International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 2 March-April 2017 p-ISSN: 2394-8280

ROLE BASED ACCESS CONTROL POLICY USING ROLE HIERARCHY FOR SOFTWARE ORGANIZATIONS IN CLOUD ENVIRONMENT

Aditi Vyas
M.Tech Scholar, Department of Computer Science & Engineering, SDBCT Indore, India
aditi.vyas0211@gmail.com

ABSTRACT:

With the rapid developments occurring in cloud computing and services, there has been a growing trend to use the cloud for large-scale data storage. This has raised the important security issue of how to control and prevent unauthorized access to data stored in the cloud. One well-known access control model is the role-based access control, which provides flexible controls and management by having two mappings, users to roles and roles to privileges on data objects. In this paper, we propose a modified blowfish encryption scheme, which integrates the cryptographic techniques with RBAC. Exploiting less secure transition, insider or outsider attacker tries to destroy the data privileges by accessing and modifying the records without permissions. Utilizing some role based access control and fine-grained access policies controls it. Yet at the same time the customary systems of the RBAC model get the process stuck in execution advertisement updates bottleneck. Additionally the verification, policy allotment, role activation and consistent monitoring of users' conduct is still not achieved. In this paper we are trying to evaluate the proposed model on the basis of the result extracted from the experimental executions. We describe a practical implementation of the proposed RBE based architecture with Blowfish algorithm on Openshift public cloud, and discuss the performance results.

Keywords: Role Based Access Control, Cloud Security, Policy Based, Blowfish, Public Cloud.

1. INTRODUCTION

Cloud computing is the latest area of work, picking up prominence because of its service based process handlings. Employ the contending offers various processes as a service to the users. For giving this, various existing computing approaches are honed to satisfy the user's needs of computationally efficient software uses according to needs. It is the combination of distributed processes, scalable computing, fault tolerant capacity and billed according to their Consumption as it was. Thus, for both the ends of cloud suffers from this frequently varying trust and complex problem handlings. In this process a massive amount of resources and cost is wasted by which a security service delivery is guaranteed. In cloud computing, this outsourcing based service architecture lets the providers and end user data demands offerings on smaller cost [16]. In Figure 1 specify role based control system.

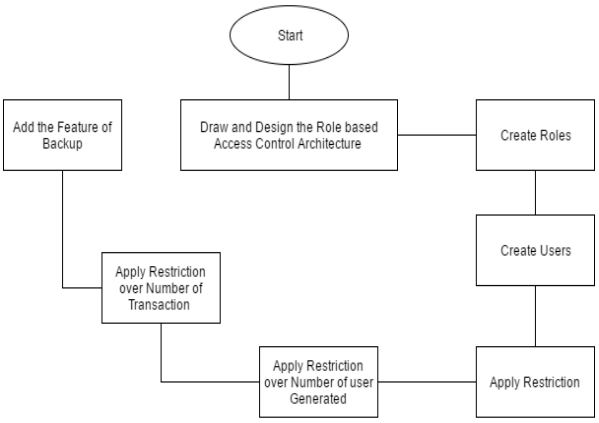

Figure 1. Role Based Access Control System

It primarily focuses on higher availability of data, scalable demands with quality solutions in comparison with local environments. All it needs to handle heterogeneous settings and devices working simultaneously on several distributed locations. Such heavy exchange compromises the service security and speed, which degrades the users trust.

In cloud, various computing works simultaneously with a proper tenancy model accordingly and requires an accurate service transition. In absence of that several issues related to security is triggered on which in future may distort the overall service and data. The features needs to be handled effectively are Scalability, Location transparency and service orchestration. In other words, for effective service insecure medium confidentiality should be achieved in higher side. Here confidentiality doesn't mean to make the data secure from outside attacker, but to make the data secure against insider cloud system i.e. provider.

The work assumes that cloud provider is not trustworthy and may collect uses sensitive data from their system to make some commercial or ethical benefits. Also, there are some situations where the data isolation is not provided and in some cases incorrect data is getting permits to access by some other users. As this environment involves heavy integration of services and policies, user's role and their access are not previously defined which makes confusion at the time of data access [16].

This work focuses its intentions towards achieving following goals:

- Each service user can make self-assurance that their data is secure against their providers even if there is some disturbance or non-cooperation by providing.
- Users can access the data according to their roles and each role is having different of separate policies for data transfer.
- The approach to improve the security and trust could not consume more resources which degrades the systems performance and increases overhead. Thus, the objective is to develop a more secure and robust system, which lets the users trust increase over the system with reduction in resource overheads by effective role, based access control through some defined policies.

