I. J. Computer Network and Information Security, 2016, 10, 53-60
Published Online October 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.10.07

Enhancing Data Security and Access Control in Cloud Environment using Modified Attribute Based Encryption Mechanism

Apurva R. Naik
Asst. Prof. Yeshwantrao Chavan College of Engineering, Nagpur, India
E-mail: apurva.n2011@gmail.com

Lalit B. Damahe
Asst. Prof. Yeshwantrao Chavan College of Engineering, Nagpur, India
E-mail: damahe_l@rediffmail.com

Abstract—Social networking and growing popularity of cloud services have made everyone to communicate each other in an easiest way. File sharing and distribution are the frequently used services provided by cloud service providers, although these facilities reduce cost of data sharing but at the same time data security and access control is the major problem. Many renowned service providers have faced the challenges to secure data and provide better access control, and we know once the data is leaked we cannot recover the data loss. Thus in order to ensure better security we need for focus on the two major problems, and those are access control and encryption policy. Cipher text policy attribute based encryption is the most effective solution for access control in real time scenarios where owner can actually decide the access rights for the end-user, but it comes with key escrow problem. We are proposing our modified escrow-free key issuing protocol to solve the problem of key escrow and our Modified Attribute Based Encryption scheme to achieve all security requirements to get a robust and secure system. Further we evaluate our model on the basis of results and lastly we conclude the paper.

Index Terms—Cloud computing, Key Escrow, Attribute Based Encryption, Integrity, Confidentiality, Access control.

I. Introduction

Cloud security is one of the major issues day by day with the increase in latest technology. Cloud service providers give us the facility in one of the three forms SaaS. Paas, IaaS. Every service provided by cloud has its own advantages. One of the important aspects focusing in the cloud computing technology the cost of data sharing but at the same time security assurance is also the important goal to be achieved.

Following are the short summary about the layers of cloud computing consisting of what type services it provides and what is the mechanism used by these services by various service providers. Cloud computing structural design consists of three layers: Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS). As shown in figure 1. The figure shows the service layer and the applications levels.

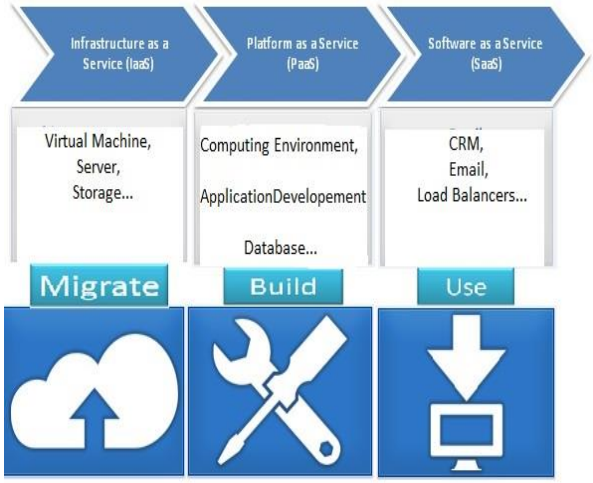

Fig.1. Cloud Services and Their Application

1. SaaS: Software as a Service (SaaS) is referred as the Cloud application services or Software as a Service (SaaS) using a cloud infrastructure or platform this cloud offers implementations of specific business functions and business processes. For example Google Docs, SAP Business by design, Providers of SAAS include ZOHO, Google, and Intuit [1] which provides various security parameters such as AES using 256 bit encryption; video alarm monitoring and disaster recovery options but intuit is not suitable for cost.
2. PaaS: Platform as a Service Cloud makes use of APIs to control the performance of a server hosting engine. Examples are Google App Engine, Windows Azure (Platform). In case of PaaS service providers like Google [2] provides an automatic encryption of the data in which it uses the 128 bit

Copyright © 2016 MECS

Advance encryption Standard, which serves security from unauthorized access i.e. security measures including internal audits, Rat Proxy etc. The only disadvantage was that there is a limit for storing data and downtimes in Google. Amazon's Simple Storage Service (S3) provides huge amount of user data storage at various storage servers located in different locations. The security features provided by Amazon web services [3] includes Amazon Identity and access management. Amazon Web Services (AWS) management console, Hash-based Message Authentication Code (HMAC) and Secure Hash Algorithm (SHA 1) signature is used for authentication. Where uploads or downloads is slow and unreliable. Maintaining the data privacy is the main issue Amazon currently facing now a days.

