IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Improve Secure Anti-Collusion Data Sharing Scheme for CP-ABE Security System

Kavitha .D[1], Karpagam .R[2]

M.Phil, Research Scholar, Department of Computer Science, Rathnavel Subramaniam College of Arts and Science, Sulur, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Science, Rathnavel Subramaniam College of Arts and Science, Sulur, Tamil Nadu, India[2]

Abstract: The data outsourcing development challenges the approaches of traditional access control architectures such as reference monitor; that a trusted server is in charge of describing and enforcing access control policies. The main scope of the project is used to deliver the user data in the third party area for on demand access. The user access the details as privilege level based on access control. The dual encryption is processed in the cloud environment which is varied form one group to another for secure process. The paper propose a novel algorithm namely ciphertext-policy attribute-based encryption to enforce access control guidelines with efficient attribute and user revocation capability. Dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key sharing in each attribute group. The ciphertext-policy EABE (CP-ABE) provides a scalable way of decoding data such that the encryptor defines the attribute set that the decrypt or needs to possess in order to decrypt the ciphertext. Thus, different users are permitted to decrypt different pieces of data per the security policy. This effectively eliminates the need to trust on the storage server for preventing unauthorized data access.

Keyword: Cloud Computing, Secure Data Sharing Scheme, Certificate Authorities, Untrusted cloud, Ciphertext-policy Attribute Based Encryption.

I. INTRODUCTION

Cloud computing means that instead of using the entire computer hardware and software to be on the desktop or somewhere inside the company's network, it's provided for as a service by another company and accessed over the Internet, usually in a completely smooth way. Exactly where the hardware and software is located and how it all works doesn't matter to the user it's just wherever up in the nebulous "cloud" that the Internet represents.

Cloud computing is a buzzword that means altered things to different people. For some, it's just another way of relating information technology "outsourcing"; others use it to malicious any computing service provided over the Internet or a related network; and some describe it as any bought-in computer service use that sits outside the firewall. However the cloud computing is defined, there's no doubt it makes most sense when it stop talking about abstract definitions and aspect at some simple, real examples-so let's do just that.

The goal of cloud computing is to put on traditional supercomputing, or high-performance computing pointer, normally used by military and research facilities, to perform tens of stacks of computations per second in consumer-oriented presentations such as financial portfolios, to deliver personalized information, to provide data storing or to power large, immersive online computer games.

The cloud computing uses webs of large groups of servers typically running low-cost consumer PC technology with specialized connections to extent data-processing tasks across them. This shared IT structure contains large pools of systems that are linked together. Often, virtualization methods are used to exploit the power of cloud computing.

Data outsourcing is becoming today a successful solution that permits users and organizations to activity external servers for the distribution of resources. Some of the most stimulating issues in such a development are the enforcement of authorization policies and the support of policy updates.

Since a common approach for keeping the outsourced data consists in encrypting the data themselves, a promising approach for solving these issues is based on the arrangement of access control with cryptography. This idea is in itself not new, but the problem of spread over it in an outsourced architecture introduces several challenges.
In this paper, illustrating the basic principles on which architecture for combining access control and cryptography can be built. It then illustrate an approach for enforcing authorization policies and supporting dynamic authorizations, allowing policy modifications and information updates at a limited cost in terms of bandwidth and computational power.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Some of the most challenging issues in data outsourcing development are the enforcement of authorization policies and the support of policy updates. Ciphertext-strategy attribute-based encryption is an auspicious cryptographic solution to these issues for implementing access control strategies defined by a data owner on outsourced data.
However, the problem of applying the attribute-based encryption in an outsourced design introduces several challenges with regard to the attribute and user revocation. The study proposes an access control mechanism using ciphertext-policy attribute-based encryption to enforce access control policies with effective attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which precedes help of the attribute-based encryption and selective group key distribution in each attribute group.

II RELATED WORKS

U. Jyothi K. Et al [1] describe a cloud computing is an emerging computing paradigm in which resources of the computing organization are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new tasks for data security and access control when users outsource sensitive data for distribution on cloud servers, which are not inside the same trusted domain as data owners. To keep sensitive user data confidential beside untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to approved users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key sharing and data management when fine-grained data access control is desired, and thus do not scale well. The difficult of concurrently achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved.

Brent Waters et al [2] present a new methodology for realizing Ciphertext-Policy Attribute Encryption (CP-ABE) under actual and non-interactive cryptographic assumptions in the standard model. The solutions agree any encryptor to specify access control in terms of any access formula over the attributes in the system. In most effective system, ciphertextscope, encryption, and decryption time scales linearly with the difficulty of the access method. The only previous work to achieve these parameters was limited to a proof in the generic group model.

