IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

Effective Security Model for Hybrid Cloud Using Multi-Replica with CPDP Approach

K.Vimala[1], K.Suganthi[2]

HOD, Department of Computer Science, Pavai Arts & Science College for Women, Rasipuram, Namakkal[1]

M.Phil Scholar, Department of Computer Science, Pavai Arts & Science College for Women, Rasipuram, Namakkal [2]

Abstract: This paper mainly concentrates on providing secure access of cloud data. As the data stored in the third party server maintains access permission details such that who can access the data. Since the access environment is cloud, multiple user may intends to store and fetch the data. Retrieval details of one user would not reveal to other users due to security reasons. Moreover, this paper provides the achievable security merits by making use of multiple distinct clouds environments with simultaneously in confidential mode. The dual encoding is carried out in the cloud environment which is varied from one group to another for secure data transmission process. Thus, different users are allowed to decode different pieces of data as per the security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access. The paper implements an algorithm namely Enhanced Multi Replica Strategy to CPDP (MRS-CPDP) control policies with user revocation capability. However, secure cloud storage system supports secrecy of the information.

Keyword: Hybrid Cloud, Security Metrics, Revocation, Multi Replica Strategy, CPDP, Hash Index Hierarchy.

I. INTRODUCTION

Cloud computing is a storage of the confidential data for common access. Hence, others use it to mean any computing service provided over the Internet or a similar network; and some define it as any bought-in computer service use that sits outside the firewall. In general, cloud computing communicates over a network where large groups of servers running low-cost consumer PC. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing. Since a common approach for protecting the redistributed data consists in encrypting the data themselves, a promising approach for solving these issues is based on the combination of access control with cryptography. This idea is in itself not new, but the problem of applying it in a redistributed architecture introduces several challenges. This paper illustrates the basic principles for combining access control and cryptography. It then summarizes an approach for enforcing authorization policies and supporting dynamic authorizations, allowing policy changes and data updates at a limited cost in terms of bandwidth and computational power. Some of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates. Encoded text-policy attribute-based encryption is a cryptographic technique which is used to hide confidential data.

Cloud computing creates a large number of security issues and challenges. A list of security threats to cloud computing is presented. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection sphere. Even more, if deploying data-processing applications to the cloud (via IaaS or PaaS), a cloud provider gains full control on these processes. Hence, a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing. Depending on the political context this trust may touch legal obligations. For instance, Italian legislation requires that government data of Italian citizens, if collected by official agencies, have to remain within Italy. Thus, using a cloud provider from outside of Italy for realizing an e-government service provided to Italian citizens would immediately violate this obligation. Hence, the cloud users must trust the cloud provider hosting their data within the borders of the country and never copying them to an off-country location (not even for backup or in case of local failure) nor providing access to the data to entities from abroad.

II. RELATED WORKS

Giuseppe Ateniese [1] proposed a method called as atomic proxy re-encryption, in this method a semi-trusted proxy converts an encrypted text. It doesn't consider the marked plaintext. They prevent that rapid and protected re-encryption will become gradually more popular as a technique for maintaining encoded files. Even though competently

DOI 10.17148/IJARCCE.2017.61056

quantifiable, the wide-spread adoption of re-encryption has been stalled by considerable security risks. This paper includes many proficient proxies re-encryption schemes that offer sanctuary perfection over earlier approaches. The main goal of this paper is that they are unidirectional and do not necessitate delegators to expose their entire security key to anyone – or even interrelate with the delegate – in order to permit a proxy to re-encrypt their encoded. In this method consider inadequate amount of trust is available in the proxy.

Mr.M. Narendra defines the disposition of low safeguarding in cloud computing, it presents an inexpensive and well-organized result for distributing group resource between the users in cloud. Regrettably, distributing data in a multi-authority method whereas conserving information and individuality seclusion from a untrusted cloud is still a challenging issue, due to the recurrent modification of the membership. In this paper implements a secure multi-authority data distributing technique, named Mona, for dynamic groups in the cloud. In dynamic transmit encryption method; each user in cloud can secretly distribute the information with others. Temporarily, the memory transparency and encryption calculation cost of the methods are autonomous with the number of rescind users in the cloud. In addition, this paper describes the privacy of the method with meticulous verification, and implements the efficiency of the methods in experiments.

