International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Method for Secure Resource Sharing at User Level In Cloud Computing

M. Swapna[1], Ch. Silas Emmanuel[2], Md. Asrar Ahmed[2], R. Nithish[2], K. Raghavendra[2]
[1]Assistant Professor, Department of Information Technology in Teegala Krisha Reddy Engineering College,Telangana, India
[2]UG Scholar, Department of Information Technology in Teegala Krisha Reddy Engineering college, Telangana, India

ABSTRACT

Sharing of resources on the cloud can be achieved on a large scale since it is cost effective and location independent. Despite the hype surrounding cloud computing, organizations are still reluctant to deploy their businesses in the cloud computing environment due to concerns in secure resource sharing. In this paper, we propose a cloud resource mediation service offered by cloud service providers, which plays the role of trusted third party among its different processes. This paper formally specifies the resource sharing mechanism between two different processes in the presence of our proposed cloud resource mediation service. The correctness of permission register and delegation mech- anism among different processes using two distinct algorithms (Register,Message processing and verification) is also demonstrated using formal verification. The performance analysis suggest that sharing of resources can be performed securely and efficiently across different processes of the cloud.

Keywords : Process Access Control, Formal Specifica- tion and Verification, Cloud Computing

I. INTRODUCTION

Cloud storage outsourcing has become a popular application for enterprises and organizations to reduce the burden of maintaining big data in recent years. However, in reality, end users may not entirely trust the cloud storage servers and may prefer to encrypt their data before uploading them to the cloud server in order to protect the data privacy.

Cloud computing has been envisioned as the bleeding edge perspective in calculation. In the cloud computing environment, the two applications and assets are passed on ask for over the Internet as services. Cloud is an area of the equipment and programming assets in the server cultivates that give different services over the framework or the Internet to satisfy customer's necessities.

Cloud computing facilitate collaboration between users and organizations, security and privacy of cloud services and the user data may deter some users and organizations from using cloud services (on a larger scale) and remain topics of interest to researchers . Typically, a cloud service provider (CSP) provides a web interface where a cloud user can manage resources and settings (e.g. allowing a particular service and/or data to selected users). A CSP then implements these access control features on consumer data and other related resources.

Attributes are found in the private cloud; so, control immediately passes to the private cloud, where duplicate check can be performed. Data stored in the public cloud is accessed only by the authorized users with the help of different individual encryption privilege keys. Convergent and Symmetric encryption techniques produce identical cipher text that results in minimum overhead.

cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. ata security is a common concern for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security.

Cloud computing is one of the most important emerging and promising field in Information Technology. It provides services to various organization over a internet with the ability to scale up or scale down their service requirements.

However, traditional access control models, such as role based access control, are generally unable to adequately deal with cross-process resource access requests. In particular, cross-process access requests pose three key challenges. Firstly, each process must have some prior understanding and knowl- edge about the external users who will access the resources. Thus, an administrator of each process must have a list of

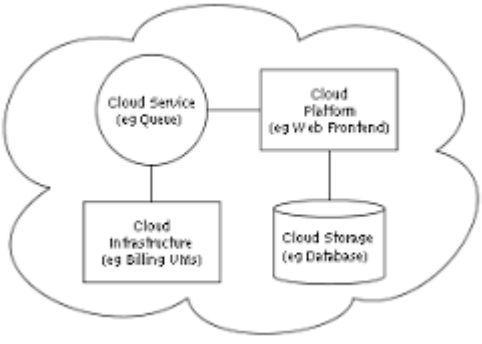

Figure 1 : Cloud computing features.