To presented three constructions within the framework. In the first system is proven selectively secure under a assumption that call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be regarded as a generalization of the BDHE assumption [12]. The next two constructions provide performance tradeoffs to achieve provable security separately under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions.

Dan Boneh et al [3] describe aHierarchical Identity Based Encryption (HIBE) system where the ciphertext consists of just three set elements and decryption requires only two bilinear map computations, regardless of the hierarchy depth [14]. Encryption is as efficient as in other HIBE systems. To prove that the scheme is selective-ID secure in the standard model and fully secure in the random oracle model. System has a number of applications: it gives very effective forward secure public key and identity based cryptosystems, it converts the NNL broadcast encryption system into an efficient public key broadcast system, and it provides an efficient mechanism for encrypting to the future. The system also cares limited allocation where users can be given restricted private keys that only allow delegation to bounded depth.

VipulGoyal et al [4] describe a more sensitive data is shared and stored by third-party sites on the Internet, there will be a requirement to encrypt data stored at these sites. One drawback of encrypting data is that it can b e selectively shared only at a coarse-grained level (i.e., giving another party private key). Develop a new cryptosystem for fine-grained distribution of encrypted data that they call Key-Policy Attribute-Based Encryption (KP-ABE). Inthe cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt.Demonstrate the applicability of construction to sharing of audit-log information and broadcast encryption. Construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

Dan Boneh et al [5] describe aIdentity-Based Encryption from the Weil Pairingproposed a fully functional identity-based encryption scheme (IBE). The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational Diffie Hellman problem. The system is based on bilinear maps between groups. The Weil pairing on elliptic curves is an example of such a map. They give precise definitions for secure identity based encryption schemes and give several applications for such systems. Analysis is the process of breaking the problem into the successfully manageable parts of study. In system analysis emphasis is given to understanding the details of an existing system or a proposed system is desirable or not. Thus, system analysis is the process of investigating a system, identifying problems, and using the information to recommend to the system.

III. SECURE ANTI COLLUSION MODEL

A. CP- ABE Methodology

The working algorithm logic in encryption is ABE comes in two flavors called Key-Policy ABE (KP-ABE) and cipher text-policy ABE. In KP-ABE, attributes are used to define the encrypted data and policies are built into user's keys; while in CP-ABE, the attributes are used to define a user's credential, and an encryptor determines a policy on

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

who can decrypt the data's-ABE is more appropriate to the data outsourcing architecture than KP-ABE because it enables records owners to choose an access structure on attributes and to encrypt data to be outsourced under the access configuration through encrypting with the corresponding public attributes.

The problem of applying the ABE to the data outsourcing architecture leads several challenges with regard to the attribute and user revocation. The revocation issue is even more difficult specially in ABE systems, since each attribute is conceivably shared by multiple users.

This implies that revocation of any attribute or any single user in an attribute set would affect the other users in the group. It may result in bottleneck during re-keying procedure or security deprivation in the system. Thus, in this study will attempt to solve these problems in attribute-based data access control using CP-ABE for data outsourcing systems.

The existing system depending full of manual process, manual system maintains the limited number of process. The existing system includes an attribute-based access control scheme using CP-ABE with effectiveattribute and user revocation capability for data outsourcing systems. The existing system consists of the following entities:

1. Trusted authority. It is a key authority for the attributes set. It generates public and secret parameters for the system. It is in charge of distributing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on the elements. It is the only party that is fully trusted by all entities participating in the data outsourcing system.

2. Data owner. This is a client who owns data, and wishes to outsource it into the external data server provided by the service provider.

A data owner is responsible for defining (attribute-based) access strategy, and enforcing it on its own data by encrypting the data under the policy before outsourcing it.

3. User. This is an entity who wants to access the outsourced data. If a user possesses a set of attributes satisfying the access strategy of the encrypted data defined by the data owner, and is not revoked in any of the attribute groups, then the user will be able to decrypt the ciphertext and obtain the data.

4. Service provider. It is an entity that provides a data outsourcing service. It consists of data servers and a data service manager. Outsourced data from data owners are stored in the data servers.

The data service manager is in charge of controlling the accesses from outside users to the outsourced data in servers and providing corresponding contents services.

The following are the drawbacks of CP-ABE system.

