Design and Analysis of Performance of Cloud Server Embedded with Cryptography and Dynamic Access Control Mechanism

MANCHALA SURYA VENKATA S K PRABHAVAT [#1] , Dr. B.V.S VARMA [#2]

[#1] M.Tech Scholar, Department of Computer Science and Engineering,
DNR College of Engineering and Technology, Sri RamaPuram, Balusumudi,
Bhimavaram - 534202.

[#2] Professor, Department of Computer Science and Engineering,
DNR College of Engineering and Technology, Sri RamaPuram, Balusumudi,
Bhimavaram - 534202.

ABSTRACT

Now a day's almost all small scale and large scale organizations try to adopt the centralized cloud server for their data storage and accessing from the remote locations connected all together from a centralized server with the help of internet. As we all know that till now no cloud service provider is providing privacy for the data in terms of encryption and key access in order to provide data authorization. Enabling cryptographically enforced access controls for data hosted in untrusted cloud is attractive for many users and organizations. However, designing efficient cryptographically enforced dynamic access control system in the cloud is still challenging. In this paper, we propose Crypt-DAC, a system that provides practical cryptographic enforcement of dynamic access control. Here Crypt-DAC try to provide dynamic access for the cloud users based on their individual users request. If any user want to download the data ,he/she need to send request permission for the cloud server and cloud server in turn check the permissions are approved from the admin.Here the admin is the main person who can decide the preferences for the end users. manner. By conducting various experiments on our proposed model, our result clearly tells that our proposed system is practical and efficient.

Keywords

Cloud Computing, Crypt-DAC, Cryptographically, Dynamic Access Control, Data Integrity, Data Authorization, Centralized Server.

1. INTRODUCTION

In current days cloud computing domain has occupied a major role in each and every part of the information processing and information storage centers. As the cloud has become a valuable resource for all parts of information processing centers, the data which is to be stored will be stored on the remote systems not on their local hardware, and accessed remotely via internet by connecting various servers. As the data will be stored on remote server, the data user need to retrieve the data from the remote server, whenever he want any data from that remote hardware. In the current cloud servers, the major limitation is data which is stored and shared over the cloud users has no security and there is also no security for accessing the data in the current cloud servers [1]. This is mainly because all the data which is stored in the current cloud servers is stored in the form of plain text rather than in a cipher text manner.