In current situation, the original data will be stored in cloud. Sometimes the unauthorized person try to access the original data, So the data get leaked. For example, a hospital may give patient records to research person who will find new treatments for the disease. Similarly, a company may have partnerships with other companies so that sharing customer data is mandatory. Another enterprise may be outsource its data processing, so that data must be given to the different companies. We can call the owner of the data as an distributor. Our goal is to detect when the owner's original data have been leaked by intruder, and if possible to identify the intruder that leaked the data. However, in some cases, it is important not to alter the original data. For example, if an outsourcer is doing our payroll, he must know the exact salary and customer bank account numbers. If medical research person will be analyzing patients records, they may need accurate data for the patients. Traditionally, data leakage detection is handled by watermarking technique. For example, a unique code is embedded in each distributed copy using various types of watermarking algorithm. If that copy is later discovered in the hands of an unauthorized person, the leaker cannot be identified. This is the major drawback in watermarking technique. Watermarks can be very useful in real-time environment, but again, it involves some modification of the original data. In sometimes watermarks can be destroyed if the data recipient is malicious.

Security is one of the most crucial aspects in cloud computing. Hence this prohibit the adoption of cloud computing. Therefore, in this paper, we collectively approaches the issue of security and performance. We present Division and Redundancy of Data in the Cloud for Optimal Performance and Security (REDUNDANCY) this will fragments the owners files into various parts and replicate them in the cloud space. The division of a file into fragments is performed based on the threshold value decided by the data owner. Such that the individual fragments doesn't hold any meaningful information. Each and

every cloud nodes we use the term node to represent computing and storage contains a distinct fragment to increase the data security. A successful attack on each and every single node must not reveal the locationsof other fragments within the cloud space. The intruder cannot predict the locations of file fragments so that it improves the security in the cloud. Now we select the nodes in such a manner that they are not adjacent and are at certain distance from each other. The node separation is done by the means of the Graph concept. Moreover, the nodes storing the fragments are placed with a certain distance by means of graph Graph inorder to restrict an intruder of guessing the locations of the fragments.

II. MOTIVATION

A Watermark is a signal that is securely, indiscernibly embedded into original content such as an image, video, text, or audio signal, producing a watermarked signal and it describes information that can be used for verification of original copy. It provides an effective watermarking technique along with the relational data. This technique ensures that some bit positions of some of the attributes of some of the tuples contain required specific values. The tuples, bit positions in an attribute, and specific bit values are all algorithmically determined under the control of a private key that key is only known to the data owner. This bit pattern constitutes the watermark code. If only one person access to the private key then it is possible to detect the watermark with higher probability. The watermark can be detected even in a small subset of a relational data as long as the sample contains some of the watermarks. Protection is based upon the insertion of digital watermarks into the original data. The watermarking technique introduces small errors into the data being watermarked. These intentional errors are called marks and all these marks collectively constitute the watermark. The marks must not have a impact on the usefulness of the data and that data should be placed in such a way that a malicious user cannot destroy them.

III. PROPOSAL OVER VIEW

Data security :

The data owner first registered into the cloud account. Each and every user has to registered into the cloud. Now the data owner and user will become the authorized person. The data owner will upload the file into the cloud. Now the data owner login into the account, at that time the cloud provider verify the already registered owner or not. If they are registered owner and then they will transfer the file to the registered user. Now the registered user login into their account the cloud provider again verify the registered user. The registered user will download the file sent by the data owner. If someone try to copy the URL, the data get leaked in someone's laptop. Now the details about the unauthorized person will be tracked. This tracked information sent as a mobile intimation to the data owner. The mobile intimation will hold informations like IP address, MAC address and GPS location.

To provide a secure cross-process resource access service, a fine-grained cross-process access control model is required . Thus, in this paper, we propose a cloud resource mediation service (CRMS) to be offered by a CSP, since the CSP plays a pivotal role managing different processes and a cloud user entrusts the data to the CSP. We posit that a CRMS can provide the CSP competitive advantage, since the CSP can provide users with secure access control services in a cross- process access environment (hereafter, we referred to as cross process access control - CTAC). From a privacy perspective, the CTAC model has two advantages. The privacy of a process, say P2, is protected from another process, say P1, and the CRMS, since P2's attributes are not provided to P1. P2's attributes attributes are evaluated only by the CRMS. Furthermore, a user

does not provide authentication credentials to the CRMS. Therefore, the privacy of P2 is also protected as the CRMS has no knowledge of the permissions that P2 is requesting from P1. The security policies defined by P1 use pseudonyms of the permissions without revealing the actual information to the CRMS during publication of the policies.