2. LITERATURE REVIEW

In a step to achieve the cloud security through effective confidentiality schemes, the paper [7]

gives an approach, which prevents the system from unauthorized access using encryption schemes. Here the data before sending to third party locations gets encrypted by some traditional methodologies and algorithms. But as the scalability and migration is a key policy and feature for cloud era, such encryption makes it complex to search this data from a huge storage repositories and hence the systems performance gets degraded. In this paper the author had also provides a concise but all-round study on data protection and privacy fortification issues coupled with cloud computing crossways all stages of data.

As of now, cloud security consideration is totally depends on the number of service level agreements (SLA's) between the providers, brokers and users. This SLA increases the trust between the various cloud entities and in absence of which security can be compromised. The paper [9] focuses on some of these SLA's and security certificates using ISO 27000 and NIST-FISMA standards which improve the consumer trust over the system. The paper also presents a new cloud security framework which enables security certifications with trusted third party data exchanges. Some supportive extensions of these security certificates with effective SLA's exchanges in multi-tenancy models is given in [10] also.

Even with such an improved trust based systems and thresholding parameters with guided security functionalities, the traditional mechanism get stacked in bottleneck problems. The paper [11], proposes a novel model which provides security and trust for effective data sharing between the users and providers. It also gives some of the measures which increase the trust on the system with secure policies of sensitive data access at trusted third party locations. It increases the user's reliability and utility of the system. Aim is towards the proper distribution of security service with justifiable certificates for each successful data transition. All its needs are to make the transition secure form insider and outsider.

The paper [12] continue the similar issues with some adjustment in security architectures and prelims the first requirement as; service provider is not trusted by the user. This article describes at a high level where several architectures combine recent and non-standard cryptographic primitives.

To overcome this limitation of above papers the article [13] presents an approach that does not require complete trust in the external service both resource content and authorization management. At the same time it allows users to retain to the provider the enforcement of the access control policy on their resources. The suggested solution relies on the translation of the access control policy into an equivalent encryption policy.

The paper [14] proposes a Temporal Attribute based Access Control (TAAC) approach for multi-authority cloud storage systems. IN the above suggested approach the authorities are independent from each other and do not require any central authority with all the controls without any certificates.

3. BLOWFISH ALGORITHM

Blowfish is symmetric algorithm, which use one key for encryption and decryption. Key length is variable from 32 to 448 bits. It is replacement of DES and IDEA algorithm**.** Below diagram show Feistel function

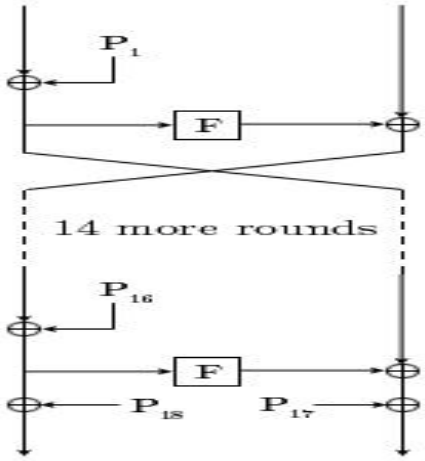

Figure 3: Feistel function of Blowfish Algorithm

4. PROPOSED WORK

Proposed system implement on public cloud with help of open shift cloud.

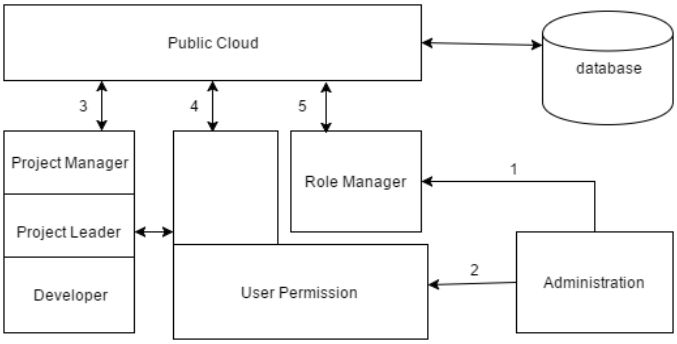

Figure 4: Role Base Access Control System on public cloud

In our system four users are

1. Administrator: - Administration create role hierarchy and the role of all the users like project manager, project leader and developer. Administrator also responsible for maintain Role Policy and permission
2. Project Manager: - Project manager encrypted data using blowfish algorithm and store all data in public cloud.
3. Project Leader: - project leader can download and modify the file and request for extra permission from admin.
4. Developer: - Developer only read and modifies project code, which uploaded by project manager and also send request for extra permission.