3. IaaS: it is called as Resource Clouds; it presents managed and scalable resources as services to the user [4]. Some examples are SQL Azure, Amazon S3. (IaaS) like Verizon [5] provides the scanning which is used for anti-virus, uniform resource locator filtering, image control and anti-spam. Encryption and Incident response management are the attractive features provided by Verizon. The only disadvantage of Verizon is configurability of different server hardware and the cost.

Clouds carry out a broad range of benefits including, computing resources, commercial savings, Flexibility. However, privacy and security concerns are exposed to be the primary issue. Table 2 shows various security issues in cloud computing. Hackers are increasingly attacking cloud as they see the cloud as a fruit bearing jackpot [6]

Many sites provide different types of access to the data like Facebook, LinkedIn Flicker, Orkut, Twitter and many more. Some may provide facility to share data publically or some may provide to have data stored privately, or some share with friends. This shows that all the owners have rights to share data to others according to the groups provided by the sites but at the same time right to choose the people for sharing data with particular attributes example according to city, designation, ID these features are not included, thus we can say currently fine grained data access is not provided.

According to the data maintained by Privacy Rights Clearinghouse in United States [7] 895,531,860 Records were compromised in 4675 Breaches, which include hacking, payment card fraud, insider, unintended disclosure and some unknown till now, in last ten years from year 2005 to 2015. Large data can be copied from internet with almost no cost and can be spread throughout the internet in very less time. In the most cases the information leakage is not reported may be due to fear of losing customer's faith or penalties [8]. Also risk for getting caught is low. Social networking sites and smart phones have made the situation critical. Thus it's the most severe threat for the data security not only for organizations but for the individuals.

Many cloud service providers like Amazon, Google Drive, AppHarbor, Microsoft azure, One Drive, Apple iCloud provide facilities to store huge amount of data in pay as you go. Cloud service providers may assure the security and reliability of their services, but actual cloud services are not as safe and reliable as they claim. The major cloud computing vendors observed accidents. Amazon's Simple Storage Service was interrupted twice in February and July 2009. In March 2009, security vulnerabilities found in Google Docs and led to serious leakage of user private information. Gmail appeared a global failure up to 4 hours. Amazon's S3 was interrupted twice in February and July in the same year in 2009. According to news published in business insider, India it was found apple iCloud[9] was compromised. From these scenarios one thing which must be noted and that is privacy as well as security are the issues that should be considered to improve.

Mostly filters are applied to provide privacy in the social network but once the data is compromised over the cloud the filters are of no use. Traditional security issues are still in existence in cloud computing, such as privacy is associated with the data, use of data and disclosure of the data. Due to openness and multi-tenant characteristic of cloud user data may accessed by other unauthorised users. We can minimize the loss by applying some standard methods. After analysing all the pros and cons of the possibilities to achieve security we decided to use AES encryption algorithm [10].

Table 1. Various Issues in Cloud Computing

Sr.No.	Type	Issues
1	Access Control	Browser Security Account and service hijacking Authentication mechanism Malicious insiders
2	Cloud services	Quality of service Reliability of service providers Multi-tenancy
3	Data security	Data loss and leakage Data privacy Data protection Data availability
4	Networking	Security configurations IP vulnerabilities
5	Security Standards	Lack of security standards Lack of auditing Trust

The Table 1 shows all the cloud issues enlisted which can cause danger to the security of organizations and private sector. We can work to minimize each problem enlisted in the table. By applying standard and most secure algorithms if used effectively.

Rest of the paper is organized as follows: Section II discusses shortly about Background of Attribute based encryption. Section III presents Related Work done in the area of the attribute based encryption and variations of the ABE scheme, the working methodology and advantages and drawbacks of the schemes. Section IV presents the Proposed Work including the working of the scheme. Section V focuses on the results observed after implementing the system, by considering overall

Copyright © 2016 MECS

Important Parameters of an ideal system and efficiency is compared. Finally we will conclude the paper in Section VI.

II. Background

The term Attribute Base Encryption is the area where many researchers have contributed from the last few decades. Traditional encryption mechanism works in the PKI in which a data owner should know the public key of the user with whom he wish to share data resulting in increase in processing and high bandwidth consumption. IBE [12] scheme only identities were used to encrypt data by the owner. For example if Alice wants to share the data with bob she simply uses the email address of bob to send the data for example: bob@gmail.com.