To demonstrate the correctness and security of the proposed approach, we use model checking to exhaustively explore the system and verify the finite state concurrent systems. Specifically, we use High Level Petri Nets (HLPN) and Z language for the modeling and analysis of the CTAC model. HLPN provides graphical and mathematical representations of the system, which facilitates the analysis of its reactions to a given input. Therefore, we are able to understand the links between different system entities and how information is processed. We then verify the model by translating the HLPN using bounded model checking. For this purpose, we use Satisfiability Modulo Theories Library (SMT-Lib) and Z3 solver . We remark that such formal verification has previously been used to evaluate security protocols such as in .

We regard the key contributions of this paper to be as follows:

We present a CTAC model for collaboration, and the CRMS to facilitate resource sharing amongst various processes and their users.

We also present four different algorithms in the CTAC model, namely: register, delegation, Message processing and backward revocation.

We then provide a detailed presentation of modeling, analysis and automated verification of the CTAC model using the Bounded Model Checking technique with SMT- LIB and Z3 solver, in order to demonstrate the correctness and security of the CTAC model.

Petri Nets have been used in the modeling of a wide range of systems, such as asynchronous, concurrent, distributed, non- deterministic, parallel and stochastic systems . However, there is a tradeoff between modeling generality and analysis capability in Petri Nets. Even an average model can become too large for analysis. In this work, we use HLPN for the

Security Properties for Register Algorithm: The register algorithm specific properties are as follows:

(Register.a) Intra-process user to permission assignment property holds when the intra-process user and the permission both exist in the intra-process-permission assignment set.

(Register.b) Intra-process user to cross-process user register property holds when the intra-process user, cross-process user and the permission match the intra'- cross-process-user-permission set.

(Register.c) Cross-process user to cross-process user register property holds when the two cross-process users and the permission match the cross-cross-process- user-permission set.

Redundancy Methodology: In REDUNDANCY methodology, we are not storing the entire file in cloud space. Now we are splitting the entire file into various fragments. These fragments have to distribute in the cloud space. Each and every fragment has to place in a particular node. So that each node contain only a single fragments. In each successful attack the node will not reveal the significant information. After the fragmentation process redundancy will takes place. In redundancy process, each fragment has to replicate its content once in the cloud space. In this way we can achieve the security in the cloud computing. In REDUNDANCY methodology, user sends the data file to cloud space. Upon receiving the file the cloud manager performs:

(1) File Fragmentation
(2) Nodes selection
(3) Stores fragment
(4) Nodes selection for fragments redundancy.

Redundancy Implementation:

In cloud, security is the major aspects for a large-scale system. This provides security of the system as whole and individual nodes. On every successful intrusion into a single node it provides more consequences for data and other nodes. A successful intrusion may lead to software failure. It may also lead to administration defenseless. File fragmentation is a term that describes a group of files that are scattered throughout the cloud. The data owner splits the file into various pieces called fragments. The size of fragmentation is decided by data owner using threshold value. In various aspects the threshold value can be fixed, they are, Allocation of File size memory and fragmenting.

In order to provide the security while placing the fragments in cloud, the concept of Graph is required. Graph is mainly used for the channel assignment problem. This will generates a non-negative (i.e. positive number) random number and builds the set T starting from zero to generated random number. It assigns colors to the each and every node, such that, initially, all of the nodes will be in open color. When a fragment is placed on the particular node, all of the neighborhood nodes are at a certain distance belonging to T and there are assigned to close color. In this process, this will lose some of the central nodes in cloud so that may increase retrieval time. If anyhow the intruders try to track the node position and take the fragment, he cannot determine the location of the other fragments. The intruder can only keep on guessing the location of the other fragments in cloud. Because the nodes are separated by using Graph concepts.

