Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

APRBM: Audit Policy Role Boundary Model for Enhanced Data Security and Isolation in Cloud

Ms. Priya Saxena
CSE & RGPV University
M.P, India

Mrs.Shweta Mishra
CSE & RGPV University
M.P, India

Abstract*—Heavy load of all types of huge amount of data, software, and other resources has increased on the internet users with the improvements in internet technology. Hence a technology was developed which helped the user to store all their data, software or other information to a remote party which is today known as cloud. Therefore user has no burden to store and keep such huge amounts of data. Users or organizations also need to share their data with other users or customers, cloud helps in doing so. It is also called Outsourcing or keeping data on a third party. Therefore here also come issues like confidentiality, privacy, isolation and security of the owner's as well as user's data. The proposed APRBM model deals with encrypted policies through regular updates using existing RBAC (Role Based Access Controls) and ESPOON-ERBAC (Enforcing Security Policies in Outsourced Environments). The suggested mechanism gets the logs updated regularly and revert the information to the owner of data for current configuration's accuracy detection. The approach is also generating the audit logs for further achieving confidentiality of data and log. The files are retrievable at any point of time by the owner with frequent handling of access privileges and authentications to these files. At the evaluation, analysis, the approach seems to serve the user security needs of the third party based storage with higher trust over the system.

APRBM satisfies the user's security requirements by the path which directs the futuristic technology creators to make robust applications. Section I puts the introductory requirement for the study, which later on makes it more detailed in its further sections. Section II describes the background information so that one can understand the phenomenon. Continuing the approach categories section III gives the study of several research articles related to the concepts. Section IV identifies some of the issues which remain unsolved by the existing mechanism. Section V, VI and VII presents a solution to overcome the issues with its complete study over the various parameters for proving the authenticity of the approach.

***Keywords*— Auditing, Encrypted RBAC, Audit Policy Role Boundary Model (APRBM), Cloud Storage, Confidentiality.**

I. Introduction

Cloud computing is an integrated technology evolving the usage of grid, distributed, utility and autonomic computing. Taken as much consideration of how strongly the provided model is secured, consumers continue to suffer from data loss due to lack of trust on the provider. On the other end, the provider faces a complex problem of handling data of such its untrusted users. Lot of efforts & dimensions has to be wasted while providing such secure architecture & dependency stack. Such outsourced data enables end users and large enterprises to process and store huge amount of data at very low cost [1]. It provides higher availability, scalability, and more enhanced quality of service than in-house solutions. These large numbers of varying dimensions result in unmanaged heterogeneous security controls that must be consistently handled. Moreover, the cloud providers host services of users about which they are not aware of these security requirements to be enforced on such services. It leads to a loss of security control over these services and the cloud platforms. Thus cloud computing service providers touted the security and reliability of their services; actual deployment of cloud computing services is not reliable as they claim because the existing security model doesn't work after migration of services to clouds [2]. This migration follows multitenant model and cloud computing is bringing remarkable impact on information security fields. Such issues generated because of following features of cloud:

(1) Feature of Service Abstraction
(2) It is Dynamically Scalable
(3) It has Location Transparency .

Various sectors including government and healthcare, are now adapting to the concept of data outsourcing. Despite all its advantages, data outsourcing raises serious security concerns for preserving data confidentiality. The main issue is that the data stored in outsourced environments are within easy reach of service providers that could gain un-authorized access. There are several solutions for guaranteeing confidentiality of data in outsourced environments.

The cloud computing model is a new methodology which delivers computation resources as a service to the consumers. It is a highly scalable distributed computing platform which offers managerial benefits to both creators & consumer. This service model faces a number of open issues that impact its credibility. Measuring benefits among all security services is considered as one of the high priority open issues in adopting the cloud computing model. Data confidentiality against cloud servers is hence repeatedly desired when users outsource data for storage in the cloud [3]. Thus the security issues are generated because of these low trusted outside processing entities such as providers. Thus the trust factors at such services are very low. The consumer always likes to make its data & service in an isolated manner of external persons. In few practical situations of service application systems the data confidentiality will come under juristic boundaries by taking their security issues [4]. For example disclosure of Healthcare information from company to consumer is a legal act. Thus it needs to be taken as more secure data and when it is handled by providers, there is an always way to do is open. Thus to make the system more reliable client needs to make some security trusted deals with its data. In some cases the cloud user will share their data among other consumers, but in a restricted access manner. There are several issues associated with access controls & data isolations for cloud consumers about cloud security such as

(1) The loss of control over cloud hosted assets

(2) The lack of security guarantees in the SLAs between the cloud provider and cloud consumer; and [5]

(3) The sharing of resources with competitors or malicious users [6].