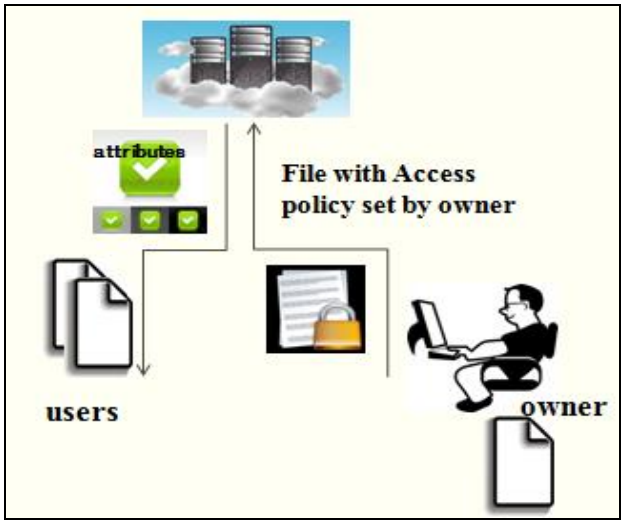

Fig.2. Working of Attribute Based Encryption Scheme

Attribute based encryption was first introduced in the year 2005 by A. Sahai and B. Waters[13]it is a public key encryption method which allows the owner to encrypt data or files according to user attributes. While in decryption the threshold value is set i.e. if there are three attributes present roll no, year, branch, name and if the threshold values are satisfied by user attributes then it results into successful decryption. Figure 2 shows the general working of attribute based encryption scheme.

III. Related Work

2006 Goyal[14] introduced KPABE scheme, the idea behind this scheme was to propose general key-policy. It is the modified model of ABE. The decisional bilinear DiffieHellman (DBDH) assumption was used for the technique. This scheme is called the KP-ABE because every secret key is associated with a tree access structure which denotes the type of cipher text can be decrypted by the secret key. Thus secret key holder can decrypt the cipher text if and only if the attributes associated with the cipher text satisfy the access policy associated with the secret key. The scheme gave superior method for encryption but has one drawback as its key policy attribute based encryption the owner cannot decide who can decrypt the file shared. It has monotonic access structure thus it cannot show negative attributes. Except with that user don't want to share data. CP-ABE [15] basically was proposed to solve the issue of fine grained data access control for the data sharing systems. In case of Cipher text policy attribute based encryption cipher text is associated with an access policy and the user secret key is associated with a set of attributes. Thus secret key holder can decrypt the cipher text if and only if the secret key satisfies the access policy associated with the cipher text. In CP-ABE the receiver has the access policy in the form of a tree structure with attributes as leaves and monotonic access structure with AND, OR and other threshold gates. This scheme not only suits the real time applications but this scheme removes the limitations of KP-ABE scheme. The limitations of CP-ABE are scheme decryption process takes extra computation overhead to the users. [16] Proposed a threshold ABE scheme this scheme was collusion resistant but it came with the disadvantages. R. Ostrovsky[17] proposed a method ABE with non monotonic access structure in which the secret keys were labelled with attributes with positive and negative attributes. In comparison to the ABE scheme with non-monotonic access structure can express a more complicated access policy. This method doubled the size of the cipher text and secret key and created encryption and decryption overheads. Yu, S., Wang, C., Ren, K., Lou, W. [18] proposed scheme combines the Attribute Based Encryption scheme with Proxy re encryption and Lazy-re-encryption to achieve the efficiency. The scheme also maintains the accountability to some extent through the advent of AHL and UL. The Attribute History lists is mainly managed for tracing the evolution of attribute versions and Proxy re encryption keys (PRE keys) and it upholds the User List (UL) for recording and accounting the IDs of all the verified and genuine users in the system. This scheme to achieves this goal by exploiting KPABE and. It enables the data owner to delegate most of computation overhead to cloud servers. Also confidentiality of user access privilege and user secret key accountability can be achieved in this model. Bethencourt, John, Amit Sahai, and Brent Waters, [19] Presented the derivative of ABE and it proved as a prominent scheme by deciding who can decrypt the data stored at cloud server following that there were other schemes which focused on scalability, fine graininess and multi authority based concepts. The challenging issue to decompose access control policies like two layer encryption is addressed in the paper and an efficient group key management scheme which supports the access control are proposed by M Nabeel, E Bertino [20], the said scheme assures the confidentiality and privacy of users from the cloud. A.Rani, [21] addressed the issues like revocation while applying encryption mechanism for data security. By mainly focusing on access control and security the author used hashing technique SHA1. The scheme used 2pc protocol between the key generation centre and data storage centre to avoid the key escrow

Copyright © 2016 MECS

problem. Balamurugan B, Venkata Krishna P. survey of all varieties of the Attribute Based Encryption (ABE) access control techniques available to be used for cloud environments [22].