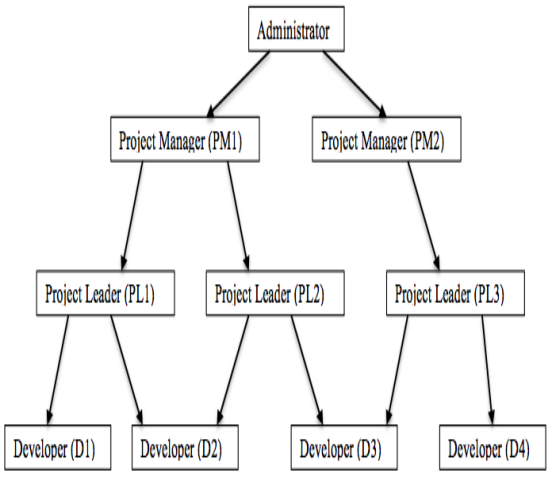

Figure 5: User Hierarchy for RBAC

Proposed system performing following operations

- Manage Role
- Encryption
- Decryption
- Mange Role Policy

Encryption and Decryption performed using blowfish algorithm. Pseudo code of blowfish describe below.

Step1: start the item size.

Step 2: 16 rounds are there in blowfish.

Step 3: x be the input of 64 bit data element.

Step 4: x will be divided into two halves x1 and x2.

Step 5: then, for i = 1 to 16:

X1 = x1 XOR Pi XOR key x2 = F(x1) XOR x2

Step 6: Swap x2and x2

Step 7: After the sixteenth round, swap x1 and x2 again to undo the last swap. Then, x2= x2 XOR P17 and x1 = x1 XOR P18.

Step 8: Recombine x1 and x2 to the cipher text

Step 9: Decryption in reverse order except p1,p2,.....p18.

Step 10: stop

5. RESULT:

We created public cloud with help of Openshift cloud.url of our cloud is *http://rbaccess1-mtechproject12.rhcloud.com/* .

File data encrypted at the time of file upload on public cloud by any user. Below diagram 6 show encrypted data of file.

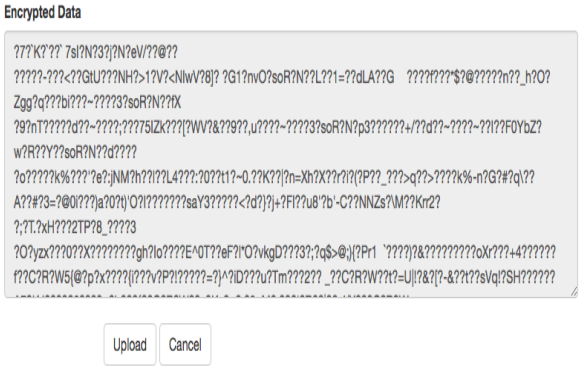

Figure 6: Encrypted Data of File on public cloud

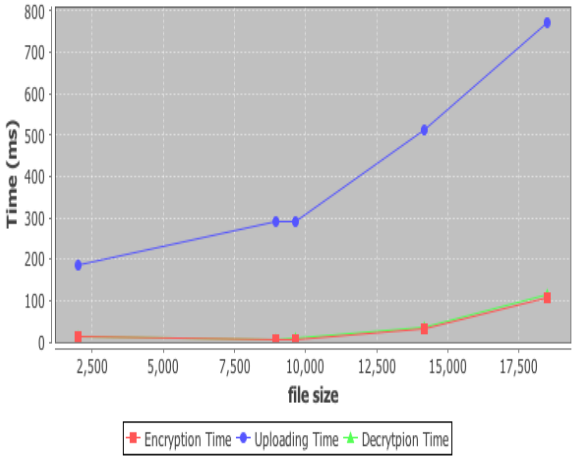

Figure 6: encryption, decryption and upload time of file

Project Manager Upload file on public cloud and access these files on basis of role. Upload file store on public cloud database. At time of file upload calculate uploading time and encryption of file.in below figure 7 show uploading time, encryption time and decryption time of files. We also maintain role policy. On base of role policy each user assign different role. Role of each user describe in below table.

Table 1: Permission Details of Each Role

Role Hierarchy	Role Name	Permission				
		Read	Modify	Download	Delete	Edit
Level-1	Project Manger	Yes	Yes	Yes	Yes	Edit
Level-2	Project Leader	Yes	Yes	Yes	No	Edit
Level-3	Developer	Yes	Yes	No	No	Edit

The aim is towards providing more security and robustness against the traditional breaches which practical implementation of cloud is facing. Proving the data and users security against its confidential and private information concerns the major area of cloud working. These intensions are kept in mind at the time of implementing the suggested concept. It has a risk associated with the cloud based outsourced environment. The most prominent approach is to control the access towards each application along with some of the traditional role based and authentication approaches. Different type of users has different type of permissions to access the information and functionalities in the application.