To overcome the above problems, several novel approaches, based on the notion of information accountability focuses on keeping the data usage transparent and traceable. The data owners can track not only whether or not the service level agreements are being implemented, but also enforce access and usage control rules as needed. Based on the feature of accountability, two types of log files are generated The regular log refers to logs being generated periodically and sent to the stakeholder while the alternative approach refers to scenario where the user(or another authorized party) can retrieve the logs as needed. The main issues are uniquely identifying the service provider, ensuring the reliability of the log files and to maintain the confidentiality of the log files so that service provider is not able to learn the roles of the user on data and their policy management.

This work proposes a novel Audit Policy Role Boundary Model (APRBM) to provide higher security with less concern management. It focuses on features of cloud computing models for all kinds of applications and data on the cloud platform which have no fixed infrastructure and security boundaries. The work will also consider the event of a security breach, which overcomes from data isolation issues. 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 mechanical.

II. LITERATURE SURVEY

Maintaining data confidentiality within the outsourced environment is one of the research area .Several work specifying techniques to have been proposed allow authorized users to perform efficient queries on the encrypted data while not revealing information on the data and the query have been proposed. During the last few years various authors had worked on scalable cloud computing for its further improvements regarding its security. Among them few articles are gives here as a related content to the specified paper. It is well-known that cloud computing has many possible advantages and many applications and data are migrating to public or hybrid cloud. In the paper [7], authors had provides a brief but all-round analysis on data security and privacy protection issues coupled with cloud computing across all stages of data.

Protections of users’ data from outside attackers are available, but currently there is no effective way for protecting users' sensitive data from service providers in cloud computing domains. In the paper [8], an approach is presented to protecting the confidentiality of users' data from service providers, and ensures that service providers cannot access or disclose users' confidential data being processed and stored in cloud computing systems. The approach has three major aspects:

1) To separate infrastructure service providers and software service providers.

2) To hide information of the owners of data

3) Obfuscation of Data. An example to show how our approach can protect the confidentiality of users' data from service providers in cloud computing is given. Experimental results are presented to show that our approach has level headed performance.

Although the cloud computing model is considered to be a very promising internet-based computing platform lacks the security constraints in the Service Level Agreements. These SLAs are formed between the cloud providers and consumers results in a loss of trust. Obtaining a security certificate such as ISO 27000 or NIST-FISMA would help cloud providers improve consumers trust in their cloud platforms’ security. In this paper [9], the authors introduce a new cloud security management framework based on aligning the FISMA standard which enables security certification. The suggested framework is based on improving collaboration between cloud providers, service providers and service consumers. The results are evaluated through the framework by managing the security of a multitenant SaaS application. Similarly the various type of SLA is managed and established between consumer and provider likewise given [10].

Some of the previous research gets blocked at trust factors and threshold calculations. A proper model of such mechanism is still not developed. Thus in the paper [11], the author proposes a novel mechanism to provide the security and trust to share the data for developing cloud computing applications. The paper is also giving some countermeasures to earn those trusts and provide the security, privacy and reliability, when a third party is processing sensitive data in a remote machine located in various countries? A concept of utility cloud has been represented to provide the various services to the users. But some of the researcher considers the problem of building a secure cloud storage service on top of a public cloud infrastructure. It is again a issues related to trust identification where the service provider is not completely trusted by the customer [12]. This paper 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.

TAAC (Temporal Attribute based Access Control) [14], an efficient data access control scheme for multi-authority cloud storage systems, where the authorities are independent from each other and no central authority is needed. TAAC can efficiently achieve temporal access control on attribute-level rather than on user-level. Moreover, different from the existing schemes with attribute revocation functionality, TAAC does not require re-encryption of any ciphertext when the attribute revocation happens, which means great improvement on the efficiency of attribute revocation. The analysis results show that TAAC is highly efficient, scalable, and flexible to applications in practice.