Deyan Chen, Hong Zhao [23] addressed the challenges in privacy protection and sharing data while protecting personal information. According to the author in analysis for data security and privacy protection issues, it is expected to have an integrated and comprehensive security solution, The idea of Authorization and access control and the need of fine grained access authorization is propose in future work of this paper. Yu, S., Wang, C., Ren, K. and Lou, W proposed the scheme [24] that uniquely integrates the proxy encryption with CP-ABE, the scheme majorly focus on issue of attribute revocation. It is proved that proposed scheme is secure against chosen plaintext attacks. As Sahai and Waters proposed a single-authority ABE scheme they left one question unanswered which was is it possible to construct the scheme for multi authority? This question was answered by Chase [25] who proposed the first multi-authority ABE scheme. It was found that it's inappropriate for security to decrypt all the secret keys by single authority. These schemes are divided into two types multi-authority with central authority and multi-authority without central authority. further Cheung and Newport [26] in addition to AND gate attributes they used a X Element which is Do Not Care term for attribute which does not appear in the AND gate. But the drawback found in the scheme was the size of cipher text increases the key also increased with total number of attributes. Thus the scheme [15] found superior to the scheme proposed by Cheung and Newport. ABE with non-monotonic access Ostrovsky[27] proposed an attribute-based encryption with non-monotonic access structure in year 2007. In which formula of access structure in user's private key can denote attributes such as negative. Boolean formula, NOT in access structure makes it different from other scheme. Even if this make its access complex but this method doubled the size of the cipher text and secret key and created encryption/decryption overheads. Hierarchical attribute based encryption G.Wang, Q.Liu, and J.Wu, proposed HABE[28] which is the combination of hierarchical Identity based encryption and cipher text attribute based encryption. The only drawback in the scheme is it does not support multiple attribute allocation. Thus it is removed by Zhiguo Wan, Jun'e Liu, and Robert H.Deng in HASBE [29] scheme proposed in 2012. S. Zhu, X. Yang and X. Wu [30] proposed the CPABE scheme without parings, this scheme is divided into two phases, phase 1 consist of generating and distributing licence and second phase consist of encrypting the data with conversation key. The scheme builds the file sharing system in order to simplify licence revocation.

J.hur proposed [31] the scheme which enhances data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without enough credentials. Also proposed scheme can do an immediate user revocation on each attribute set while taking full advantage of the scalable access control provided by the cipher text policy attribute-based encryption, Therefore, the scheme achieves more secure and fine-grained data access control in the data sharing system enables immediate user revocation on each attribute set while taking full advantage of the scalable access control provided by the cipher text policy attribute-based encryption CPABE. Therefore, the proposed scheme achieves more secure and fine-grained data access control in the data sharing system. Finally the author concluded the scheme is efficient and scalable to securely manage user data in the data sharing system. Zhibin Zhou; Dijiang Huang; Zhijie

Wang[32] proposed PPCP-ABE which is compared with the CPABE scheme, after testing it is concluded that PP-CP-ABE reduces the size of cipher text from linear to constant and supports expressive access policies and the security of proposed model is based on selective-ID attackers. Venkateshprasad Kalluri and D.Haritha [33] presented the basic development of the CP-ABE scheme and process of the formation of access structure in CPABE. As cloud computing is very adaptive technology and access control helps reduce computational demanding operations on the cloud server.

The paper [34] addresses the problem of provenance and how to encrypt search while protecting confidentiality of data provenance stored in the cloud. The proposed system is capable of handling complex queries for data search, finally, the system entities do not share any keys and even if a compromised User (or Auditor) is revoked, the system would be able to perform its intended operations without requiring re-encryption.

Shuaishuai Zhu, Xiaoyuan Yang, XuGuang Wu, proposed CP-ABE-WP[35] which is an improved CP-ABE, Based on the proposed scheme, they created a secure file sharing system (SFSS) with attribute computing support to simplify license revocation mechanism, system cost, the scheme distribute the file sharing permission by issuing license to the target receivers. Apart from these researches the authors [36] worked on intrusion detection with layered approach, [37][38]efficient data storage and solutions to security attacks respectively.