Michael Hitchens raised the major privacy problem of how to manage and predice the unconstitutional access to the cloud data. The main access control model is role-based access control (RBAC). This method provides flexible controls and management. These management controls done by using two mappings such as users to roles and roles to rights on data. In this paper, it proposes a role-base encryption (RBE) scheme. This scheme combines the cryptographic techniques with role-base encryption scheme. This scheme allows RBAC policies to be imposed for the encoded information stored in public clouds. Based on this scheme, it presents a protected role-base encryption scheme based hybrid cloud. It allows an association to store the information steadily in a public cloud. In addition it describes a practical implementation of the proposed role-base encryption scheme based architecture, and converse the performance results. To implements that cloud users only need to keep a single key for decryption and system operations.

Ning Shang proposes a major issue in public clouds, such as how to particularly distribute a file based on the fine-grained attribute based access control strategy. This approach is used to encode files fulfilling variety of policies with multiple keys by using a public key cryptosystem such as attribute based encryption; in addition it includes proxy re-encryption. Nevertheless, this approach has some drawbacks: it doesn't proficiently handle including/eliminating cloud users or uniqueness attributes, and strategy modifications; it needs to keep different encoded copies of the same files; it acquires high cost during computational. It contains direct application of a symmetric key cryptosystem. In this system users are clustered based on the strategy then it satisfies and assigning different keys for each group in cloud, also has similar drawbacks.

III. ENCODED DATA FOR COLLUSION AVOIDANCE

In encoded data for collusion avoidance phase, attributes are used to describe the encoded data and access policies are defined based on user authorities. Hence, the transmission data can be encoded based on authorities and attributes they sustained on. The revocation process is controversy in cloud communication systems, since each user will be assigned with one single attribute. It also defines the affects due to the revocation of users from the group. In existing system, attribute-based access control scheme using data encryption scheme with efficient attribute and user revocation capability for data outsourcing. Even though in the majority of cases it may be legitimate to assume a cloud provider to be honest and handling the customer's affairs in a respectful and responsible manner, there still remains a risk of malicious employees of the cloud provider, successful attacks and compromization by third parties, or of actions ordered by a subpoena.

Data owner redistributes data to the external data server provided by the service provider by defining access policy, and enforcing it on its own data by encrypting the data under the policy before outsourcing it. If cloud user possesses a set of attributes satisfying the access policy of the encoded data defined by the data owner, and is not renounce in any of the attribute groups, then the user will be able to decrypt the encrypted text and obtain the data. Storage provider consists of data servers and a data service manager. The cloud service provider is in charge of controlling the accesses from outside users to the redistribute d data in servers and providing corresponding contents services.

The following are the drawbacks of encoded data for collusion avoidance system:

- Managing the redistribute data copies in a confidential manner is difficult.
- Other cloud user can easily track the path of data to know from which cloud server the data has been transmitted.

DOI 10.17148/IJARCCE.2017.61056

- The one who owns need to take charge of maintaining all the membership lists for each attribute group to enable the direct user renounce.
- Keys are generated in discriminate manner to provide security among other cloud users.
- User can be renounce from particular group. After revocation, key assigned to the renounced user will be redefined and reused for another new user.

IV. HYBRID CLOUD DATA SIMULACRUM TECHNIQUE

In a cloud environment, a file in its totality, stored at a node leads to a single point of failure. A successful attack on a node might put the data confidentiality or integrity, or both at risk. The aforesaid scenario can occur both in the case of intrusion or accidental errors. In such systems, performance in terms of retrieval time can be enhanced by employing replication strategies. However, replication increases the number of file copies within the cloud. Thereby, increasing the probability of the node holding the file to be a victim of attack the cloud manager system (a user facing server in the cloud that entertains user's requests) upon receiving the file performs: (a) fragmentation, (b) first cycle of nodes selection and stores one fragment over each of the selected node, and (c) second cycle of nodes selection for fragments replication. The cloud manager keeps record of the fragment placement and is assumed to be a secure entity.

