ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Improved Key policy-based Security Framework for Cloud Computing

Ajay Deshmukh, Arpit Solanki

Research Scholar, Department of Computer Science & Engineering, RKDF SOE, Indore, M.P, India[1]

Assistant Professor, Department of Computer Science & Engineering, RKDF SOE, Indore, M.P, India[2]

ABSTRACT: It requires some mechanism in which encryption is performed and if the user requires performing some operations on secure file without decrypting it can be fulfilled. Thus homomorphic encryption lets the user facilitates about the performing operations on encrypted data which reduces the complexity of confidentiality operations. Also to prevent Cloud Servers from being capable to discover both the data file contents and user access privilege information used to generate key along with the fastest access of secured data by using Attribute-based encryption (ABE).
In this thesis, we offer a new KP-ABE formation with constant cipher text size by adopting and applying the knowledge of the identity-based broadcast encryption method. In our algorithm construction, the access policy can be expressed or defined as any intonation access structure.

KEYWORDS: Cloud, Cloud organization, Data privacy, Cloud service provider (CSP), Information Dispersal Algorithms (IDA), Security framework, Cloud security policy.

I. INTRODUCTION

The encryption technique is been finalized and now this paper is going to present the results for vivid KP-ABE methodology with constant-size of the cipher texts. We had firstly studied the feasible and reliable withdrawal operations in CP ABE scheme: single attribute withdrawal, attribute set withdrawal and unique identifier withdrawal. After that, based on unique identifier revocation procedure.

We will suggest the CP-ABE scheme in which mischievous users can be efficiently and more collaboratively revoked. Our motive going to present the cipher text policy based on the encryption scheme with complete efficient revocation with the help of using linear undisclosed allocation pattern and binary tree as the essential tools.

We are going to that the allocating proficiency can be easily provided in the wished-for arrangement, but all the representatives are accompanying with their creative delegator's matchless identifier. The overview of our proposed paper has been diagrammatically presented with the help of two illustrative reorientations-

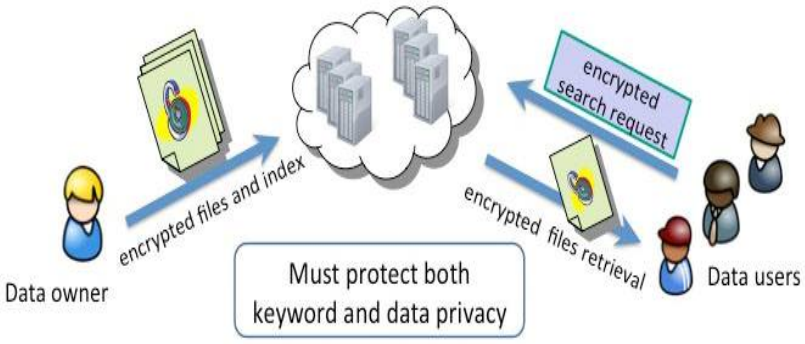

Figure 1. Encryption System

The figure1 represented here shows that the data owner is encrypting his confidential files and index which he want to be secure from the outsiders, here the encryption technique is involved.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