IV. Proposed Work

In our proposed scheme we are focusing mainly on the basic security requirements i.e. confidentiality, integrity and availability as well as some additional futures like authenticity and accountability.

There are following entities will be participating in the process.

1. Owner: it is the one who owns data and wishes to share the data into the external data storing center for ease of sharing and cost saving. At the same time he will be responsible for defining attribute based access policy.
2. User: it is the entity who is interested to access the data. If the user posses the attributes which satisfy the access policy which is enforced by the data

owner and if he is not been revoked then he will be able to decrypt data shared by the owner.

3. Data storage center: the data sharing service is offered by data storage center (DSC), and it is responsible for controlling access form users. It is a key authority which generates partial keys with key generation center and helps to remove key escrow. It provide retrieval, sharing and destruction service.
4. Key generation center: KGC is another key authority which generates partial keys with data storage center.

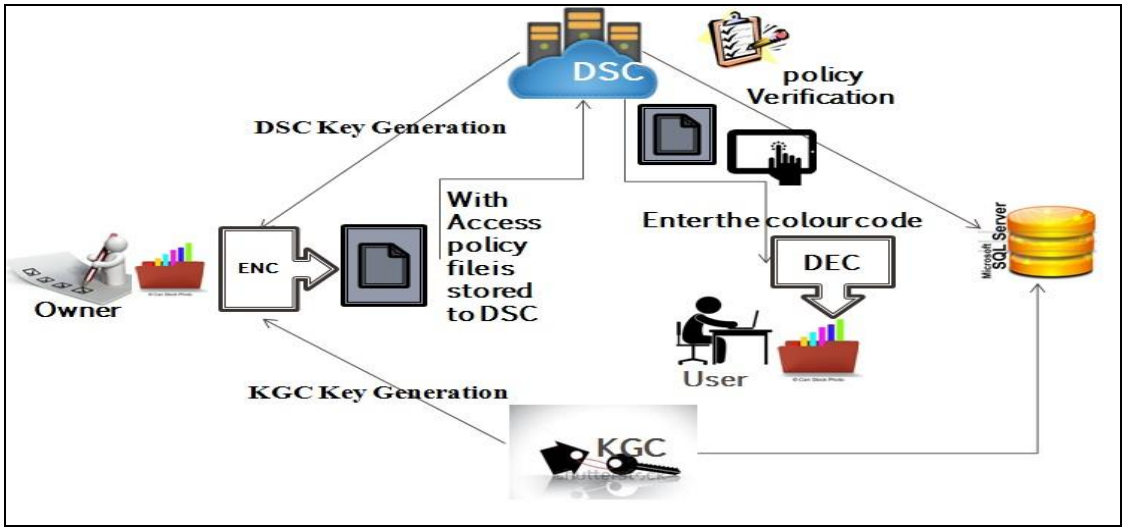

Fig.3. Working of Modified Attribute Based Encryption

Firstly the owner selects the attributes for the user with whom he wishes to share the file, after selecting the attributes, KGC and DSC generates two different partial keys for the owner, then owner who wish to share his file encrypts the file with first key that is issued from KGC and then that partially encrypted file is again encrypted by the owner with key generated by DSC. This protocol solves the key escrow problem which is the most serious problem that causes threat to confidentiality of keys. The figure 3 shows the working of our proposed model. By implementing this technique confidentiality is automatically maintained.

Notations:

A-Attributes
K1- Key generated by Key Generation Centre.
K2-Key generated by Data Storage Centre.
Pl-Plain text
FKn-File Encrypted by K1
En- File encrypted by K2
C-Colour code

ENCRYPTION PROCESS:

Start
Input_encryption_func(A,K1,K2,Pl)

Step 1:Compute k1, k2 for each file
Step 2: Encryption 1 :(Pl, K1)->FKn
Step 3:Encryption 2 :(FKn, K2)->En
Output: En, C

Output: Encrypted File-En

DECRYPTION PROCESS:

When the file is stored in the data storage centre with selected attributes, at the same time the second authentication of colour code is generated and saved in the database with the selected number of users i.e. even if any intruder may gain access to the user password for the system he cannot retrieve the files from the cloud without entering the colour code for the selected file. i.e. at the other end when user is required to enter the unique attribute, when all the attributes associated file are satisfied then only he will be able to decrypt the file.

Start
Input_Decryption_func(En, C, K1,K2,A)
if (Attr==A)
{
If (code C== Sec_code)
Decryption 1 :(file_dsc_enc, K2)-→FKn
Decryption 2:(file_kgc_enc, K1)-→Pl
Else
Enter correct Code
}
Else
Access denied
Output: plaintext file- Pl.