Similar to the above proposed phenomenon a little work as been done on secure cloud factors that explores cryptographic temporal constraints, especially for data sharing. This paper presents a temporal attribute based encryption (TABE) scheme to implement temporal constraints for data access control in clouds [15]. This scheme has a constant size for ciphertext, private-key, and a nearly linear-time complexity. In addition, it implements a prototype system to evaluate the proposed approach. Initial experimental results shows not only for validating the effectiveness of the scheme and algorithms, but also shows that the scheme has better performance for integer comparison than BSW's bitwise comparison scheme.

DAAC is proposed in [16] which distribute access control in clouds, where one or more KDCs distribute keys to data container and users. The key distribution centre may provide access to particular fields in all records. Thus, a particular key replace separate keys from owner. The owner and user are allocated a certain set of attributes. Owner encrypts the data with the attributes it has and stores them in the cloud. The users with matching set of attributes can retrieve the data from the cloud. Thus various approaches are suggested based on the runtime environment to improve the user attribute based encryption performance.

III. PROBLEM STATEMENT

Computing inevitably poses new challenging security threats for many reasons. Existing access control approaches are not suitable for cloud deployment. Following features of cloud environments provides hiccups to these approaches:

Problem (I) : Traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying the correctness of data storage in the cloud becomes even more challenging. , data handling can be outsourced by the service provider to other entities in the cloud and theses entities can also delegate the tasks to others.

Problem (II) : Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. Also the entities in cloud follow complex and dynamic hierarchical service chain.

One of the required aspects of data security is to create models of requirements level of security. It gives the extent up to which it needs to be secure.Thus this work extends the concept of encrypted role based access control by providing support for secure auditing .This novel Audit Policy Role Boundary Model (APRBM**)** conducts automated logging and distributed auditing of relevant access performed by any entity, carried out at any point of time at any cloud service provider. The primary objective of this work is stated :

- To develop a security framework for cloud that can work on cross platform.
- To propose a novel Audit Policy Role Boundary Model (APRBM**)** for providing improved security through audit policy updates and encrypted role based policies
- To clearly isolate the user access & data transfers.
- To focus which security threats can be unsafe to cloud computing and how they can be avoided.
- To analyze the cloud computing technology architecture and the cloud computing data security features and to elevate the cloud computing data security model.

IV. PROPOSED APRBM APPROACH

In this proposed architecture of Audit Policy Role Boundary Model (APRBM**)** for secure audit mechanism using ESPOON ERBAC. The above mechanism is totally based on verifications process for role assignments thus called as Audit Policies and used for recognising the clear separation between the users according to their role thus called as Role

Boundary. The two types of user namely administrator and requester (end user) interact with data placed in outsourced environment using interfaces. In this approach the prime concern is on providing the better role based access control for securing the data at third part locations. The suggested mechanism has the features of role repositories and log repositories by which understanding the behaviour of user can be done easily.

A. Components:

1) *User: Administrator or Service User* – This means which type of user is going to execute the APRBM to achieve the role based access to the system. It has normal user and administrator among which a separation is identified.
2) *Analysed Policy Interface*- This is used for analysing the policies generated for separation of role. It includes the security permission to role after which role is assigned according to the user requirements. These components have a local role storage repository which stores the decisions done by this phase.
3) *Activation Checks*- It measures the taken decisions and their authenticity. It also checks the already executed roles, their inherited mechanism from different role repositories; user details more than one access etc.
4) *Service Providers Role Verifications*- This module checks the current status of roles and let the provider control to reassign role and, activate some new permissions, verifies their usage hierarchies.
5) *Logger/Log Repository*- It stores the final results and categorised them so as to identify some important patters. These identified frequent patters will result the behaviour of different users and their assigned roles. It helps in anomalous behaviour detections.

B. Description:

Initially the cloud user will request for data access which is handled by policy interface which analyses the request and decide the best suited role to make it logged to the system. The permission is granted by assigning roles to the users. More than one user form the same firm can assigns different roles simultaneously. After the appropriate role is activated the request is stored in local role repository database for further usage. These repositories can also handling multiple requests simultaneously for different clouds or third party interfaces. Now the policy interface forwards the generated best suited role according to the user characteristics and usage for data. Now the verifications of existing activated role occurs in which role activations details from activated role repository is checked for previously activated role or not and if yes then still it is active or not. In this verification process the permissions and hierarchies is also verified for their details and role assignments. The concern is to only make the data access order correct so as to improve over the access security breaches.