6 CONCLUSION:

Cloud computing is the recent area of works which propels the service based usage for software solutions and gaining the interest of users and developers definitely. As the users are occupying towards the cloud based networked software's and resources, the user's authenticity and access control polices get over aged with conventional systems. For controlling this security process various mechanisms had been suggested over the last few years and among them the work focused its intension towards role based access control. The role based access control always depends upon the assigned role of the user, but sometimes it makes the security attacker more active regarding the variable information. Thus, if the number of persons using the system is high, then the data theft issues are more.

REFERENCES

[1] Muhammad Rizwan Asghar, Mihaela Ion, Giovanni Russello, and Bruno Crispo. ESPOON: Enforcing Encrypted Security Policies in OutsoEnvironments. In The Sixth International Conference on Availability, Reliability and Security, ARES'11, pages 99–108, August 2011.

[2] Dongyoung Koo, Junbeom Hur & Hyunsoo Yoon, "Secure and efficient data retrieval over encrypted data using Attribute-based encryption in cloud storage", in Computers and Electrical Engineering Journal of Elsevier, ISSN: 0045- 7906, doi:10.1016/j.compeleceng.2012.11.002, Vol. No 39, Jan 2013. pp 34–46

[3] Muhammad Rizwan Asghar, Giovanni Russello, and Bruno Crispo. Poster: ES POONERBAC: Enforcing security policies in outsourced environments with encrypted rbac.

In Proceedings of the 18th ACM conference on Computer and communications security, CCS '11, pages 841–844, New York, NY, USA, 2011. ACM.

[4] Shucheng Yu, Cong Wang, Kui Ren & Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", in Proceedings of IEEE Infocomm., ISSN: 978-1-4244-5837-0/10, 2010.

[5] Guojun Wang, Qin Liu, Jie Wu & Minyi Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", in Computer & Security Journal of Elsevier, ISSN: 0167-4048, doi: 10.1016/j.cose.2011.05.006, Vol. No. 30, July 2011. pp 320- 331

[6] Deyan Chen & Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", in International Conference on Computer Science and Electronics Engineering, IEEE Computer Society, ISSN: 978-0-7695- 4647-6/12, doi: 10.1109/ICCSEE.2012.193, 2012.

[7] Stephen S. Yau & Ho G. An, "Confidentiality Protection in Cloud Computing Systems", in International Journal of Software Informatics, ISSN 1673-7288, Vol.4, No.4, December 2010, pp. 351-365

[8] Mohemed Almorsy, John Grundy & Amani S. Ibrahim, "Collaboration-Based Cloud Computing Security Management Framework", in 4th International Conference on Cloud Computing, IEEE Computer Society, ISSN: 978-0- 7695-4460-1/11, doi:10.1109/Cloud.2011.9, 2011.

[9] Daryl C. Plummer, Thomas J. Bittman, Tom Austin, David W. Cearley & David Mitchell Smith, "Cloud Computing: Defining and Describing an Emerging Phenomenon", in Gartner Research Publication, ID Number: G00156220, June 2008.

[10] Pardeep Kumar, Vivek Kumar Sehgal , Durg Singh Chauhan, P. K. Gupta & Manoj Diwakar, "Effective Ways of Secure, Private and Trusted Cloud Computing", in International Journal of Computer Science Issues, ISSN (Online): 1694- 0814, Vol. 8, Issue 3, No. 2, May 2011.

[11] Seny Kamara & Kristin Lauter, "Cryptographic Cloud Storage", in Microsoft Research Article.

[12] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Pelosi & P. Samarati, "Encryption-based Policy Enforcement for Cloud Storage", in IEEE Transaction, at Universita degli Studi, di Milano, 2010.

[13] Kan Yang, Zhen Liu, Zhenfu Cao, Xiaohua Jia, Duncan S. Wong & Kui Ren, "TAAC: Temporal Attribute-based Access Control for Multi-Authority Cloud Storage Systems", in IEEE Transaction, 2011.

[14] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Xiaorui Gong & Shimin Chen, "POSTER: Temporal Attribute-Based Encryption in Clouds", in ACM Journal, ISSN:978-1-4503- 0948-6/11/10, Oct 2011.

[15] Sushmita Ruj, Amiya Nayak and Ivan Stojmenovic, "DACC: Distributed Access Control in Clouds", in International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-1, ISSN: 978-0-7695-4600-1/11, doi:10.1109/TrustCom.2011.15, 2011.

[16] Aditi Vyas, Prof. Hemant Kumar Pathak "Outsourced Security Policy Updates Through Role Hierarchies for Security and Isolation in Cloud Computing ", International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015