Here DSC which is genuine but curious, if we consider cannot decrypt the file individually because it has only partial key. Same as DSC the KGC cannot decrypt the file alone. The entry is maintained in database provided the DBA is genuine, and database performs log monitoring which maintains all the records of users, files

accessed by users etc.

The log is maintained in database to performs log monitoring which maintains all the records of users log to the system, date of access, action performed etc. on the basis of these information the admin can take decision whether to revoke user from the system or not.

V. Results and Descussion

We implemented the test results on the two different schemes CP-ABE-WP [30] and our proposed model MABE. The tests are performed on the windows environment Microsoft visual studio 12. Intel i3, 1.70 GHz processor, with 4 GB RAM.

When it comes to the system efficiency there must be one parameter everyone should consider and that is time. Encryption and Decryption time parameter plays an important role. The following table shows the encryption and decryption time required for the files.

Following are the results based on the encryption and decryption time required by system, when files are tested on datasets [11].

Table 2. Encryption Time

File size	CP-ABE-WP[3]	MABE
20	593.034	21.0012
40	593.034	22.0013
60	1247.07	24.0014
80	1220.07	27.0016
100	1297.07	39.0022

Table 3. Decryption time

File size	CP-ABE-WP[3]	MABE
20	24.0014	75.1907
40	28.0017	50.4356
60	30.0017	58.0879
80	34.0019	69.4321
100	34.0019	63.2145

From the results we observed that we have decreased the total computation time. Following figure 4 shows analysis graph which shows, the time required for encryption, decryption and total computation overhead on the basis of the values obtained. After comparing values we observed that the overall computation overhead of the existing scheme is more than our scheme.

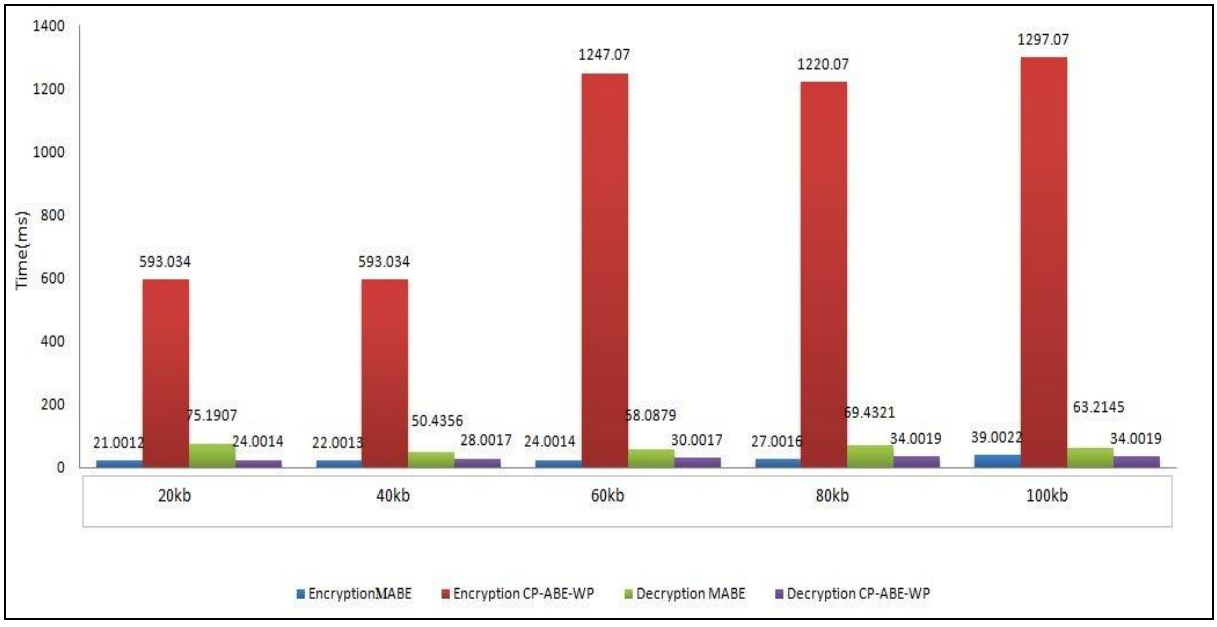

Fig.4. Encryption and Decryption time required for Modified Attribute Based Encryption

