RESEARCHERID
THOMSON REUTERS

[Kushwaha* *et al.*, 7(6): June, 2018]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

IMPLEMENTATION OF DATA CONFIDENTIALITY USING IMPROVED KP-ABE SYSTEM

Vinod Kumar Kushwaha[*1], Malti Nagle[2]

[*1]Research Scholar, Surabhi College of Engineering & Technology, Bhopal, M.P, India.
[2]AssistantProfessor, Surabhi College of Engineering & Technology, Bhopal M.P, India.
Department of Computer Science & Engineering.

DOI: 10.5281/zenodo.1297365

ABSTRACT

In cloud computing there is problem associated with whole life of cloud data. For storage three important aspects of data is Data confidentiality, Data integrity and availability. Data encryption is used for confidentiality. Now, after this encryption data is sent to storage. Now, after the user supplies its key than the data is opened. Thus to provide user based security control for cloud provider is the primary objective of this work and can be achieved by Holomorphic encryption. Key management is another problem because the user is not expert to manage keys. The user has faced such problems. To develop a security architecture and implement client based confidentiality tool for storage in cloud computing and evaluate traditional security solutions and identify their remaining issues by which overall performance gets degraded. We will implement homomorphic encryption using improved KP-ABE system to achieve data confidentiality.

KEYWORDS: Cloud, Cloud Security, Data privacy, ABE, KP-ABE, Cloud Storage

1. 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 suggested 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.

Figure 1. Encryption System

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-

The figure 1 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: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

The figure 2 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 provides his all the essential properties and behavior 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.

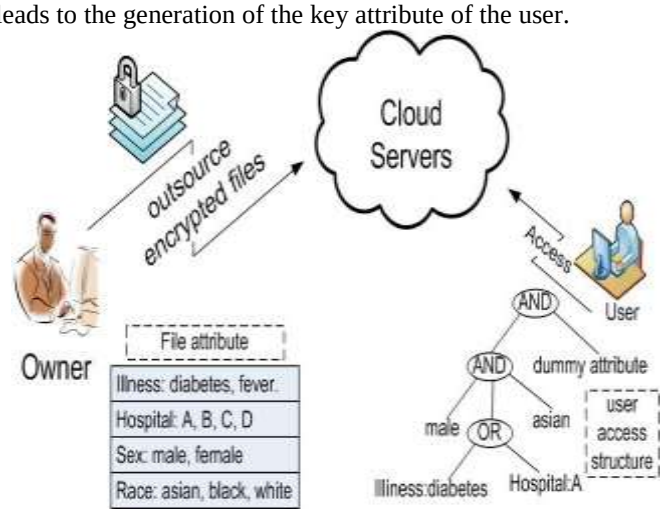

Figure 2. Attribute based Encryption

In this manner the key generation with the help of the attributes is done.

2. LITERATURE SURVEY

A Policy-based Security Framework for Storage and Computation on Enterprise Data in the Cloud [1]

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 used 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.

3. PROPOSE SYSTEM

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 consist 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: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

- **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].

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 a access structure T. Following three step 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^siSecret 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 P_k.

4. IMPLEMENTATION AND RESULT

With help of OpenShift Red hat public cloud developed application KP-ABE. Following step are used for create application.

1) Register user details openshift public cloud and verify through mail.
2) Create application in with following tools
   - JBoss Developer Studio
   - Mysql 5.0
   - PHP MY Admin4.0
3) Application map with Eclipse (Kepler)IDE

Table 1: User Credential on public cloud

S. No	User ID	Password
1	vinod@gmail.com	vinod123
2	user@gmail.com	User123

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

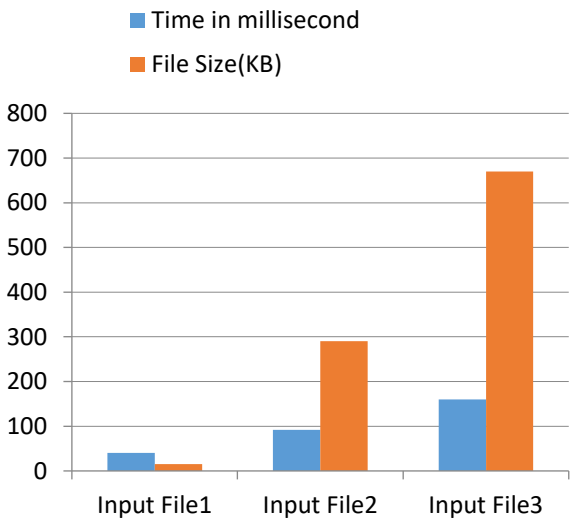

Figure 4 Graph of KP-ABE for different Files

Table 2: Time Complexities of modified KP-ABE

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

5. CONCLUSION

The third party mechanism deals with continuous monitoring of user record. This monitoring along with improved throughput and efficiency is achieved. Out of these methods an enhanced secure scenarios is generated through our proposed KP-ABE. At the initial level of our research, we get the following benefits.

