ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/331196102

EncryScation: A Novel Framework for Cloud IaaS, DaaS security using Encryption and Obfuscation Techniques

Conference Paper · April 2016

CITATIONS
4

READS
148

2 authors:

Krunal Suthar
Sankalchand Patel College of Engineering
10 PUBLICATIONS **29** CITATIONS
SEE PROFILE

Jayeshkumar Madhubhai Patel
Ganpat University
96 PUBLICATIONS **215** CITATIONS
SEE PROFILE

All content following this page was uploaded by Jayeshkumar Madhubhai Patel on 19 February 2019.

The user has requested enhancement of the downloaded file.

EncryScation: A Novel Framework for Cloud IaaS, DaaS security using Encryption and Obfuscation Techniques

Krunal Suthar
Ph. D. Scholar
Computer Engineering Department
Rai University
Ahmedabad, India
Krunal_bece@yahoo.co.in

Dr. Jayesh Patel
Associate Professor
Department of MCA
Acharya Motibhai Patel Institute of Computer Studies
Kherva, India
jayeshpatel_mca@yahoo.com

***Abstract*—Now a days every industry needs more income with less investment behind infrastructure. Here, the new era of Cloud computing comes where the user can have everything on rent and "pay as go" fundamental. Cloud users are able to store their valuable data on Cloud premises and make themselves free from local burden. While users data is available on Cloud servers, it is very important for the user that data must be secure when it is in transition and even after it has been stored on server. Most of the researchers think for the user centric(side) scenario i.e mainly consider the security issue related to Cloud users like Integrity checking, Authentication, Versioning Etc. On the other hand, some researchers provide their view related to working of Cloud service providers i.e. Database encryption, Security based on Metadata, Data Obfuscation Etc. To have proper confidentiality, Security and integrity of data, this paper presents two techniques, that is: Encryption, authentication at client side as well as Data Obfuscation at server side. Encryption helps user to provide secrecy to its data when it is transferred in the network. Data obfuscation helps service provider to secure the users data on his premises. By applying these two techniques, the user and Service provider gets maximum protection against intruders and unauthorized access.**

Keywords— Cloud Storage; Data Protection; Confidentiality; Encryption; Obfuscation

I. INTRODUCTION

The cloud computing services i.e Iaas, SaaS, Daas, are mostly used by many of the users now days. In which users can have its own virtual machine which it can use with very least cost and for many reasons like storing its large data, use highly available processing power, get power to use licensed software Etc. In contrast to numerous benefits offered by Cloud computing viz. elasticity, availability, scalability, reliability, speedy processing, location independency etc.; information security concerns are yet to be need addressed before its wide acceptance. As a user, it store lots of important data like Financial information, credential information, Files Etc. on others premises, securing this data is very important before it gets uploaded to the storage cloud, and also in case of data available on cloud storage. Some time Data gets tampered or misused at Providers machine. Cloud user as well Cloud service providers can find solution to achieve Security using techniques like Encryption, Obfuscation.

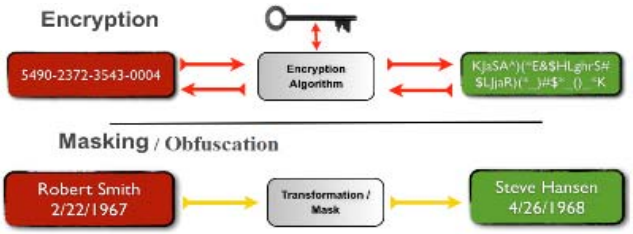

Fig. 1. Encryption / Obfuscation

As shown in above Fig. 1 the primary purpose of encryption is to protect the confidentiality of information stored on local or transmitted via the network. Encryption algorithms play a very important part in the security of data in communications as they not only provides confidentiality, but also the key elements of security like Authentication, Integrity and Non-repudiation.

Data obfuscation is the process of changing the format or structure of data to hide actual meaning of data and makes reverse engineering very difficult. The benefit of obfuscation over encryption is that encrypted data cannot be processed until it is decrypted, but obfuscated data can be processed without de obfuscation.

If we consider encryption of data on client machine based on sensitivity of its data and then storing the information to cloud storage server, gives surety to client about secure transmission of their file on network. For Providers once it available on his premises database which contains information about lots of client in public domain using Obfuscation technique its ensure that no any users data are misuse or tempered by unauthorized access.