VI. Conclusion and Future scope

Attribute based encryption is the is largely used technique for providing access control, In comparison to KP-ABE, CP-ABE schemes are more suitable for the realistic scenes. In CP-ABE scheme user can decide with whom he wants to share his data and it is used to implement the access control over social networking sites and cloud storages, also it provides the fine grained access control. While in KPABE owner cannot select the data sharing policy. CP ABE is the promising solution suitable for cloud system environment. We have designed a system which will fulfill all properties required for a security system that are confidentiality, integrity, availability, access control, authentication, accountability. The main issue of key escrow is solved, and many essential features like password encryption and mail verification are implemented. In addition to these log monitoring and revocation makes the system more effective. As per the analysis done it is observed that the

time required total computation is less in our MABE scheme thus it provides more security because the double encryption method makes the cipher text more secure. Thus according to our analysis and test, MABE mechanism is secure and efficient. Our modified Attribute Based Encryption mechanism in the overall computation overhead is minimized. Which makes the system faster and double encryption makes the system more secure. Thus according to our analysis and test, MABE mechanism is secure and efficient.

In future the system should be tested on larger file sizes; the video format should be tested.

More fined grained access can be provided by deciding more number of attributes and level of security.

REFERENCES

[1] http://www.salesforce.com/assets/pdf/misc/WPForcedotcomSecurity.pdf

[2] https://cloud.google.com/files/Google-Common-Security/

[3] http://media.amazonwebservices.com/AWSSecurityBestPractices.pdf

[4] Allen Oommen Joseph, Jaspher W. Kathrine, Rohit Vijayan, 'Cloud Security Mechanisms for Data Protection: A Survey.", International Journal of Multimedia and Ubiquitous Engineering, 2014.9(9), pp.81-90.

[5] http://cloud.google.com/files/Google-Common-Security-WhitePaperv1.4.pdf

[6] http://www.computing.co.uk/ctg/news/2429256/hackers-see-cloud-as-afruit-bearing-jackpot-for-cyber-attacks

[7] http://www.privacyrights.org/data-breach/new/

[8] http://www-03.ibm.com/security/data-breach/

[9] http://en.wikipedia.org/wiki/2014celebrityphotohack/

[10] http://www.axantum.com/AxCrypt/etc/seagate128vs256.pdf

[11] http://www.cs.cornell.edu/home/llee/data/convote.html

[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology: Proceedings of (CRYPTO '84), Springer, Berlin, Germany, 1985. vol. 196 of Lecture Notes in Computer Science, pp. 47–53,

[13] A.Sahai and B.Waters, "Fuzzy identity-based encryption," in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 3494. Springer, pp. 457–473, 2005.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89–98, November 2006.

[15] Bethencourt J, Sahai A, Waters B. "Ciphertext-policy attribute-based encryption." InSecurity and Privacy, 2007. SP'07. IEEE Symposium on 2007 May 20 (pp. 321-334).

[16] D. Nali, C. Adams, and A. Miri, "Using threshold attribute based encryption for practical biometric-based access control," International Journal of Network Security, vol. 1, no. 3, pp. 173–182, 2005.

[17] R. Ostrovsky, A. Sahai, and B.Waters, "Attribute-based encryption with nonmonotonic access structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 195–203, November 2007.

[18] Yu, S., Wang, C., Ren, K., Lou, W., "Achieving secure, scalable and finegrained data access control in cloud computing", In INFOCOM, March-2010.

[19] Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertextpolicy attribute based encryption." Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007.

[20] Nabeel, M.; Bertino, E, "Privacy Preserving Delegated Access Control in Public Clouds," in Knowledge and Data Engineering, IEEE Transactions on , vol.26, no.9, pp.2268-2280,Sept.2014 doi: 10.1109/TKDE.2013.68

[21] A.Rani, "Improving Security and efficiency in Distributed Data Sharing and Data Leakage Detection System", International journal of emerging sciences and research technology, ISSN: 2277-9655, November, 2013.

[22] Balamurugan B, Venkata Krishna P, "Extensive Survey on Usage of Attribute Based Encryption in Cloud", journal of emerging technologies in web intelligence, vol. 6, no. 3, august 2014.

[23] Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, 2012.

[24] Yu, S., Wang, C., Ren, K. and Lou, W., 2010, April. "Attribute based data sharing with attribute revocation." In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (pp. 261-270). ACM.

[25] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography, vol. 4392 of Lecture Notes in Computer Science, pp. 515–534, Springer, Berlin, Germany,2007.