A. Multi replication of resource Model

This Fig 4.1 architecture enables to verify the integrity of results obtained from tasks deployed to the cloud. On the other hand, it needs to be noted that it does not provide any protection in respect to the confidentiality of data or processes. On the contrary, this approach might have a negative impact on the confidentiality because due to the deployment of multiple clouds the risk rises that one of them is malicious or compromised. The idea of resource replication can be found in many other disciplines. In the design of dependable systems, for example, it is used to increase the robustness of the system especially against system failures. In economic business processes and especially in the management of supply chains single-source suppliers are avoided to lower the dependency on suppliers and increase the flexibility of the business process.

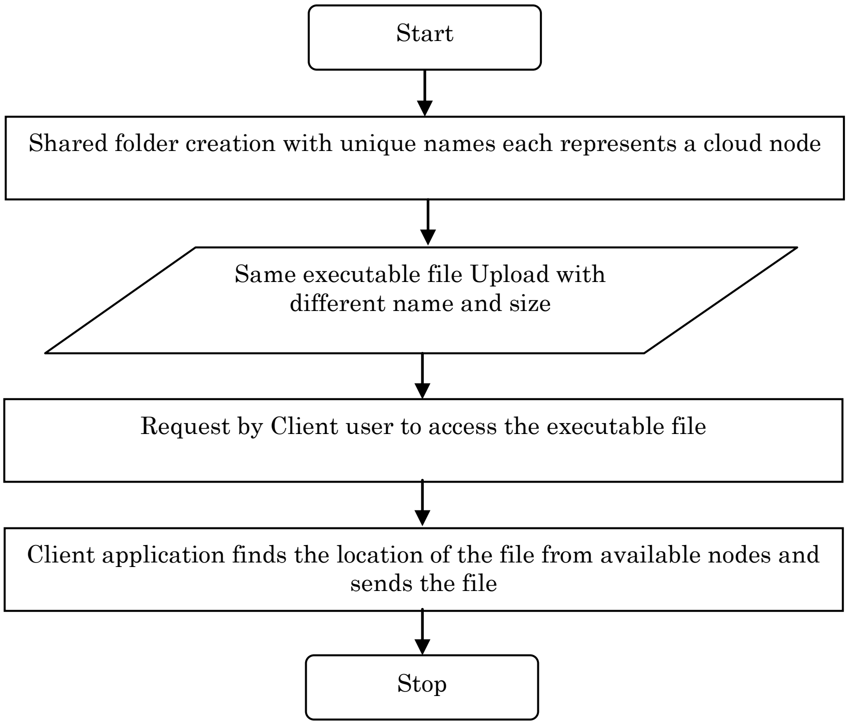
Start
Shared folder creation with unique names each represents a cloud node
Same executable file Upload with different name and size
Request by Client user to access the executable file
Client application finds the location of the file from available nodes and sends the file
Stop

Fig 4.1 Replication of Resource

B. Logic Fragments

This architecture variant targets the confidentiality of data and processing logic. It gives an answer to the following question: How can a cloud user avoid fully revealing the data or processing logic to the cloud provider? The data should not only be protected while in the persistent storage, but in particular when it is processed. The idea of this architecture is that the application logic needs to be partitioned into fine-grained parts and these parts are distributed to distinct clouds (Fig. 4. 2). This approach can be instantiated in different ways depending on how the partitioning is

DOI 10.17148/IJARCCE.2017.61056

performed. The clouds participating in the fragmented applications can be symmetric or asymmetric in terms of computing power and trust.

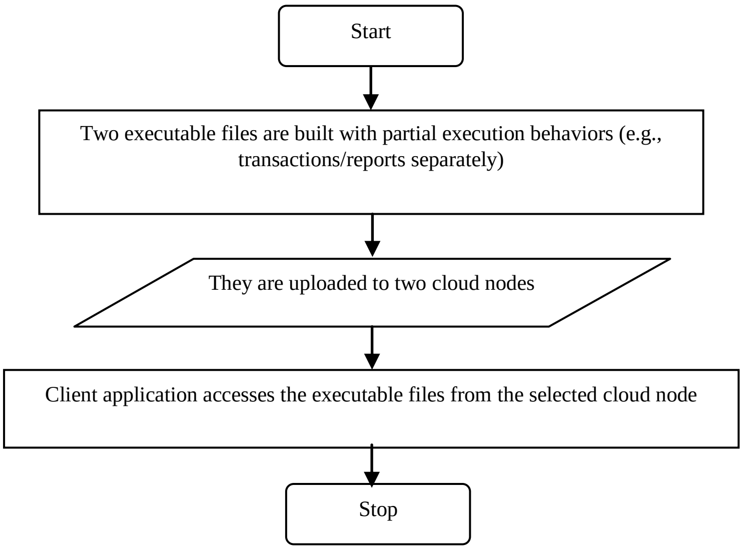
Start
Two executable files are built with partial execution behaviors (e.g., transactions/reports separately)
They are uploaded to two cloud nodes
Client application accesses the executable files from the selected cloud node
Stop