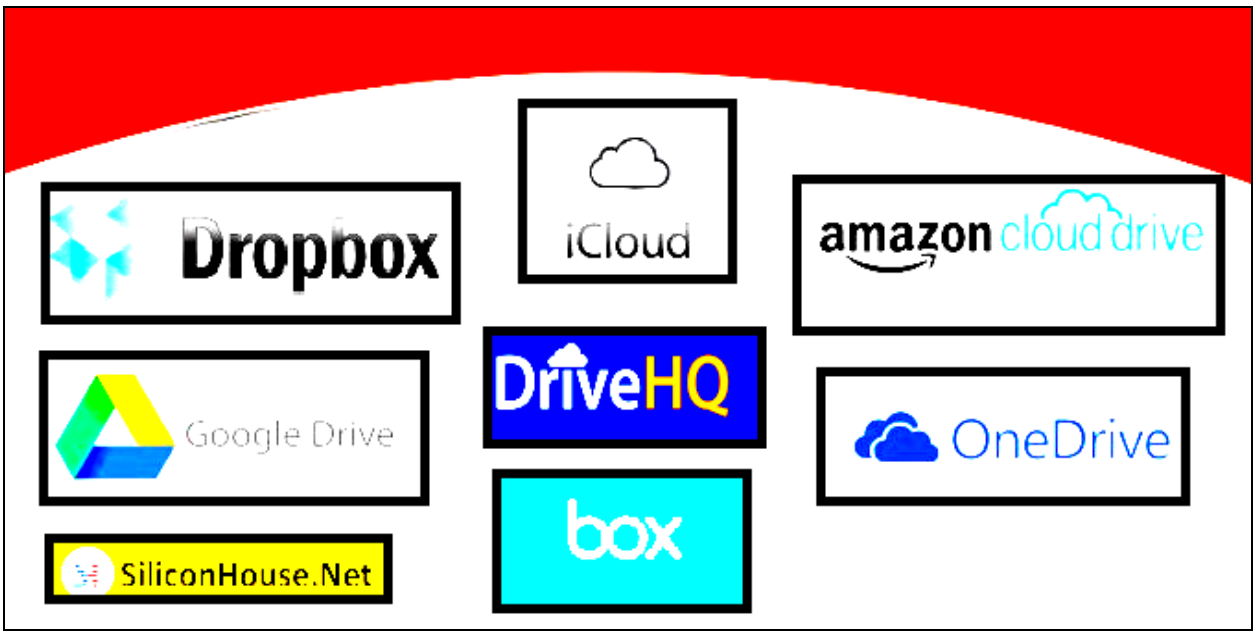

Figure.1. Denote the Different types of Cloud Service Providers

As we know that cloud has exaggerated user attention in storing their valuable or sensitive information however limits in allocating resources dynamically. As we know that cloud has received more and more user's attention towards data storage, it still has some restrictions in size constraints. In enterprise settings, we tend to see the increase in demand for knowledge outsourcing that assists within the strategic management of corporate knowledge. In the recent cloud service providers, it is straightforward to use without charge accounts for email, image

album, file sharing and/or remote access, with storage size a lot of than Fifteen GB (for free usage) and up to 1 TB or more for the premium users [2].Next in the current cloud service providers there is no concept like ranking the files which is stored and uploaded by the data owners. In the cloud there are various types of services available in which Data Base as a Service (DaaS) is one of the main and prominent services among others. This service is not having security for the data which is stored in the cloud, compared with various other cloud services, hence our main motto is to provide security for this DaaS service by integrating various encryption and other techniques are proposed in this current paper.

As we all know that till now no cloud service provider is providing privacy for the data in terms of encryption and key access in order to provide data authorization. In this paper, we propose Crypt-DAC[5], a system that provides practical cryptographic enforcement of dynamic access control. Here Crypt-DAC try to provide dynamic access for the cloud users based on their individual users request. If any user want to download the data ,he/she need to send request permission for the cloud server and cloud server in turn check the permissions are approved from the admin.Here the admin is the main person who can decide the preferences for the end users. manner. By conducting various experiments on our proposed model, our result clearly tells that our proposed system is practical and efficient

2. LITERATURE SURVEY

Literature survey is that the most vital step in software development process. Before developing the tool, it's necessary to work out the time factor, economy and company strength. Once this stuff is satisfied, ten next steps are to work out which OS and language used for developing the tool. This literature survey is mainly used for identifying the list of resources to construct this proposed application.

MOTIVATION

Two notable creators. Yong Qi and Yi Shi [6] has composed a paper on"AppSec: A Safe Execution Environment for Security Sensitive Applications". In this paper the creators focused more on the Malicious OS portion can without much of a stretch access client's private

information in primary memory and pries human-machine cooperation information, even one that utilizes security requirement dependent on application-level or OS level. This paper presents AppSec, a hypervisor-based safe execution condition, to ensure both the memory information and human-machine cooperation information of security-touchy applications from the untrusted OS transparently.AppSec gives a few security components on an untrusted OS. AppSec acquaints a sheltered loader with check the code uprightness of utilization and dynamic shared items. During runtime, AppSec shields application and dynamic shared items from being changed and confirms part memory gets to as per the application's expectation

Two notable creators William C. Battalion III and Adam J. Lee [7], has composed a paper on" An Actor-Based, Application-Aware Access Control Evaluation Framework". In this paper the By differentiate, we formalize the entrance control reasonableness examination issue, which looks to assess how much a lot of up-and-comer get to control plans can address the issues of an application-explicit outstanding task at hand. This procedure includes the two decreases to evaluate whether a plan is fit for actualizing a remaining burden (subjective examination), just as cost investigation utilizing requested measures to evaluate the overheads of utilizing every applicant plan to support the outstanding task at hand (quantitative investigation). We formalize the two-feature reasonableness investigation issue, which officially portrays this assignment. We at that point build up a scientific system for this sort of investigation, and assess this structure both officially, by measuring its proficiency and precision properties, and for all intents and purposes, by investigating a scholarly program board of trustees outstanding task at hand

Two notable writers Anna Lisa Ferrara and Georg Fuchsbauer [8], has composed a paper on "Cryptographically Enforced RBAC". In this paper the creators for the most part thought about the Cryptographic access control vows to offer effortlessly conveyed trust and more extensive materialness, while decreasing dependence on low-level online screens. Conventional executions of cryptographic access control depend on straightforward cryptographic natives while ongoing undertakings utilize natives with more extravagant usefulness and security ensures. Worryingly, not many of the current cryptographic access-control plans accompany exact ensures, the hole between the arrangement determination and the usage being investigated just casually, if by any means. In this paper we start tending to this inadequacy[7]-[10]. Not at all

like earlier work that focused specially appointed strategy particular, we take a gander at the settled Role-Based Access Control (RBAC) model, as utilized in a run of the mill document framework. To put it plainly, we give an exact grammar to a computational adaptation of RBAC, offer thorough definitions for cryptographic approach authorization of an enormous class of RBAC security arrangements, and exhibit that a usage dependent on property based encryption meets our security ideas. We see our principle commitment as being at the applied level. In spite of the fact that we work with RBAC for solidness, our overall procedure could manage future exploration for employments of cryptography in different access-control models[12].