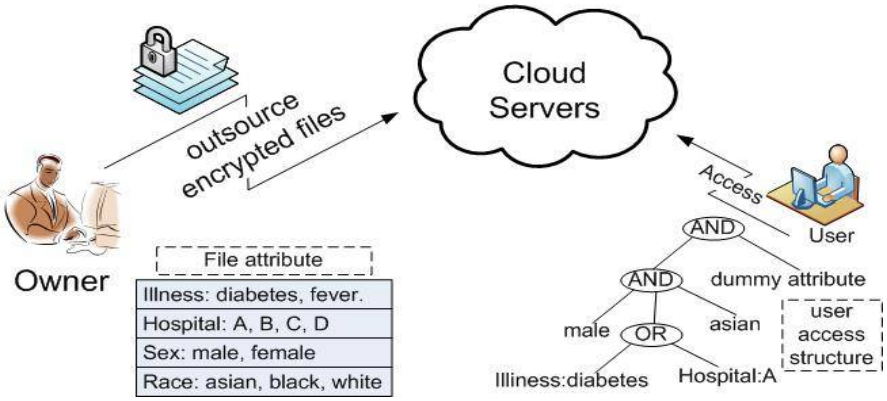

Figure 2. Attribute based Encryption

The figure2 represents the encryption technique here, the user here provides his attributes for e.g. his illness which can be fever, diabetes etc., name of the hospital like A,B,C,D, his gender i.e. male or female, his race i.e. Asian, black or white. The user will provide his all the essential properties and behaviour which are required here. Now all the attributes are going to be on the cloud, the cloud is going to merge or focus on all the attributes of the user, these will going to leads to the generation of the key attribute of the user. In this manner the key generation with the help of the attributes is done.

II. RELATED WORK

A Policy-based Security Framework for Storage and Computation on Enterprise Data in the Cloud
SouryaJoyee De, Asim K. Pal, 2014 47th Hawaii International Conference on System Science

Previous workings on protected cloud storage and computation have careful consideration on different adversarial models. These models consider a Byzantine adversary, which can be defined as the challenger, which can act as a random, which can corrupt as small number of servers. In this corruption process, the corrupted clouds can blastoff three types of attacks:

1) The storage cheating on corrupted servers can delete rarely accessed files (which means the file which cannot use by user frequently) to moderate the cost of storage or arbitrarily change the stored data.
2) Computation – this is a type of cheating in which the servers either generate improper (incorrect) results of computations or it may uses different inputs for computations going on to reduce computational cost.
3) Privacy- this is a kind of cheating in which corrupted cloud server can leak user's confidential information to other parties. It means that the data of the user is not at all safe the data can be transferred from user's account to other accounts.

.

III. PROPOSED ALGORITHM

We propose the system with multiple uses and owners. For any organization, Institute confidential file s/data handle by more than one director .in such type of situation data security and authentication is challenging task. We are proposing system have more one owner, each owner having individual access key and password for accessing the data/files of organization. We also define key based policy with following descriptions [3]:
Proposed system consists of following Operation:

- **Key Generation:** Access secret is generated for every user UN agency registers within the system. System collects some attributes from user as well as identity attributes like e-mail, user-name etc. mistreatment these attributes and a few alternative options a singular secret is generated and from that key, employing a pattern operate, a 6 digits code is passed and generated to the user [7]. In propose system three type of users
    - Owner
    - Public User
    - Customer

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

- **Define Access Policy and Encryption Key**: File Access policies are generated for every file supported the confidentiality of the file. The owners might store the file as non-public, public or custom and should set the permissions as scan, edit, transfer and delete.
- **Decryption:** Before accessing a file, the file policies and user policies are matching. If each matches, then per the access key of user the system finds the permissions allowed for that user and retrieves the mix code. The key codes are retrieved and combined to form the key. Then secret writing is doing thereupon key.

- **File Revocation:** File revocation suggests that creating the file for good inaccessible. Deleting the file policies and coding keys will this. Deleted the key can't be reformed and secret writing is not possible. Once a file is making an attempt to access, initial the file policies are checked, if there's no file policy then there itself the file is inaccessible. The system twice ensures the inconvenience of a file [9].

- **Hash Value (MD-5):** Generate the hash price for store file on cloud. MD5 processes a variable-length message into a fixed-length output of 128 bits. Those functions are as follows:

Proposed Algorithm:

Algorithms of for KP-ABE with enhancement are discussed as below:
KP-ABE Key Generation (A, M_K):

Proposed algorithm output a secret key D added with an access structure T. Following three steps describe access structure A:

1. Every root node represent with r, set secret value = y.

2. Using loop each non leaf node
   a. If the ^ (And) operator and all child node mark with unsigned.
   b. If the ^{V} (OR)operator), and Mark this node as assigned and set value s.