Simultaneously during that verification some of the already inherited roles are also checked from local repository. After identifications of activations, permissions and hierarchies the results are taken into a log formats. There are two components in this logger and log repository. The logger is downloaded whenever the data are accessed, and is copied along with the data. It manages a particular instance or copy of the user's data and is responsible for logging access to that instance or copy. The log repository allows the user access to the log files. Its functions include automatically logging access to data items that it contains, encrypting the log record, and periodically sending them to the log repository. The log repository is responsible for auditing for both regular and on demand mode. The log repository is also responsible for handling log file corruption.

Now the generated log will contains the details about the user behaviours, their data access, changed policies, updations, and other details for behaviour analysis. This is informed to administrator by some detection mechanism. Thus the work is also been capable of identifying the anomalous behaviour. Finally the administrator assigns the role and monitors the performance of already activated role during the last access.

User makes a request (1) which is forwarded to policy interface. Policy interface forwards (2) it to role repository for appropriate role activation. Role repository (3) after verification makes the role of the active and forwards it to policy interface .Policy store after role activation (4) depending upon permissions to the user provides access to Data store. Data store performs computation and forwards (5) result to Logger There is two components the logger, and log repository.

C. Applications

Various policy based mechanism is been proposed through the last few years to facilitate the user based on the policy for improved data access mechanism.

1) *Commercial Outsourced Storage:* Offsite storage or backup provider can use such secure policy models to make the data separated for large number of users. It can be used through searchable encryption methods through tagging the specific user data structure to each data of different user. It can also provide the backup comforts through policy logging.
2) *Electronics Healthcare Records:* To construct an outsourced healthcare system where patients can securely store their Electronic Health Record (EHR) such policy based decision is required. In their solution, each EHR is associated with a secure search index to provide search capabilities while guaranteeing no information leakage. However, one of the problems associated with CP-ABE is that the access structure, representing the security policy associated with the encrypted data, is not protected.
3) *HR Management Primitives:* Here the proposed work is used for checking all employees' requirements related to sign non-disclosure and confidentiality agreements. It will also check the employee screening policies and selection procedures. Accounts review, periodic updates, legal issues details etc are some other areas of work.
4) *Disaster Recovery and Business Continuity:* At the time of certain natural failures the system needs to be recoverable fast. If the policy load is high and uncertain such efficient recovery is not possible. Thus the propose model will frequently makes the changes for performance factors related to backups and recovery.

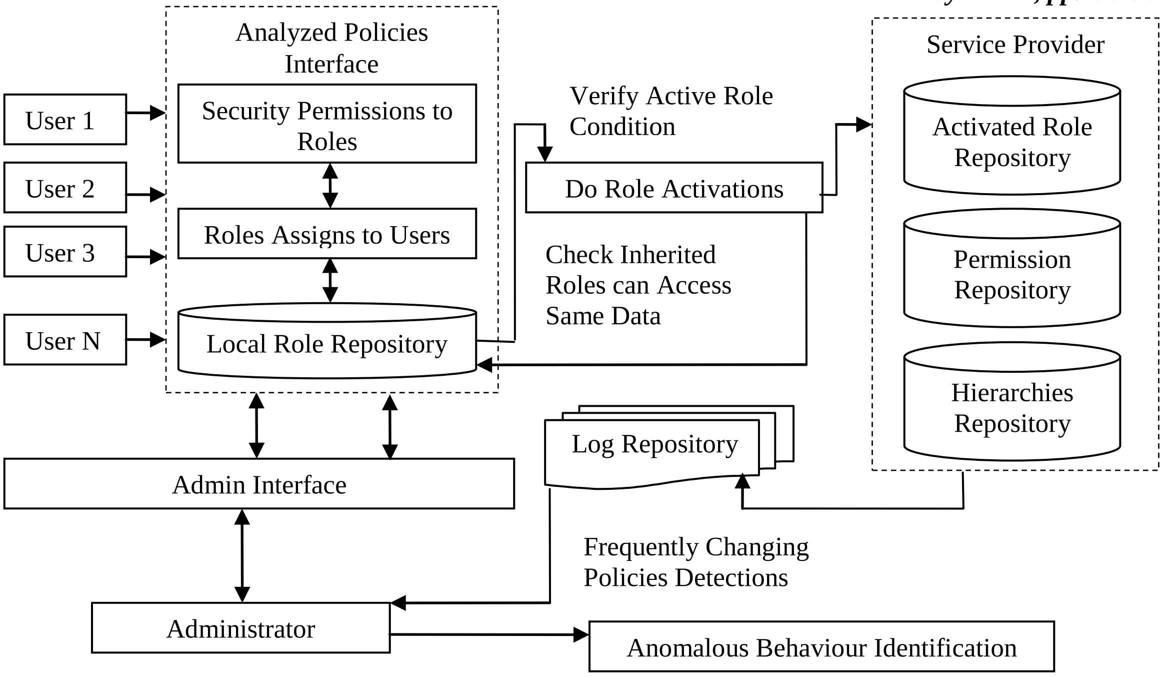
Analyzed Policies Interface
Security Permissions to Roles
Roles Assigns to Users
Local Role Repository
User 1
User 2
User 3
User N
Verify Active Role Condition
Do Role Activations
Check Inherited Roles can Access Same Data
Service Provider
Activated Role Repository
Permission Repository
Hierarchies Repository
Log Repository
Admin Interface
Frequently Changing Policies Detections
Administrator
Anomalous Behaviour Identification