3. THE PROPOSED METHOD INTEGRATED WITH CRYPTOGRAPHY AND DYNAMIC ACCESS CONTROL MECHANISM

In this application we try to construct an integrated method by combining cryptography and dynamic access control for providing security for the cloud data which is stored from the remote locations. As we all know that till now no cloud service provider is providing privacy for the data in terms of encryption and key access in order to provide data authorization. In this paper, we propose Crypt-DAC, a system that provides practical cryptographic enforcement of dynamic access control. Here Crypt-DAC try to provide dynamic access for the cloud users based on their individual users request. If any user want to download the data ,he/she need to send request permission for the cloud server and cloud server in turn check the permissions are approved from the admin.Here the admin is the main person who can decide the preferences for the end users. By conducting various experiments on our proposed model, our result clearly tells that our proposed system is practical and efficient

1. Our protocol supports DAC model with cryptographically parameters to enable more security in real world.
2. At the same time, the privacy of the user is also preserved. The cloud system only knows that the user possesses some required attribute, but not the real identity of the user.
3. To show the practicality of our system, we simulate the prototype of the protocol.
4. The proposed cloud servers have a facility to access the data in a secure manner under dynamic access control.

5. There is a new concept like allowing permissions dynamically from the cloud admin and in turn has no privilege to restrict the un-authorized users.

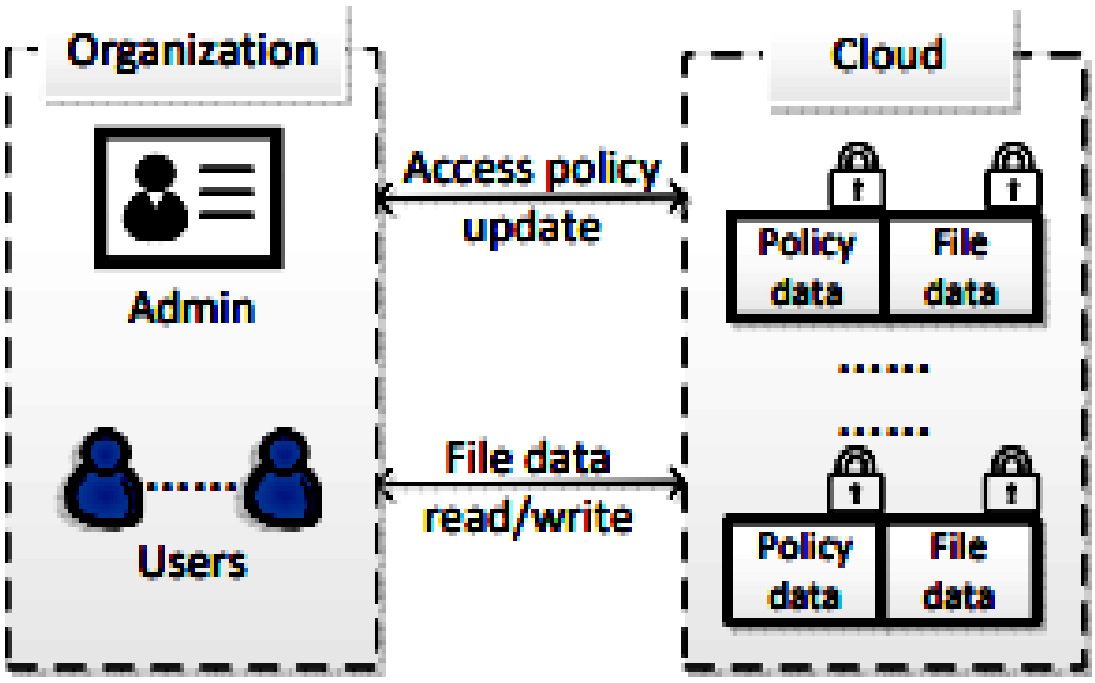

Figure. 2. Denote the Proposed Architecture Using DAC Model

From the above figure 2, we can clearly identify the data owner/data user need to register first into the application and then they will try to request the cloud server for getting the access policies which are required for accessing the file. The Cloud server will receive the user request and then try to verify the user identity and then it will decide whether to give access or not. For each and every individual user the access policies may be changed and this DAC will dynamically give different rights for individual users. Once the user get the DAC permission for entering into the system. Now he try to search for the file ,so that the user will be asked for file permissions from the admin.Here the admin will try to give search and download permissions if the user is known for that admin.Once the user receives the file access permissions,then the user can able to see which type of permissions he is allowed from the admin.In this whole process if any user who don't have key permissions or file permissions try to access the cloud for data, he will not be allowed to access the file in plain text manner.

