ISSN:0975-9646



# Outsourced Security Policy Updates Through Role Hierarchies for Security and Isolation in Cloud Computing

[1] Aditi Vyas, [2] Prof. Hemant Kumar Pathak
*Department of Computer Science & Engineering*
*Sushila Devi Bansal College of Technology, Indore (M.P) -453331, India*

***Abstract:*** **Cloud computing is a shared medium used for effectively utilizing the resources to deliver computing capabilities as a service. It gives a combined effect derived from multiple computing paradigms such as distributed, autonomic, grid, elasticity and utility. The cloud provides services in browser dependent environment from trusted third party server. Here, elasticity offers varying load on the processing servers with a large number of users simultaneously working on distributed applications and hence their verification and authorization become less concern process. Taking the advantage of this less secure transition, insider or outsider attacker tries to destroy the data privileges by accessing and modifying the records without permissions. It gets controlled by using some role based access control and fine grained access policies. But still the traditional systems of the RBAC model get the process stuck in performance ad updates bottleneck. Also the verification, policy allotment, role activation and continuous monitoring of users' behavior is still not achieved. This paper presents a new model for handling outsourced policies with their updates using role hierarchies based allotment. Such operations make the users data more isolated from other processes, users and exchanges. The aim is towards making the policy based security more robust and reliable through multilevel verification and authorization. At the analytical evaluation, approach is proving its strong presence in front of existing system and future result will guide various applications security considering cloud based outsourced environment in mind.**

***Index Terms*****:** Cloud Computing, Security, Confidentiality and Access Control, Role Based Models, Policy Updates;

## I. INTRODUCTION

Cloud computing is the recent area of work, gaining popularity due to its service based process handlings. Hire the competing offers various processes as a service to the users. For providing this, various existing computing methodologies are sharpened to satisfy the user's needs of computationally efficient software usages as per needs. It is the combination of distributed processes, scalable computing, fault tolerant capability and billed as per their consumption only. Here the services and data are outsourced to different locations and an intermediate provider which decreases the users trust over the system. User requires a trusted environment for making its data access more secure. Also the provider's faces several problems related to this high end integration of device and systems for transferring the services to the end users. 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 [1].

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. Consistent and computationally effective configurations are required to deal with such problems. Likewise, the service providers to the users are not aware about the user requirements and how to enforce such security policies on these users. Without these policies, security is not being effectively applied by which the data security is not guaranteed. The policies embraced on such services needs to be reliable and transferable according to the users and provider's requirements, unable to achieve these reduce the controls on security. As of now it is clear that actual service deployments and service handlings is not reliable as they claims due to their unorganized and lesser secure migrations [2].

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.

This work focuses its intentions towards achieving following goals:

(i) 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.
(ii) Users can access the data according to their roles and each role is having different of separate policies for data transfer.
(iii) 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.

## II. BACKGROUND

As cloud is gaining popularity, their application areas and users is also increasing abruptly. Now , there are so many areas which are successfully using cloud applications with their other software's and process like government and healthcare organization is now using data outsourcing. Even with higher benefits of cloud service architectures there are various issues which are associated with this shifting and degrades its data outsource values. As outsourced environment is facing problem with preserving data confidentiality because here the data is in easy reach of service providers that cloud gain interest for some unauthorized access. Thus some work needs to be planted for achieving high confidentiality of data which analyses the users sensitivity of information for its data and lets it be secure from cloud and other users [3].

Data security can be guided by effective access schemes such as two factor authentications with robust infrastructures that resist reparation by some unauthorized entry. It is achieved by defining and implementing the life cycle of data security and isolating the information of several users by using tagging at storage areas and files. The regular data backups, with customers being able to audit their basic parameters (scope, save intervals, save times and storage duration). It must also assure that the data is fully and reliably deleted at the customer's request and using unauthorized access of this data comes under juristic boundaries [4]. All these policies need to be predefined by the providers and users using several SLA's lack of which causes data losses [5]. It comes under the category of rights and ID (Identification) management.