3. For each leaf attribute a_j,i ε T , compute D_j;i = T_j^si
Secret Key S_k= { D_j,i}

4) KP-ABE Decryption (E, D): Proposed algorithm takes input as cipher text (E) using the attribute policy decrypted the Message with secret S_k and public key $Pk_;$

Figure 3: Proposed Algorithm

IV. EXPERIMENTAL RESULTS

With help of Open Shift Red hat public cloud developed application KP-ABE. Following step are used for create application.
1. Register user details open shift public cloud and verify through mail.
2. Create application in with following tools
   - JBoss Developer Studio
   - Mysql 5.0
   - PHP MY Admin4.0

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

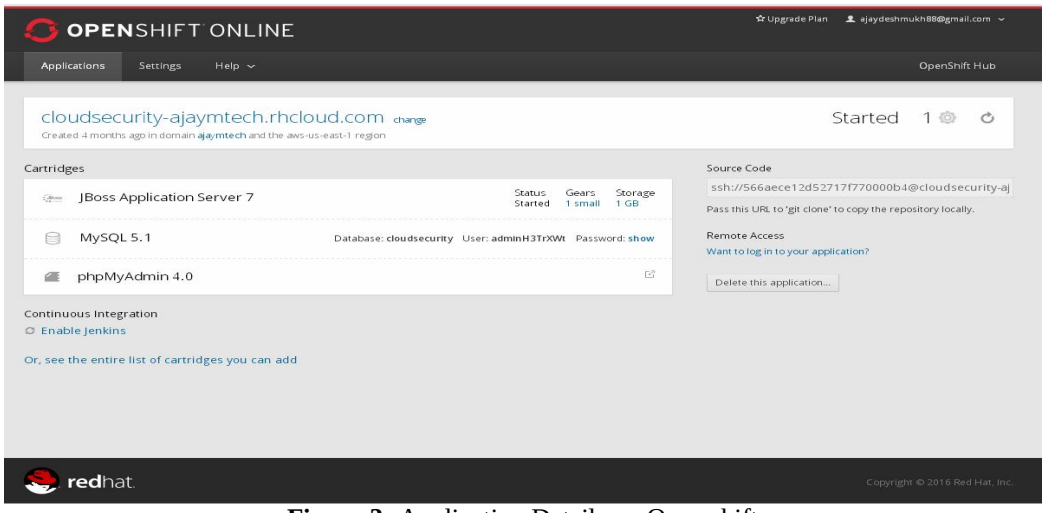

Figure 3: Application Details on Open shift

Figure 3. Show application details of cloud which is created by us. Functionality performs using language JAVA/JSP/Servlet.

3. Application map with Eclipse (Kepler) IDE

Table: User Credential on public cloud

S. No	User ID	Password
1	ajay@gmail.com	ajay123
2	deshmukh@gmail.com	deshmukh

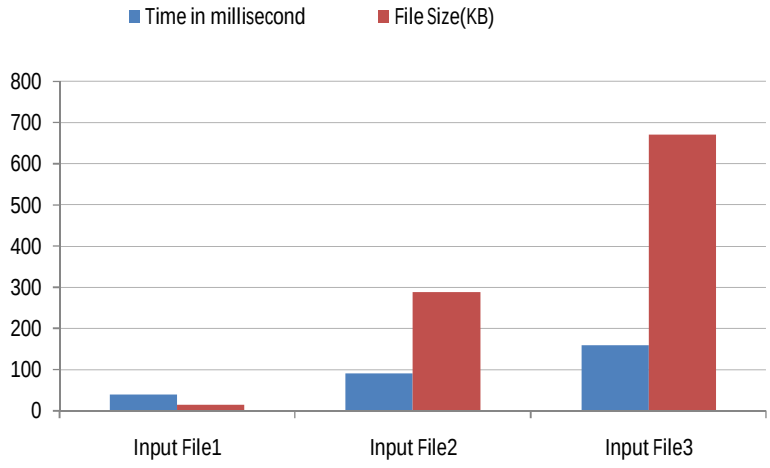

Figure 4 Graph of KP-ABE for different Files

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Table 2: Time Complexities of modified KP-AB