Fig 4.2 Logic Fragments

C. Tiers Communication Model

The architectural Fig 4.3 pattern described in the previous enables the cloud user to get some evidence on the integrity of the computations performed on a third-party's resources or services.

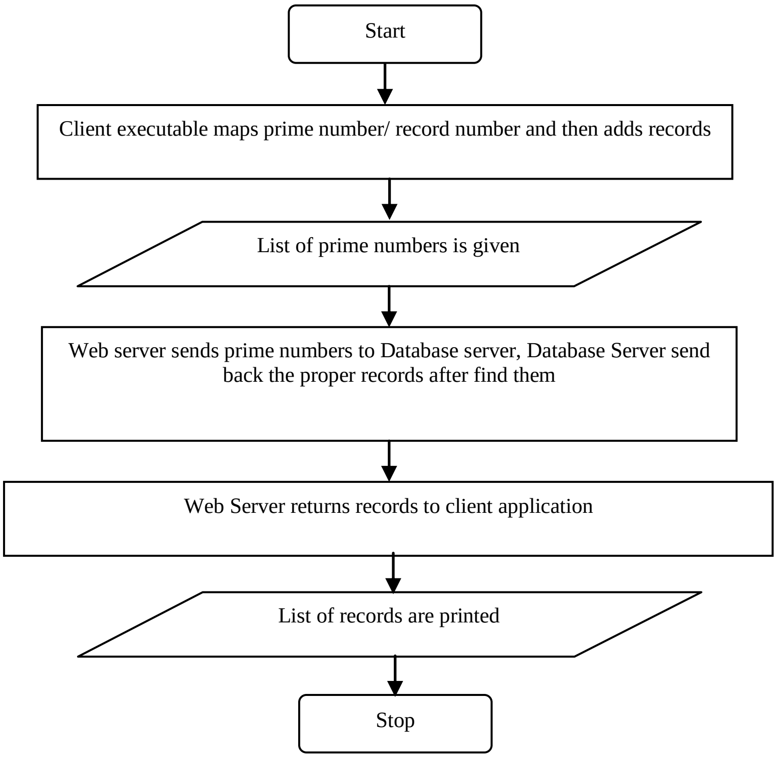
Start
Client executable maps prime number/ record number and then adds records
List of prime numbers is given
Web server sends prime numbers to Database server, Database Server send back the proper records after find them
Web Server returns records to client application
List of records are printed
Stop

Fig 4.3 Tiers Communication

The Fig 4.3 architecture introduced in this section targets the risk of undesired data leakage. In case of an application failure, the data are not immediately at risk since it is physically separated and protected by an independent access control scheme. Moreover, the cloud user has the choice to select a particular probably specially trusted cloud provider for data storage services and a different cloud provider for applications. Also generic data services might serve for a wide range of applications there will be the need for application specific services as well. The partitioning of application systems into tiers and distributing the tiers to distinct clouds provides some coarse- grained protection

DOI 10.17148/IJARCCE.2017.61056

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

against data leakage in the presence of flaws in application design or implementation. This architectural concept can be applied to all three cloud layers.

D. Hash Index Hierarchy for CPDP

To support distributed cloud storage, we illustrate a representative architecture used in our cooperative PDP scheme as shown in Figure 4.4. Our architecture has a hierarchy structure which resembles a natural representation of file storage. This hierarchical structure $\mathcal{H}$ consists of three layers to represent relationships among all blocks for stored resources. They are described as follows:

- ○ Express Layer: offers an abstract representation of the stored resources.
- ○ Service Layer: offers and manages cloud storage services.
- ○ Storage Layer: realizes data storage on many physical devices.