- Handling the outsource data copies in a secure manner is difficult.
- Storing and retrieving of data from a cloud server are takes more time and effort.
- The data owner need to take full charge of maintaining all the membership lists for each element group to enable the direct user revocation.
- All the data is maintained by single service benefactor so the data privacy affected by the third party storage area.
- The single data service manager is in-charge of managing the attribute group keys per each attribute group.
- Key storage of each outsourced data maintenance will be difficult for the cloud administrator.
- Keys are assigned randomly and independently from each other, so the user can access the data of another user group by the system.
- No capability to capture a series of attribute queries option.
- User profile is group into single group attribute in the tuples structure only.
- Past query based suggestion is not given to user group.

Below mentioned are the main objectives of the proposed system:

- To revocate users by any service provider may if unauthorized user tries to access the data above a given count.
- To maintain data servicing by more than one service provider.
- To make all data service managers take charge of managing the attribute group keys per each attribute group.
- To assign keys based on a condition and unique among all users.

IV ENHANCED CP-ABE- METHODOLOGY

In proposed Secure-ECP-ABE system, first, enabling user access control enhances the backward/forward privacy of outsourced data on any membership changes in attribute groups compared to the attribute revocation schemes.

Second, the customer access control can be done on each attribute level rather than on system level, so that other fine-grained user access control can be possible. In practical scenarios, users may miss many key update messages so that it cannot sometimes keep the key states up-to-date. This is called stateless receiver problem. In the proposed scheme, rekeying in the attribute set is done with a stateless group key distribution mechanism using a binary tree. This alleviates the scalability problem and resolves the stateless receiver problem. Third, data owners need not be concerned about any access strategy for users, but just need to define only the access control policy for

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

attributes as in the previous EABE system. The main objective of the proposed system is to reduce the time consuming and make the system more user friendly, efficient, accurate and fast process. The primary objective of the proposed system,

- To revocate users by any service provider may if unauthorized user tries to access the data above a given count.
- To maintain data servicing by more than one service provider.
- To make all data service managers take charge of managing the attribute group keys per each attribute group.
- To assign keys based on a condition and unique among all users.

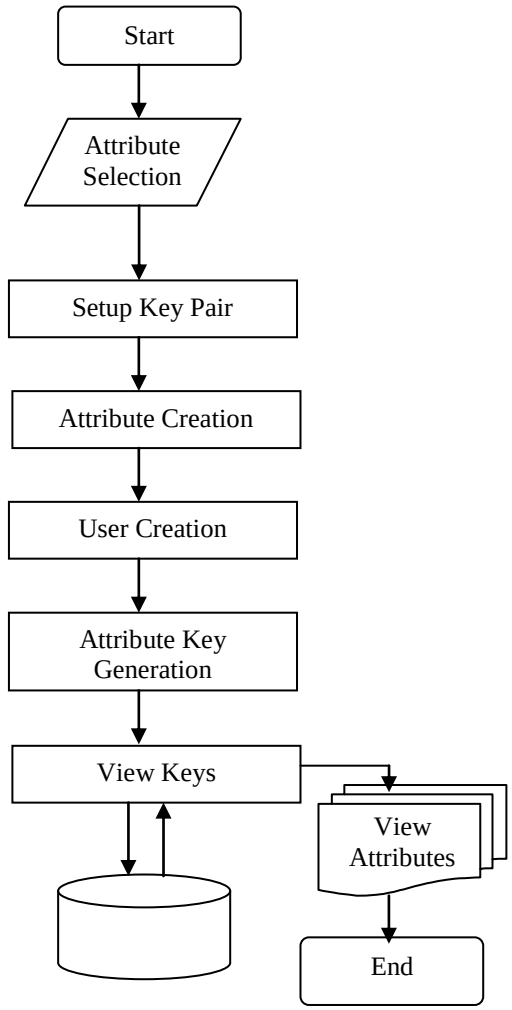

Fig 4.1 Ciphertext-Policy Attribute-Based Encryption with User Revocation

The proposed system implements all the existing system concepts in which the Ciphertext-Policy Attribute-Based Encryption with User Revocation is carried out. Like existing system, the proposed scheme also adapts a dual encryption approach to overcome the user access control problem in attribute-based encryption system.

In addition, multiple service providers are included and data is distributed among them.

User privileges may be changing for data maintained by different service providers.

This requires different kind of encryption mechanisms in data maintained by different service providers. The following are the advantages of proposed system.