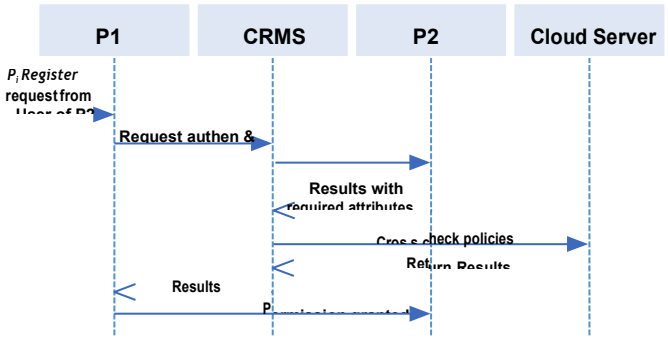

Figure 2 : Flow for permission request in the cloud

Steps for permission register request in the cloud

There are three main entities, namely: the SP (P1), the SR (P2), and the CRMS. The roles of these entities are described as follows:

a) *Process* P1 *responsibilities:* P1 is responsible for pub- lishing cross process policies on the CRMS. P1 receives access requests from P2 and redirects the request to the CRMS for further processing.

b) *Process* P2 *responsibilities:* The CRMS redirects ac- cess requests to P2 for authentication.

c) Once the redirected access request is received, the responsibility of P2 is to authenticate the identity of particular user.

In redundancy process, unique copy exists and the same copy will exists once again. The redundancy process is used to increase the data availability and their by improve the retrieval time. This performs a controlled redundancy. In redundancy process, copies of the same data item have the same value. There are three types of redundancy, It places the fragment on the node that provides the limited access cost. Hence improve retrieval time for accessing the fragments and reconstruction of the original file. While replicating the fragment, the separation of fragments is achieved by Graph, is also taken care of node placement. In case of a large number of fragments or small number of nodes, it is also possible that some of the fragments can be left without being replicated because of using Graph concepts.

Cloud Computing leverages many existing technologies such as web services, web browsers, and virtualization, which contributes to the evolution of cloud environments. Therefore, any vulnerability associated to these technologies also affects the cloud, and it can even have a significant impact.

As discussed previously, Graph prohibits storing the fragment and also avoid the neighborhood of a node storing a fragment, resulting in the eliminating the nodes used for storage. In such a case, only for the remaining fragments, the nodes that are not holding any of the fragments are selected for storage randomly. The nodes were separated by means of Graph concepts. The fragmentation process ensured that no successful information was obtained in successful attack. No node in the cloud, stored more than a single fragment of the same file. The REDUNDANCY methodology performance is compared with full-scale redundancy techniques. This results in simultaneous focus on the security and performance. Resulted in increased security level of data.

Registration algorithm:

Consider the processes p1 and p2.

1. Finding the intra process with cross process detection Set.
2. Cross process to the cross user detection set inclusion.

a) In response, P2 sends the user authentication response (valid or invalid) and process authentication response to the CRMS.
b) *CRMS responsibilities:* The CRMS receives the permission-register request redirected from P1. Once an access request is received, the CRMS evaluates the request on the pre-published policies and responds to P1.

The steps for initiating a permission-register request are as follows: *Permission register request:* A user wishing to access a resource at P1.

Step 2: Request redirection to the CRMS: Upon selection of a shared service the user wishes to access, the user is redirected to the CRMS site. On the site, the user will be asked for the parent process. The user selects the parent process and the CRMS redirects the user's request to the selected process (P2 in this case).

Step 3: Process P2 *authentication:* The user has to authen-
ticate at her parent process, P2. Upon successful authentication, the user will be redirected again to CRMS with the attributes requested by the CRMS for cross process policy execution.

Step 4: CRMS redirection to process P1 *& permission register:* The user's attributes are evaluated against the P1 policy and if the policy criteria is successfully fulfilled, then the user is provided service access at P1; otherwise, the access request is denied. The CRMS also takes into account any conflict of interest policies, such as Chinese Wall Policy.

Registering a user: An register query defines a request from an intra-process/cross process user for the activation of a permission p_i, where p_i P_i. We formally define an registering.