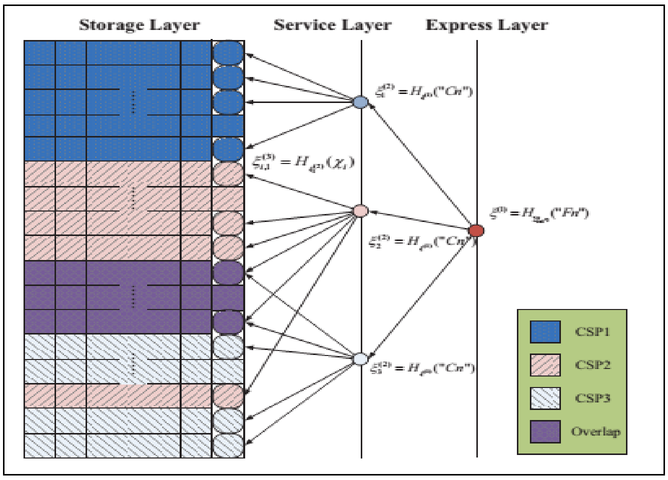
Storage Layer
Service Layer
Express Layer
$\xi_1^{(2)} = H_{\xi^{(1)}}(\text{"Cn"})$
$\xi_{1,1}^{(3)} = H_{\xi^{(2)}}(\chi_1)$
$\xi^{(1)} = H_{\xi_{\text{Fn}}}(\text{"Fn"})$
$\xi_2^{(2)} = H_{\xi^{(1)}}(\text{"Cn"})$
$\xi_3^{(2)} = H_{\xi^{(1)}}(\text{"Cn"})$
CSP1
CSP2
CSP3
Overlap

Fig 4.4 Index-Hash Hierarchy of CPDP model

In this proposed methodology make use of this simple hierarchy to organize data blocks from multiple CSP services into a large size file by shading their differences among these cloud storage systems. For example, in Figure 4.5 the resources in Express Layer are split and stored into three CSPs that are indicated by different colors, in Service Layer. In turn, each CSP fragments and stores the assigned data into the storage servers in Storage Layer. To also make use of colors to distinguish different CSPs. Moreover, we follow the logical order of the data blocks to organize the Storage Layer. This architecture also provides special functions for data storage and management, e.g., there may exist overlaps among data blocks (as shown in dashed boxes) and discontinuous blocks but these functions may increase the complexity of storage management.

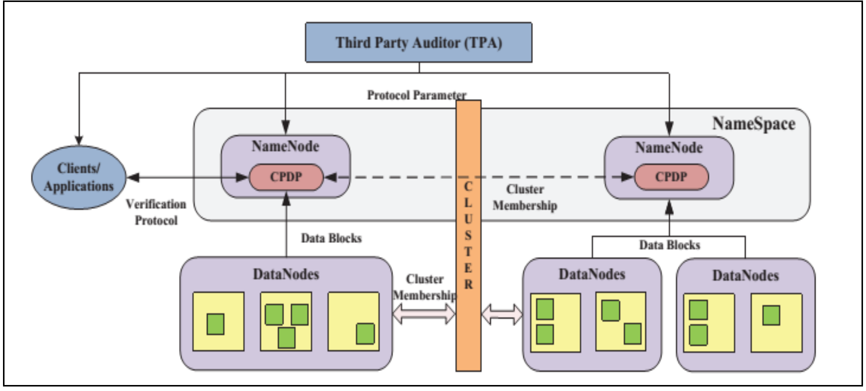

Fig 4.5 CPDP scheme for Cloud Database

V. EXPERIMENTAL RESULTS

The proposed approach of the replication of data storage with heterogeneous cloud service provides is evaluated using the communication path cost among the storage providers as follows:

$$\text{Path Cost}(n) = g(n) + h(n)$$

where g(n) is the path cost for reaching n (cloud node) and h(n) is called the heuristic cost and is the estimate of cost from n to the actual node. It searches all of the solutions of allocating a fragment to a node. The solution that minimizes the cost within the constraints is explored while others are discarded.

