access control in cloud computing,’’ IEEE Trans. Comput., vol. 65, no. 7, pp. 2325 2331, Jul. 2016.
[4] L. Zhou, V. Varadharajan, and M. Hitchens, ‘‘Trust enhanced cryptographic role-based access control for secure cloud data storage,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 11, pp. 2381 2395, Nov. 2015.
[5] Information Technology-Cloud Computing-Reference Architecture, Standard ISO/IEC 17789:2014, 2014.
[6] Information Technology-Cloud Computing-Overview and Vocabulary, Standard ISO/IEC 17788:2014, 2014.
[7] E. Thomas, P. Ricardo, and M. Zaigham, Cloud Computing: Concepts, Technology, and Architecture, 1st ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2013

[8] M. Peter and G. Timothy, ‘‘The NIST de nition of cloud computing, recommendations of the national institute of standards and technology,’’ NIST, Gaithersburg, MD, USA, Tech. Rep. 800-145, 2013.
[9] L. Zhou, V. Varadharajan, and M. Hitchens, ‘‘Achieving secure role-based access control on encrypted data in cloud storage,’’ IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947 1960, Dec. 2013.
[10] X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, and M. Li, ‘‘Achieving secure and efcient data collaboration in cloud computing,’’ in Proc. IEEE/ACM 21st Int. Symp. Qual. Service (IWQoS), Jun. 2013.