File Name	File Size (KB)	Encryption Time (in millisecond)	
		(KP-ABE)	Improved (KP-ABE)
File1	40	19.0	15.0
File2	330	108.0	90.0
File3	2230	406.0	244.0

V. CONCLUSION AND FUTURE WORK

In this paper we have spoken our ongoing research about a semantic approach about our policy-based security framework for business management processes. We have renowned all the security concerns, which are demanded in day-to-day purpose and these requirements, are classified into two levels that is Task and Process Level. The architecture of security framework is premeditated to maintenance runtime policy controlling and execution. Security policies are built on the top of ontology to enrich representation of security concerns and enable reasoning for the clash of detection and policy negotiations.

REFERENCES

[1] A. Acquisti, and J. Grossklags, "Privacy and Rationality in Individual Decision Making", IEEE Security and Privacy Vol. 3 No. 1, IEEE, 2005, pp. 26-33.

[2] M. A. AlZain, and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii International Conference on System Sciences, IEEE, 2011.

[3] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "Cloud Computing Security: From Single to Multi- Clouds", 45th Hawaii International Conference on System Sciences, IEEE, 2012.

[4] A. Bessani, M. Correia, B. Quaresma, F. Andre, and P. Sousa, "DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds", Proceedings of the 6th conference on computer systems EuroSys'11, ACM, New York USA, 2011, pp. 31-46.

[5] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider, „Twin Clouds: An Architecture for Secure Cloud Computing", Workshop on Cryptography and Security in Clouds, 2011.

[6] S. Chaves, C. B. Westphall, and F. R. Lamin, "SLA Perspective in Security Management for Cloud Computing", 6th International Conference on Networking and Services, IEEE, 2010.

[7] Y. Chen, and R. Sion, "On Securing Untrusted Clouds with Cryptography", Proceedings of the 9th annual ACM Workshop on Privacy in Electronic Society WPES'10, ACM, New York USA, 2010, pp. 109-114.

[8] N. Christin, S. Egelman, T. Vidas, and J. Grossklags, „ It's All About the Benjamins: An empirical study on incentivizing users to ignore security advice", Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2012, pp. 16-30.

[9] S. De, S. Saha, and A. K. Pal, "Achieving Energy Efficiency and Security in Mobile Cloud Computing", Proceedings of the 3rd International Conference on Cloud Computing and Services Sciences CLOSER 2013, SciTePress, 8-10 May 2013, Aachen, Germany.

[10] J. Fontana**, "**Are human firewalls the enterprise info. sec of the future? http://www.zdnet.com/are-human- firewalls-the-enterprise-info-sec-of-the-future- 7000008497/" (a discussion on Tom Scoltz et al, Gartner's Report on People Centric Information Security Strategy, 2012.)

[11] O. Goldreich, "Foundations of Cryptography Volume II Basic Applications". Cambridge, UK: Cambridge University Press, 2004.[12] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures", 8th IEEE Conference on Dependable, Autonomic and Secure Computing, IEEE, 2009, pp. 711-716.

[13] A. W. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44th Hawaii International Conference on System Sciences, 2011, pp. 1-10.

[14] M. Jensen, J. Schwenk, J. Bohli, N. Gruschka, and L. Iacono, "On T echnical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, IEEE, 2009.

[15] M. Jensen, J. Schwenk, J. Bohli, N. Gruschka, and L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds", IEEE 4th International Conference on Cloud Computing, IEEE, 2011.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

BIOGRAPHY

Ajay Deshmukh is a Research Scholar in the Computer Science Department, RKDF School of Engineering, and RGPV University. He received Bachelor Degree (BE) in Computer Science and Engineering in 2011 from RGPV, Bhopal, MP India. His research interests are Network Security and Cloud Computing.

Arpit Solanki is an Assistant professor in the Computer Science Department, RKDF School of Engineering, and RGPV University. He received Bachelor Degree (BE) in Computer Science and Engineering from Govt Engineering College, Ujjain MP, and received MTech Degree from MNNIT Allahabad India His research interests are Security Cloud Computing and Artificial Intelligent.