In security, data access control is fully derived by effective identity and rights managements. It should be defined by cloud service provider and measured and evaluated by end user through suitable organizational personal and technical teams. The basis for this support can be either that a service provider supplies the customer with an ID management system themselves, or that they supply interfaces to external identity providers. For both models, service providers with or without an integral ID management system, the issues of authentication and authorization which need to be mapped in Cloud Computing platforms [6]. In cloud based environment the services, devices and software's is used by several users. The role based system and authorization ensures that only the person with defined role and authorized personal may use resources. Role based data access and control (RBAC) is the most prominent field of work for cloud improvements. It is used for safety and security critical systems with strong authentication of two factors. Here strong authentication schemes mean two factors i.e. one hardware car or chip and other is software like one time password etc.

The defined policy based right managements system must ensure that each role may only see the abstract data required to complete the task only by which confidentiality is guaranteed. Means each data and users information must be isolated from each other. Also the access control and rights should be reviewed and monitored regularly with least privileges should be used to achieve the task. So finally the components required to work with role based data access is two factor authentication, Role based data access with regular monitoring, least privilege model and critical administration. It should be designed by considering following factors design effectively:

(i) Types of data,
(ii) Functionalities and interfaces
(iii) Format of the data
(iv) Defined Users Role
(v) Policies for a role in accessing the isolated data

To clearly analyses the factors and parameters which affect the most in cloud security various research papers are studied and guided this work presented in the next section of this paper**.**

## III. LITERATURE SURVEY

During the last few years cloud learning's and researches are getting sudden increased in the area of academics as well as industries. The aim is towards improvements of some models by which application usages can be made more delightful and secure with effective administration controls by the providers.

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 fro 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.

In some paper, a special subjective study is focused in which the insider's attacks are taken as a critical issues rather than outsider attacks. These insider attackers are due to some internal authority tries to leak the information for commercial benefits. It cloud be cloud service provider itself and hence some more robust security mechanism is required for such situations. The paper [8] presents a confidentiality approach for making the data more secure against provider. The approach is containing three main components: Isolation of software and infrastructure service provider, Owners information hiding with service

orchestration and data obfuscation. Experimental results are presented to show that our approach has level-headed performance.

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 gets stucked 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. The article had also surveyed the benefits such architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.

To overcome this limitation of above papers the article [13] presents an approach that does not require complete trust in the external service w.r.t. 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 evaluation is measured on resources and on a hierarchical key structure that limits both the number of keys to be maintained and the amount of encryption to be enforced.

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. The approach is feasibly achieving its goal of temporal access control on attribute-level rather than user orientation even with the providers. Also, it does not require re-encryption because of its varying attribute revocation functionality and hence proves its effectiveness than other existing techniques.

Similar to above schemes some other work apart from attribute revocation can be used by other authors for further improvements and given as TABE (Temporal Attribute Based Encryption) [15] and DAAC (Distributed Authentication and Access Control) [16] in cloud computing. While TABE implement temporal constraints for data access control in clouds with a nearly linear-time complexity and constant size for private-key & ciphertext. But DAAC is having one or more KDCs distribute keys to data container and users and owner encrypts the data with its behavioural attributes and let them store in trusted cloud locations.

## IV. PROBLEM STATEMENT

After studying the various factors which compromises the cloud security at third party locations, it is found that some problem remains unaddressed and needs to be solved for high end security. Also by using role based access, the privileges are effectively defined and make the system more reliable and robust for any vulnerable situations. So many approaches had worked with information accountability which makes the data traceable and transparent usages. Also the requirements suggests that the data owner can track the data and identify whether the SLA's are implemented or not along with enforcing the new policies and access control and usage control rules. Also the system should make the generated log also secure because it contains sensitive information about the data and leaking of which causes security loss. Thus after considering all the facts and points, there are some identified areas of work given as:

*Problem 1:* In third party cloud locations, user's loss controls on data and hence the security is compromised. Thus some policies needs to be defined by which regular monitoring of data access needs to be applied and is not available with traditional mechanism.

*Problem 2:* Traditional cloud application allows user to apply any modification without knowing its authenticity and working areas. Also the isolation of the same data to different persons is not effectively defined. Thus some novel mechanism is required with additional policies by which data access and privileges can be defined according to the user's role.