FIGURE 1: ARCHITECTURE OF PROPOSED APRBM (AUDIT POLICY ROLE BOUNDARY MODEL)

V. EVALUATION FACTORS

This section numerically evaluates the performance of proposed APRBM scheme in terms of the computation overhead, Means of Revocation, Access policies and Key and Ciphertext size.

1) *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 computation overhead of this operation is the encryption of the data file using the symmetric
2) *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 doing so.
3) *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 operation overhead for the first stage. That for the second stage will be included in the file access operation.
4) *Key and Ciphertext Size:* It is again a very important parameter used to detect the authenticity of suggested approach. It gives the actual size and complexity for practical implementation of suggested approach.

VI. EXPECTED OUTCOMES

Cloud users typically have no control over the Cloud resources used and there is an inherent risk of data exposure to third parties on the Cloud or the Cloud provider itself. At the initial level of our research proposed APBRM mechanism will provides following benefits over existing RBAC and ESPOON-ERBAC.

1) As compared to many of its existing approaches, data isolation and access control can be guaranteed by using access and key policies for various types of user. Policies are used here to define the fine grained access control.
2) Data owners can monitor whether or not the service level agreements are being followed and identifies the existing policies. It can also enforce some of the new policies which had been approved from higher authorities.
3) Can enforce access and usage control rules for organisational controls for managing information security and level wise data isolation.
4) The works will ensure the reliability of logs and its generation through authenticated users. It will also maintain the information accountability issues.
5) The work also ensures confidentiality of log files so that service provide cannot deduce useful information about roles and policies.

VII. CONCLUSION

The role based access control always depends upon the assigned role to the user but sometime it makes the security attacker more active regarding the varying information. Thus if the number of persons using the system is high then the data theft issues are more. One of the many solutions to this is assigning roles to individuals. For this various approaches is suggested over the last few years and among them RBAC and ESPOON-EERBAC is recognized one. Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations based on audit policy updates on data blocks, including: update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against malicious data modification attack, and even server attacks. Improved security and data access can be implemented in efficient manner. It will also ensure the successful satisfaction of various integrity rules for correctness of data and authentication of user role model. Thus the above work is capable of maintaining those roles by using role repository and identifies the anomalous behaviours easily. The initial measured values of approaches prove its correctness in near future.

VIII. FUTURE WORK

Some problems and concepts that remain unaddressed can be performed in 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 RBAC some of the suggested APRBM model is implemented. The accuracy and viability of 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

This research work is self financed but recommended from the institute so as to improve the security solutions for cloud computing using access control and role based policies. Thus, the authors thank the anonymous reviewers for their valuable comments, which strengthened the paper. The authors also wish to acknowledge SVITS administration for their support & motivation during this research. They also like to give thanks to Mrs. Shweta Mishra 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.

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] Muhammad Rizwan Asghar, Mihaela Ion, Giovanni Russello, and Bruno Crispo. ESPOONERBAC: Enforcing security policies in outsourced environments.Elsevier Computers & Security (COSE), 35:2–24, 2013. Special Issue of the International Conference on Availability, Reliability and Security (ARES).

[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] 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

[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] 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.

[7] 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.

[8] 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

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.