- Any service provider may revocate users if unauthorized user tries to access the data above a given count.
- Data servicing is maintained by more than one service provider, the authentication process is enhanced.
- All data service manager take charge of handling the attribute group keys per each attribute group.
- Keys are assigned based on a condition and unique among all users, so the key duplication is not occurred in the current system.
- Handling the outsource data copies in a secure manner is easy to compare proposed attribute access control model.
- To capability and capture a series of attribute queries option.
- User profile is group into same group with attribute in the tuples structure only.
- Past query based suggestion is given to user group.
- All the data is maintained by multiple service providers so the data privacy do not affected by the third party storage area.
- The single data service manager is in-charge of managing the different attribute group keys per each attribute group

A. Cipher Text-Policy Attribute-Based Encryption with User Revocation

Step 1:
The setup algorithm is executed which is a randomized algorithm that takes no input other than the implied security parameter. It outputs the public key PK and a master key MK.

Step 2:
The attribute key generation algorithm is executed which takes input the master key MK, a set of attributes $\Lambda \subseteq L$, and a set of user indices $U \subseteq u$ as parameters.

It outputs a set of private attribute keys SK for each user in U that identifies with the attributes set.

Step 3:
The key encrypting key (KEK) generation algorithm is executed in this module, which takes a set of user indices $U \subseteq u$ as input, and outputs KEKs for each user in U, which will be used to encrypt attribute group keys $K_{\square i}$ for each $Gi \in G$.

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Step 4:
An encryption algorithm (which is a randomized algorithm) that takes as input the public parameter PK, message M, and an access construction 'A' over the universe of attributes. It outputs a cipher text CT such that only a user who possesses a set of attributes that satisfies the access structure will be able to decrypt the message.

Step 5:
The re-encryption algorithm is a randomized algorithm that takes as input the cipher text CT including an access structure 'A', and a set of attribute sets G. If the attribute groups appear in 'A', it re-encrypts CT for the attributes; else, returns ⊥. Specifically, it outputs a re-encrypted cipher text CT' such that only a user who possesses a set of attributes that fulfills the access structure and has a valid membership for each of them at the same time will be able to decrypt the message.

Step 6:
The decryption algorithm is executed which takes as input the cipher text CT' which contains an access structure 'A', private key SK, and a set of attribute group keys K_Λ for a set of attributes Λ. The decryption can be done if Λ satisfies 'A' and K_Λ is not revoked for any$\lambda \in \Lambda$.

Step 7:
If the data contains most important information and in order to protect the data security, more privileged service providers view most of the data and less privileged service providers view limited data. This form is used for the purpose of the authentication with the credential details of the username and password.

Those details are entered by user in the textbox controls and login process done by the command button event. Here the details are extracted from the login table for the authorization process.

B. Trusted Key Pair
The trusted key pair created in the application for further process, following the key generation of the public key and the master key which are used for the purpose of encryption of the message. All such keys are created as group key.

These details are generated by create command button event and showed in the multiline text mode. This key is saved in the application using save command button event.

C. Attribute Creation
This form is used to create the attribute details in the application, It contains details such as attribute id, attribute names that are entered by user in the textbox controls, and saved by the save command button.

The delete button is used is used to delete the specified record and close command button is user to terminate the current form.

D. User Creation Form
The user creation form is to create the user details for accessing the attribute with privilege level. The user id, user name and passwords are entered by user in the textbox controls these details are saved by the save command button event.
The delete button is used is used to delete the specified record and close command button is user to terminate the current form.

E. Attribute Key Generation
Attribute key generation form is used to process the key generation process in the application. The access structure form is used to create the access specification for each and every user for specifying the details with the rights to select, insert, update and delete operation in those processes which are selected by the check box control.

Attribute identity number and user identity numbers are selected by user from the Combo Box control. Given attribute name and user names are displayed in the textbox control. All these information are saved in the database using save command button event.

F. Attribute Group Key Generation
Attribute group key generation form is used to create group key in the application, attributes assigning with the group, identify each user belonging to the given group id.

The attribute identity number is selected by the user in the checkbox control. Group identity number is inserted in the textbox control. All these details are saved in the specified table.

G. Group Key generation for Users
This form is used to assign the user to group, for accessing the given process. The user identity number is selected by user in the check box control and group identity number is selected by the combo box control and all these details are saved in the specified table.

H. Key Encrypting Key Generation for Users
This form is used to encrypt the key value for corresponding username and user id. The id details are selected by user in the checkbox control and user key is generated using create command button event.

The corresponding username, user id and the given key encrypting values are inserted into the user details table.