DOI 10.17148/IJARCCE.2017.61056

S. No.	Cloud Nodes	Existing		Proposed	
		G (n)	H (n)	G (n)	H (n)
1	25	8	0.8	5	0.5
2	50	14	0.14	12	0.12
3	75	24	0.24	20	0.20
4	100	32	0.32	27	0.27
5	125	45	0.45	39	0.39

Table 5.1Secure Communication Cost Path Analysis

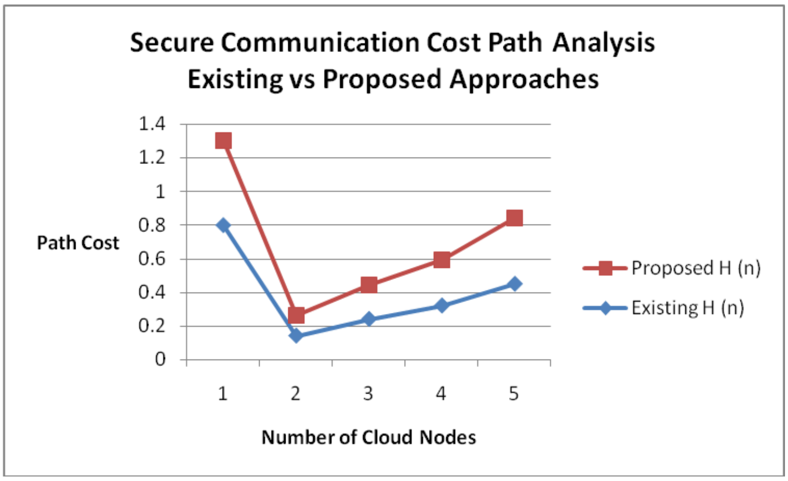

Fig 5.1Secure Communication Cost Path Analysis

VI. CONCLUSION

This paper concludes that the sharing of information between the group in the cloud servers will be confidential by encrypting the data using multi-replica strategy approach. This approach reduces the communication cost of nodes that involved in the data transmission process when compared with existing approach. However, encoding of data takes place twice and decoding at receiver is done for once in data communication phase. This work produces better results for the user who are communicating through cloud environment.

VII. ACKNOWLEDGMENT

I also extend my sense of gratitude to Head of the Department, **K.Vimala** for her valuable and creative suggestions, constant encouragement and guidance, which helped me to succeed in this venture.

REFERENCES

[1] United States Congress, “Health Insurance Portability and Accountability Act of 1996.

[2] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005).

[3] Water s, B.: Cipher text - policy attribute- based encryption: An expressive, efficient, and provably secure realization. Cryptology ePrint Archive, Report 2008/290 (2008), http://eprint.iacr.org/.

[4] A. Shamir. Identity-based cryptosystems and signature schemes. In G. Blakley and D.Chaum, editors, Proceedings of Crypto 1984, volume 196 of LNCS, pages 47–53. Springer, 1984.

[5] A.Sahai and B.Waters. Fuzzy Identity Based Encryption. In Advances in Cryptology – Eurocrypt, volume 3494 of LNCS, pages 457–473. Springer, 2005.

[6] Y. Desmedt and J. Quisquater, “Public-key systems based on the difficulty of tampering” Advances in Cryptology – Crypto ’86, Lecture Notes in Computer Science, Vol. 263, SpringerVerlag, pp. 111–117, 1986.

[7] ARMBRUST, M., AND ET AL. Above the clouds: A Berkeley view of cloud computing.Tech. Rep. UCB/EECS-2009-28, EECS Department, U.C. Berkeley, Feb 2009.

[8] B. Wang, B. Li, and H. Li, “Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud,” Proc. 10th Int’l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[9] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, “Efficient and provably-secure identity-based signatures and signcryption from bilinear maps,” in ASIACRYPT, ser. Lecture Notes in Computer Science, vol. 3788. Springer, December 4-8 2005, pp. 515–532.

[10] N.Shang,M.Nabeel,F.Paci, and E.Bertino,“A privacy preservingapproach to policy-based content dissemination,” in ICDE ’10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, 2010.

[11] M. Burkhart,M. Strasser, D. Many, and X. Dimitropoulos, “SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics,” Proc. USENIX Security Symp., pp. 223-240, 2010.

[12] Groß and A. Schill, “Towards User Centric Data Governance and Control in the Cloud,” Proc. IFIP WG 11.4 Int’l Conf. Open Problems in Network Security (iNetSeC), pp. 132-144, 2011.

DOI 10.17148/IJARCCE.2017.61056