*Problem 3:* Normal data access should be treated as transaction system always because each user is having sensitive and precious information. Traditionally, only some of the application are satisfying this property and having high security. To achieve this two factor authentication (Hardware and Software Combinations) should be used.

*Problem 4:* Handling of several roles, their activation, monitoring and deactivation needs to be handled effectively and hence requires least privilege model. Traditionally this was not defined and hence dynamic roles handling is required.

To serve the above need for higher and maintainable security policies this work proposes a novel outsourced security policy updates through role hierarchies for

isolation in cloud computing. The approach will deals with all types of security situations in cloud environments and works towards increasing the trust over the system for end user. The work also analysed the existing service delivery models of cloud computing and identifies that the resources of cloud services based on may be owned by multiple providers. Thus the work also proposes a novel security model with enhanced mechanism.

## V. Proposed Approach

This work proposes a novel outsourced security policy updates mechanism using role hierarchies for improved and robust data access and isolation in cloud computing. The approach is a role based access model with newly integrated methods for further enhancements in security and users trust over the system. The suggested work uses two way authentications which includes a combination of software and hardware along with some defined policies for each role of users. These roles are further activated and deactivated as per the need of data access. The policies allotted to these rules should contain the least privileges required for completing the task.

The phenomenon of role based access and least controls are based on the verification process for role allotments to the user. As per the needs and it defines some policies for making the roles and privileges updates regularly to the provider and users. It decides a clear separating boundary between the user and its defined roles.

Usually, in cloud computing the technologies and their integration are measured in terms of the successful service delivery with data security. In a third party environment data security can be breached by both insider and outsider. In case of an outsider there are so many mechanisms available like intrusion detection and process blockers. The suggested work will guide the overall role allotments and data access using the defined policies and will store them for futuristic usages. The work also defines various roles repositories along with controlling administrative authorities.

The suggested work can be practically achieved by categorizing the requirements into function based modules. Here these modules are taken as components for integration and development. Each component will work as individual entities and serves as defined policy based architecture. Components and their step wise working is visualized in figure 1.