[26] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 456– 465,November 2007.

[27] R. Ostrovsky, A. Sahai, and B.Waters Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 195–203, November 2007.

[28] G.Wang, Q.Liu, and J.Wu, "Hierarchical attribute-based encryption for fine grained access control in cloud storage services," in Proc.ACM Conf. Computer and Communication security(ACM CCS), Chicago.IL,2010.

[29] Zhiguo Wan, Jun'e Liu, and Robert H.Deng, "HASBE: A Hierarchical Attribute Based solution for Flexible and Scalable Access Control in Cloud Computing," IEEE Transaction on Information Forensics and Security, Vol.7, No.2, April 2012.

[30] S. Zhu, X. Yang and X. Wu, "Secure Cloud File System with Attribute Based Encryption," 5th International Conference on, Intelligent Networking and Collaborative Systems (INCoS), 2013, pp. 99-102.

[31] Junbeom Hur, "Improving Security and efficiency in Attribute-Based Data Sharing", IEEE Transactions on Knowledge and Data Engineering, vol.25, no. 10, pp. 2271-2282, Oct. 2013, doi:10.1109/TKDE.2011.78

[32] [32] Zhibin Zhou, Dijiang Huang; Zhijie Wang, "Efficient Privacy Preserving Ciphertext-Policy Attribute Based-Encryption and Broadcast Encryption," in Computers, IEEE Transactions on , vol.64, no.1, pp.126-138, Jan. 2015doi: 10.1109/TC.2013.200.

[33] Venkateshprasad, Kalluri, D.Haritha, "CIPHER-Text Policy Attribute Based Access to Cloud", IJCSIT Vol. 5 (3), 2014, 2796-2799.

[34] Shin, Dongwan, Rodrigo Lopes, and William Claycomb. "Authenticated dictionary-based attribute sharing in federated identity management." Sixth International Conference on Information Technology: New Generations, ITNG'09 2009. IEEE.

[35] Shuaishuai Zhu, Xiaoyuan Yang, XuGuang Wu, 'Secure Cloud File System with Attribute based Encryption ", 5th International Conference on Intelligent Networking and

Collaborative Systems, 2013 Pages 99-102.
[36] Tesfahun, A. and Bhaskari, D.L., "Effective Hybrid Intrusion Detection System: A Layered Approach", *International Journal of Computer Network and Information Security*, 2015. *7*(3), p.35.
[37] Arani, M.G. and Shamsi, M. "An Extended Approach for Efficient Data Storage in Cloud Computing Environment", *International Journal of Computer Network and Information Security*, *7*(8), 2015, p.30.
[38] Lazzez A, Slimani T. Forensics investigation of web application security attacks. International Journal of Computer Network and Information Security. 2015 Feb 1; 7(3):10.

Authors' Profiles

Apurva R. Naik has received B.E. in Computer Science and Engineering from R.T.M.N.U. Nagpur, Maharashtra, INDIA in 2013. M.Tech in Computer Science and Engineering from YCCE, Nagpur Maharashtra, INDIA in 2016. She has 1 years of experience in teaching. She was lecturer of Computer Technology department in a polytechnic College Nagpur. Currently working as Assistant Professor in Department of Information Technology at Yashwantrao Chavan College of Engineering, Nagpur, INDIA. Her areas of interest are Network Security, Cyber forensics and Ethical Hacking. She has 1 paper in International Conference.

Lalit B. Damahe has received Diploma in Electrical Engineering from BTE Mumbai in 1998, B.E. in Computer Technology from R.T.M.N.U. Nagpur in 2003, M. Tech in CSE from R.T.M.N.U. Nagpur in 2010. He has more than 11.5 years of Experience in teaching. He was Assistant Professor in Dept. of Information Technology at Priyadarshini College of Engineering, Nagpur, for nearly 9 years. Currently working as Assistant Professor in Computer Technology at Yashwantrao Chavan College of Engineering, Nagpur, INDIA. His areas of interest are Image Processing and Computer Graphics and Computer Networks. He is the member of ACM and IACSIT professional society and he has more than 10 papers in National/ International Conferences/ Journals to his credit.

How to cite this paper: Apurva R. Naik, Lalit B. Damahe,"Enhancing Data Security and Access Control in Cloud Environment using Modified Attribute Based Encryption Mechanism", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.10, pp.53-60, 2016.DOI: 10.5815/ijcnis.2016.10.07