- Improved security solution with less operational overheads and retains reliability on novel encryptions
- Unauthorized access is blocked using improved key generation through user characteristics.

Continuous monitoring gives the user behavior measurements and analyzes the affection of such novel cryptosystem on other services

REFERENCE

[1] Shucheng Yu , “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.
[2] Srijith “Towards Secure Cloud Bursting,Brokerage and Aggregation” 2010 Eighth IEEE European conference on web services
[3] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE,KuiRen, Member, IEEE, and Wenjing Lou, Member, IEEE “Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE-2012
[4] Cong Wang1, Qian Wang1, Kui Ren1, and Wenjing Lou2,” Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing”, IEEE INFOCOM 2010, San Diego, CA, March 2010
[5] Ms. Vaishnavi Moorthy1, Dr. S. Sivasubramaniam2,” Implementing Remote Data Integrity Checking Protocol for Secured Storage Services with Data Dynamics and Public Verifiability In Cloud Computing, IOSR Journal of EngineeringMar. 2012, Vol. 2(3) pp: 496-500
[6] C. Hota, S. Sanka, M. Rajarajan, S. Nair, "Capability-based Cryptographic Data Access Control in Cloud Computing", in International Journal of Advanced Networking and Applications, Volume 01, Issue 01, 2011.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[7] Rosario Gennaro and Daniel Wichs, Fully Homomorphic Message Authenticators IBM Research, T.J. Watson, May 23, 2012
[8] K. Kajendran, J. Jeyaseelan, J. Joshi, "An Approach for secures Data storage using Cloud Computing" In International Journal of Computer Trends and Technology- May to June Issue 2011
[9] W. Luo, G. Bai, "Ensuring the Data Integrity In Cloud computing" In Proceedings of IEEE CCIS, 2011.
[10] S. Sanka, C. Hota, and M. Rajarajan, "Secure data access in cloud computing," in 2010 IEEE 4th International [13] http://en.wikipedia.org/wiki
[11] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.
[12] Dianli GUO and Fengtong WEN, "A More Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment", in Journal of Computational Information Systems, ISSN; 1553–9105, Vol. 9:No. 2, 2013, 407-413
[13] Kristin Lauter, Michael Naehrig andVinod Vaikuntanathan, "Can Homomorphic Encryption be Practical", in ACM, 2008.
[14] Craig Gentry, "Computing Arbitrary Functions of Encrypted Data", in ACM by IBM T.J. Watson Research Center, 2008.
[15] Bharath K. Samanthula, Gerry Howser, Yousef Elmehdwi, and Sanjay Madria, "An Efficient and Secure Data Sharing Framework using Homomorphic Encryption in the Cloud", in Cloud 1st conference by ACM, ISSN: 978-1-4503, DOI: 1596-8/12/08, 2012.
[16] Robert Griffin and Subhash Sankuratripati, "Key Management Interoperability Protocol Profile Version 1.1", in OASIS Standards Organizations at http://docs.oasis-open.org/kmip/profiles/v1.1/os/kmip-profiles-v1.1-os.doc, 2013.
[17] Web Article, "Amazon Web Services: Overview of Security Processes" by Amazon Services at http://aws.amazon.com/security,June 2013.
[18] K. Raen, C. Wang, Q. Wang, "Security Challenges for the Public Cloud", Published by IEEE Computer Society, Jan/Feb 2012
[19] J.-P. Aumasson, L. Henzen, W. Meier, and R. Phan, "SHA-3 proposal BLAKE," December 2010.
[20] GALS System Design: Side Channel Attack Secure Cryptographic Accelerators
[21] AES encryption and decryption http://www.iis.ee.ethz.ch/~kgf/acacia/c3.html
[22] Kamara, S., Lauter, K.: "Cryptographic cloud storage". In: Proceedings of the 14th international conference on financial cryptography and data security, FC'10, pp. 136-149. Springer-Verlag, Berlin, Heidelberg (2010)

CITE AN ARTICLE

Kushwaha, V. K., & Nagle, M. (2018). IMPLEMENTATION OF DATA CONFIDENTIALITY USING IMPROVED KP-ABE SYSTEM. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 7*(6), 391-395.