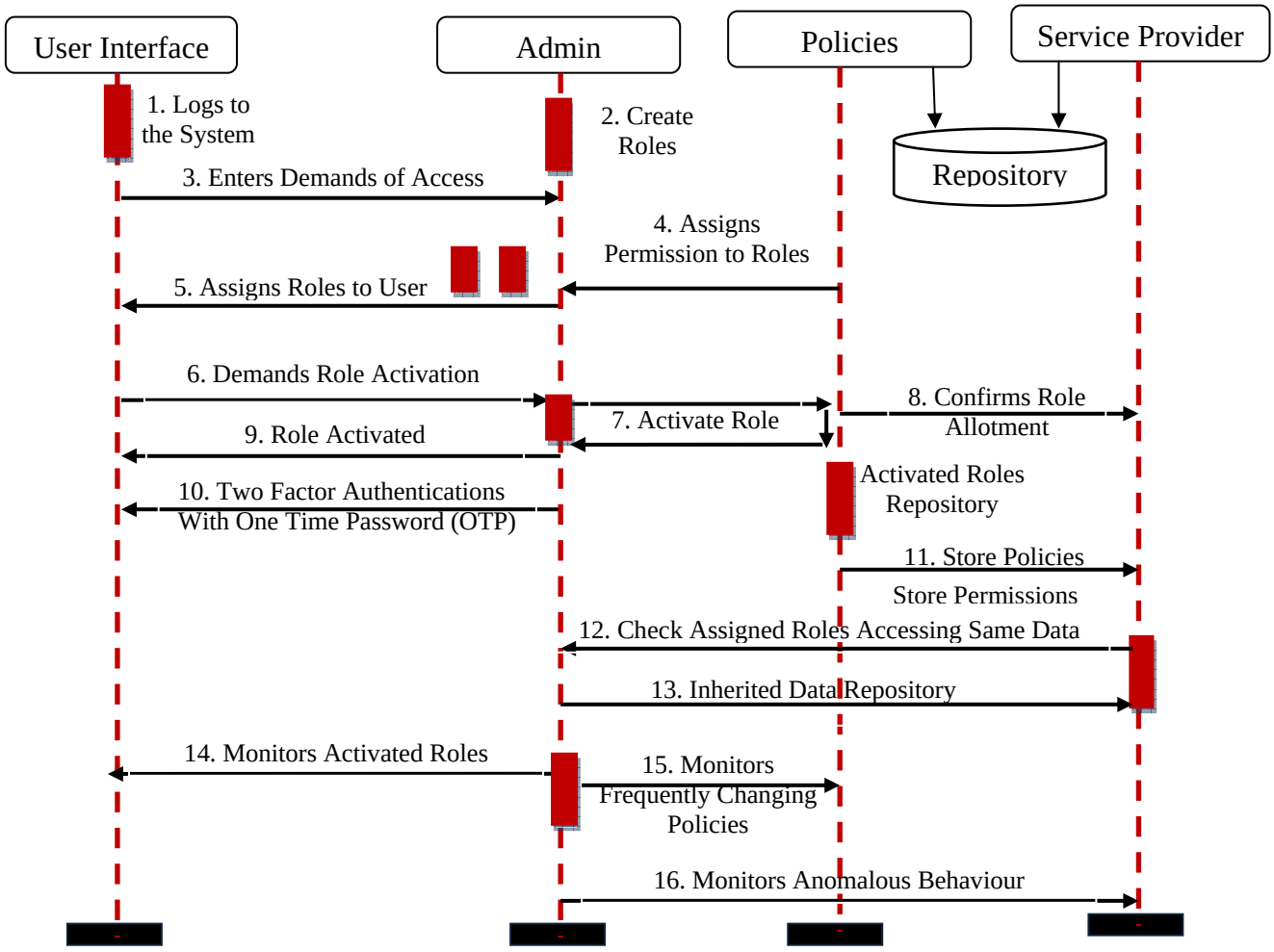


Figure 1: A Novel Outsourced Security Policy Updates Mechanism Using Role Hierarchies

**Components**

(i) **User Interface:** It serves the user oriented services to satisfy the requirements of security user's role based access. This component regularly generates the demands for different privileges and forwards them to other authorizing interfaces.

(ii) **Admin Interface:** It creates the roles according to user demands and configures the policies and privileges for accessing the data. The admin interface also directs the policy creator and users about their rights and authentications.

(iii) **Policy Interface:** This component works as verification for policy updates and role allotments. It also assigns the roles and verifies the permissions.

(iv) **Service Provider:** It works as providers for dealing and initiating all the service types and user requirements for which policy needs to be created. It will also work for verification in combination with admin and policy interface.

(v) **Repository:** It works as storage and retrieval location where the entire current and previous configuration is stored. It also holds the policies and role allotment details for each respective demand.

**Description:** The suggested approach works towards improving security of cloud based data access using role based access control using policy updates. Hence the works start with users demands for logging to the system for accessing data or using some service as a user role access privileges. For each users request of different types, service and requirements, admin will creates different roles. At the same time when a role is created it needs to be assisted with some controls of policy interfaces. Thus policy interface assigns permissions to each roles transfer them to admin control, after which it has to be assigned to the demanded user. Permission and their respective roles are being regularly stored to repository for further usages and data analysis. After role assignments these roles need to be activated after the confirmation from admin, policy and service provider interfaces. Before this role is completely activated another security policy with two factor authentication is applied by which at one time password is generated to verify the end users authenticity and isolation.

After the role assignment and activation is complete and the user is continuously operating on its terms and rights, regular monitoring is performed to identify the sudden change is user's behaviour and roles which confirms some unauthorized activity. The monitoring service will check that assigned roles was accessing the same data irrespective with other data and privileges for complete isolation. Monitoring and admin interface will also verify the inherited data repository with frequently changing nature of, user or its rules for anomalous behaviour. It cloud be analyzed by storing repository data or some change in the fields of regular operations.

The above approach will work as an effective policy sharing and distribution of access according to the user roles. By the suggested mechanism role based access control can be further improved with regular monitoring and policy updates. It will also help in identifying of anomalous behaviours or user and will control the data access by formal privileges distribution and allotments. Each time a user need to access the data, it should select the role after which policy can be viewed and applied. Thus, at the initial level of work with cloud authentication and authorization, the works seem to provide effective results on integrating with various real time application areas.