I. Encryption Form
This form is used to encrypt the text using public key for the purpose of other users who do not know the given message. So, the public key is extracted using get key command button and displayed in the label control, the message is entered in the textbox control then the given encrypted message is displayed in the label control.

The encrypted message is saved in the application using creates cipher text and save command button event.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

J. Re-Encrypt Form

This form, re-encrypt the encrypted data in the application based on the group key because the other user will not identify the same encrypted message. In this form, group identity number and cipher texts are selected from the combo box controls, and details are re-encrypted in the cipher text grid view control using re-encrypt command button event.

K. Decrypt Cipher Text

Decrypt cipher text retrieves the plain data in the application. The given cipher text is entered the data is showed to the user.

In this form user identity number and cipher texts are selected from the combo box control, group identity is displayed in the label controls. The message is decrypted in the cipher text grid view control using the decrypt command button event.

L. Select Query Form

This form is used to check the user level access privileged rights in the application; query is inserted in the textbox control and processed by the check command button event.

M. Encrypt Block Security Form

This form is used to create cipher text in this experimental system given database the user access the high privileged level or not. The field one , field two and field three data's are entered by user in the list box controls and privilege settings is selected by the check box control.
The Advanced Encryption Key (AES) is entered in the textbox control and data is encrypted using the encrypt command button event.

V.RESULTS

The Table 5.1represents experimental result for Secure Anti Collusion Algorithm model. The table shows the selecting the number of Attributes, Access control count and Access permission count. The table contains the various attributes, owner and access policy control and access permission count.

Table 5. 1Secure Anti Collusion Algorithm Model

S. No	Attribute	Owner	Access Control [N]	Access Permission Count [N]
1	Name	A	4	80
2	Age	B	6	120
3	DOB	C	10	200
4	Salary	D	12	240
5	Attendance	E	17	340

The Figure 5.1represents experimental result for existing Secure Anti Collusion Algorithm model. It shows the selecting the number of Attributes and Access permission count based on the access control policy count.

VI.CONCLUSION

The fast development of versatile cloud services, a lot of new challenges have emerged. One of the most important problems is how to securely delete the farm out data stored in the cloud severs.
The proposed ciphertext-policy attribute-based encryption with user revocation scheme provides a big advantage by supporting user-defined time-specific authorization and fine-grained access control and data secure self-destruction.

Some of the most challenging issues in data outsourcing scenario are the implementation of authorization policies and the support of policy updates. This thesis proposes a cryptographic approach to implement a fine-grained access control on the outsourced data that is dual encryption protocol exploiting the combined features of the ciphertext-policy attribute-based encryption and group key management algorithm.

The proposed scheme permits a data owner to define the access control policy and enforce it on his outsourced data. It also features a mechanism that qualifies more fine-grained access control with efficient attribute and user revocation capability. It is sent that the proposed scheme is efficient and scalable to securely manage the outsourced data.

The proposed ciphertext-policy attribute-based encryption model does includes the set of the attributes, tree access policy, and the definition of the time instant, because the costs are negligible if compared with the key generation.

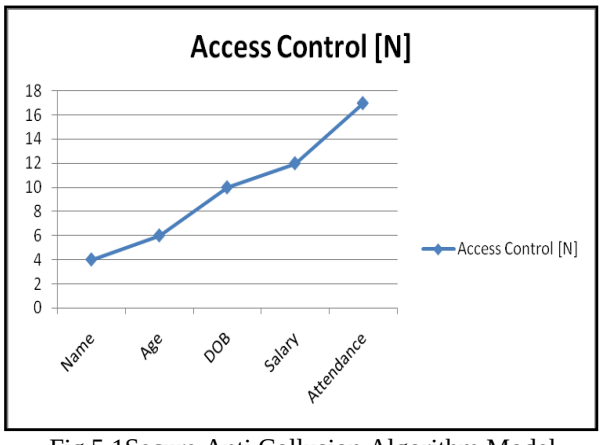

Fig 5.1Secure Anti Collusion Algorithm Model

- The data integrity in multiple copies of same database is not considered. The error situation can be improved if there is any mismatch.
- The web site and database can be hosted in real environment during the implementation.
- In future Minimum Spanning Tree logic may applied for the access control tree
- Further the T-DES algorithm can be used for the encryption and decryption process

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

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] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Proceedings of Crypto '99, volume 1666 of LNCS, pages 537–554, 1999.
[9] 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.
[10] 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.
[11] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A privacypreserving approach to policy-based content dissemination," in ICDE '10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, 2010.

DOI10.17148/IJARCCE.2016.51053