Alternatively, the algorithm evaluates the next option, which is checking the user against cross-process to cross-process user permission delegation set. If the result turns out to be false, then the algorithm checks for the presence of input query parameters in the cross-process to cross-process delegation set. If such a delegation has previously been been performed, then a result will be produced as shown in the data visualization for security.

Message Processing and validation Algorithm: The backward revo- cation algorithm is based on the backward revocation query defined in Section IV. The backward revocation algorithm is invoked on the CRMS when the attribute of the delega- tee (cross-process user/process) does not match the delegation.

Revocation Algorithm

There are two ways in which we can revoke a previously granted permission from the cross-process user/cross-process.

1) Revoke the permission from the service provider's side; or
2) Revoke the permission when the attributes of the user change and no longer match the published security policies on the CRMS. utilization more difficult than the traditional storage where data is kept in the absence of encryption. One of the typical solutions is the searchable encryption which allows the user to retrieve the encrypted documents that contain the user-specified similarwords, where given the similarword trapdoor, the server can find the data required by the user without decryption.Given the trapdoor and the ,ciphertext, the server can test whether the similarword underlying the ,ciphertxt is equal to the one selected by the receiver.

IV. CONCLUSIONS

We have shown that it is possible to access the likelihood of an unauthorized person is responsible for a leak, based on the overlap of his data with the leaked data. Our model is relatively simple, but we believe that it provides the essential trade-offs. Hence we have presented a variety of data distribution strategies that can improve the distributor's chances of identifying a leaker. We proposed the REDUNDANCY methodology, a cloud storage security scheme that collectively deals with the security and performance that increase the retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. The fragmented file will be replicated their by increasing data availability and provide security to the cloud. Future work will include a comparative analysis of the proposed CTAC model with other state-of-the-art cross domain access control protocols using real-world evaluations. For ex- ample, one could implement the protocols in a closed or small scale environment, such as a department within a university. This would allow the researchers to evaluate the performance, and potentially (in)security, of the various approaches under different real-world settings.

V. REFERENCES

[1]. B. Mungamuru and H. Garcia-Molina, "Privacy, Preservation and Performance: The 3 P's of Distributed Data Management,"technical report, Stanford Univ., 2008.

[2]. V.N. Murty, "Counting the Integer Solutions of a Linear Equation with Unit Coefficients," Math. Magazine, vol. 54, no. 2, pp. 79-81, 1981.

[3]. S.U. Nabar, B. Marthi, K. Kenthapadi, N. Mishra, and R. Motwani, "Towards Robustness in Query Auditing," Proc. 32nd Int'l Conf. Very Large Data Bases (VLDB '06), VLDB Endowment, pp. 151-162,2006.

[4]. P. Papadimitriou and H. Garcia-Molina, "Data Leakage Detection," technical report, Stanford Univ., 2008.

[5]. P.M. Pardalos and S.A. Vavasis, "Quadratic Programming with One Negative Eigenvalue Is NP-

[6]. Hard," J. Global Optimization, vol. 1, no. 1, pp. 15-22, 1991.

[7]. J.J.K.O. Ruanaidh, W.J. Dowling, and F.M. Boland, "Watermarking Digital Images for Copyright

[8]. Protection," IEE Proc. Vision, Signal and Image Processing, vol. 143, no. 4, pp. 250-256, 1996.

[9]. R. Sion, M. Atallah, and S. Prabhakar, "Rights Protection for Relational Data," Proc. ACM SIGMOD, pp. 98-109, 2003.

[10]. L. Sweeney, "Achieving K-Anonymity Privacy Protection Using Generalization and Suppression," http://en.scientificcommons.org/ 43196131, 2002.

[11]. Gartner Inc: Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: . Accessed: 15-Jul-2011

http://www.gartner.com/it/page.jsp?id=145422 1 Online. Available: . Accessed: 15-Jul-2011

[12]. Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: Cloud Computing: A Statistics Aspect of Users. In First International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Berlin; 2009:347–358.Google Scholar