4. IMPLEMENTATION PHASE

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed protocol. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My-SQL Server.The application is divided mainly into following 3 modules. They are as follows:

1. Data Owner/Admin Module
2. Cloud Server Module
3. End User Module

1. DATA OWNER/ADMIN MODULE

In this module, the data owner uploads their data with its chunks in the cloud server. For the security purpose the data owner encrypts the data file's chunks and then store in the cloud. The data owner can change the policy over data files by updating the expiration time. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

DYNAMIC OPERATION

1. **Upload**: is the operation to encrypt and upload the file
2. **Delete**: Is the operation to delete a corresponding data owner file in the cloud.
3. **Verify:** Verifying the data whether it is safe or not in the cloud.

2.CLOUD SERVER MODULE

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. The end user request will be processes based on the queue.

3. END USER MODULE

The Cloud User/End User who has a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data. The end user sends the request for corresponding file request and it will be processed in the cloud based on the queue and response to the end user.

5. CONCLUSION

In this proposed work we for the primary time designed and implemented a secure Crypt-DAC, a system that provides practical cryptographic enforcement of dynamic access control. Here Crypt-DAC try to provide dynamic access for the cloud users based on their individual users request. If any user want to download the data ,he/she need to send request permission for the cloud server and cloud server in turn check the permissions are approved from the admin.Here the admin is the main person who can decide the preferences for the end users. manner. By conducting various experiments on our proposed model, our result clearly tells that our proposed system is practical and efficient.

6. REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute based encryption, in IEEE S&P, 2007.

[2] X. Wang, Y. Qi, and Z. Wang, Design and Implementation of SecPod:A Framework for Virtualization-based Security Systems, IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 1, 2019.

[3] J. Ren, Y. Qi, Y. Dai, X. Wang, and Y. Shi, AppSec: A Safe Execution Environment for Security Sensitive Applications, in ACM VEE, 2015.

[4] V. Goyal, A. Jain, O. Pandey, and A. Sahai, Bounded ciphertext policy attribute based encryption, in ICALP, 2008.

[5] V. Goyal, O. Pandey, A. Sahai, and B.Waters, Attribute-based encryption for fine-grained access control of encrypted data, in ACM CCS, 2006.

[6] J. Katz, A. Sahai, and B. Waters, Predicate encryption supporting disjunctions, polynomial equations, and inner products, in EUROCRYPT,2008.

[7] S. Muller and S. Katzenbeisser, Hiding the policy in cryptographic access control, in STM, 2011.

[8] R. Ostrovsky, A. Sahai, and B. Waters, Attribute-based encryption with non-monotonic access structures, in ACM CCS, 2007.

[9] A. Sahai, and B. Waters, Fuzzy identity-based encryption, in EUROCRYPT, 2005.

[10] T. Ring, Cloud computing hit by celebgate, http://www.scmagazineuk.com/cloud-computing-hit-by-celebgate/article/370815/, 2015.

[11] X. Jin, R. Krishnan, and R. S. Sandhu, A unified attribute-based access control model covering DAC, MAC and RBAC, in DDBSec, 2012.

[12] W. C. Garrison III, A. Shull, S. Myers, and, A. J. Lee, On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud, in IEEE S&P, 2016.

7. ABOUT THE AUTHORS

MANCHALA SURYA VENKATA S K PRABHAVAT is currently pursuing her 2 years M.Tech in the Computer Science and Engineering at DNR College of Engineering and Technology, Sri RamaPuram, Balusumudi, Bhimavaram - 534202.Her area of interest includes Cloud Computing.

Dr. B.V.S VARMA is currently working as a Professor in the Computer Science and Engineering at DNR College of Engineering and Technology, Sri RamaPuram, Balusumudi, Bhimavaram - 534202.He has more than 18 years of teaching experience in various engineering colleges. His research areas include the Data Mining, Cloud Computing.