**Applications**

Various policy based mechanisms are bieng proposed through the last few years to facilitate the user based on the policy for improved data access mechanism.

- Credit Based Systems
- Social Networking
- Outsourcing Based Storages for Commercials
- Healthcare Industry
- Insurances Firms
- HR Management Primitives
- Disaster Recovery and Business Continuity

## VI. Result Evaluation Factors

This section gives the parameters of evaluating the suggested work in terms of the computation overhead, Means of Revocation, Access policies and Key and Ciphertext size.

- *Computational Overhead:* This step is used to identify the computation overhead required to execute the suggested approach. It will be measured in terms of CPU cycles, and Size in MB for executing the suggested policy framework. The main computational overhead of this operation is the encryption of the data file using the symmetric
- *Access policies:* These are some user designed policies required to control the access for different data at third party locations. It can be measured in term of numeric values and set of rules which measures the accurate and exact measures. It can be taken as a number of time users demanded the data and for the same correct data is fetched and the policies required do so.
- *Means of Revocation*: It gives the details regarding the types of access policies required and the revocation methods used to forwards the desired data to the users. This operation is composed of two stages. The first stage occurs between the data owner and Cloud Servers. The second stage can actually be utilized as the file access operation. Here we just count the operating overhead for the first stage. That for the second stage will be included in the file access operation.
- *Key and Ciphertext Size:* It is again a very important parameter used to detect the authenticity of the suggested approach. It gives the actual size and complexity of practical implementation of the suggested approach.

## VII. EXPECTED BENEFITS

Cloud computing is an outsourced environment where service, location and process transparency is very critical aspects. In absence of that the trust in the system gets degraded loose security policies. The suggested work will work towards achieving high security with less overheads and managerial controls. At the primary level of works and evaluations the approach provides following benefits:

1) Data isolation and effective access control can be provided by updating policies for role based access control.
2) Role allotment and access privilege are controlled by two factor authentication and hence the security over the system and trust gets increased.
3) Inside, outsider and impersonation types of attacks are removed easily with small policy verifications
4) Regular monitoring of role creating, allotment, permissions decisions, usages and changing natures of privileges can lead to easy identification of anomalous behaviour.
5) Usage and role policies are used here to define the finer grained access control and its reliability can be maintained by log monitoring.
6) High reliability and lesser cost of operations.
7) The work also ensures confidentiality of log files so that the service providers cannot deduce useful information about roles and policies.

## VIII. CONCLUSION

Cloud computing is the recent area of works which motivates the service based usage for software solutions and gaining the interest of users and developers very drastically. As the users are diverting towards the cloud based networked software's and resources, the user's authenticity and access control polices get over aged with traditional systems. For controlling this security process various mechanisms had been suggested over the last few years and among them this work focuses 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. Thus to overcome these issues and interrelated problems this paper proposes a novel outsourced security policy updates mechanism using role hierarchies for improved and robust data access and isolation in cloud computing. Formal drafting and integration with selective policies makes the works satisfying the current user group demands.

## FUTURE WORK

Some problems and concepts that remain unaddressed can be performed in the future as a theoretical background, but the first thing is to develop a prototype so as to prove the results. Such as with the help of existing role based models some of the modifications can be further made in suggesting model. The future aspects also cover the accurate analysis of policies and exchanges of controls for different privileges. The accuracy and viability of the approach has to be identified more effectively. Later on, some authenticated role assignment process can be designed. It can also be used for quantitative & qualitative analysis etc.

## ACKNOWLEDGEMENT

The work is evaluated and drafted with the help of some of the authorities of the SBDCT institutes which leads me to the great outcomes. Without them it would not be possible for me to overcome the problems and issues faced. Thus, the authors thank the anonymous reviewers for their valuable comments, which strengthened the paper. They also like to give thanks to Prof. Hemant Kumar Pathak and head of the dept. Prof. Ritu Gupta, who had guided me throughout this research and being held always for discussion regarding the cloud security and polices & for producing the approach adapted for this paper.

## IX. 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.