This paper uses encryption and obfuscation techniques to provide efficient cloud storage confidentiality. Normally, Integrity or confidentiality is ensured by encryption mechanism, but for security issues in cloud encryption alone is

978-1-4799-9991-0/15/$31.00 ©2015 IEEE

not sufficient for information security [1]. Encryption required integrating with obfuscation technique. While Obfuscation alone is also not good for providing complete security of data in cloud storage because the unauthorized users are able to get information through attack like brute force or sometimes by reverse engineering, which break security of Cloud environment.

The paper is arranged as follows: in Section 2 we discuss about various security proposals, in Section 3 we discuss proposed methodology in detail with analysis. Section 4 gives Conclusion. Finally last Section provides list of References.

II. Literature Review

First, Authors at [1] proposed a cryptographic technique for data security Issues in Cloud computing. In model data are encrypted before stored on storage servers and key of file are available to data owner only; user is only approved by issuing the corresponding decryption keys by owner. Along with encryption they also used obfuscation methods to increase the confidentiality of data. Authors also proposed Algorithms are for encryption and obfuscation technique. Before storing data on Cloud premises it's encrypted or obfuscated at client side. Author argues that the proposed technique is safe to store the cloud users' data on cloud premises. Authors also argue that Encryption only or obfuscation only is not sufficient for cloud data storage. We can say both the technique together provides adequate security/Confidentiality to Cloud User's data in the cloud environment.

Author at [3] presented a model for DaaS Which work to secure data which available on Cloud Machines. Proposed methodology provides two important features First Features indicate about how store data on DaaS. Second feature says that how get data from DaaS so that data confidentiality preserve. They also proposed sensitive columns mechanism for character encryption before sending it on Cloud premises, it also obfuscate Database columns at client side which contains numeric values using mathematical function before sending to Cloud storage. Main focus of proposed model to work with query over encrypted and obfuscated..

III. Proposed Methodology

A. Overview

There are mainly three entities in EncryScation viz. (a) Cloud service provider (CSP) (b) Cloud Data owner (DO) and (c) Cloud Data user (DU). As Shown in Figure 2 CSP is the central component of the entire system and acts as secure data storage repository. It offers the Cloud user to work after authenticate himself. It maintains Cloud users' information; access control (credential) information for all the data files it which is necessary. It also maintains versions of files to keep track of changes made in every data file. Further importantly It provides strong security to users data which available on its database using Data obfuscation..

DO is a Cloud data owner who generates the data. Being an owner of the data, it has got all rights to delete, modify and verify its own data. DO can issue access rights (along with other credentials) to the other users, whom needs the data file.

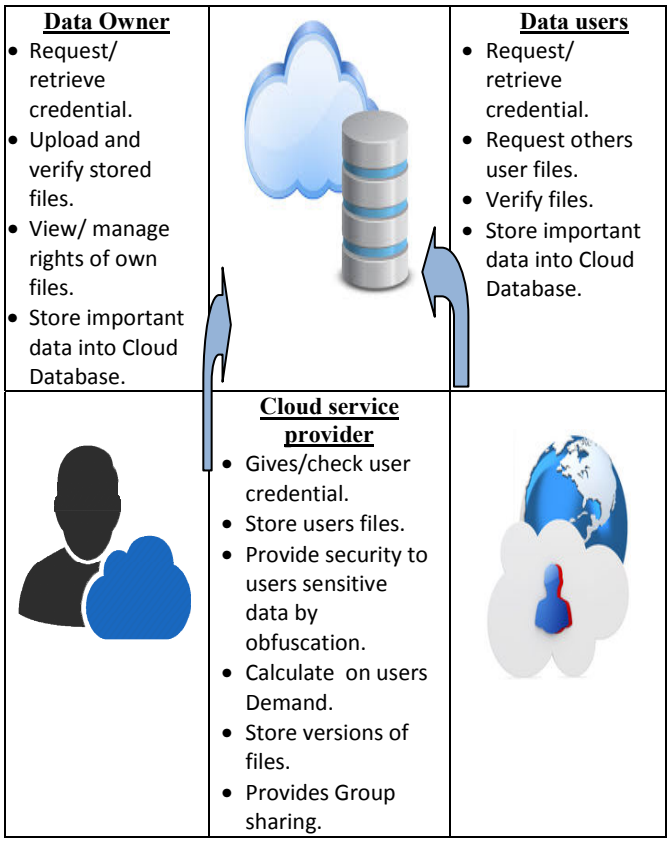

Fig. 2. Proposed model(Basic)

DO intimates to CSP about the action of granting access right to individual or by creating Group sharing facilities. DO maintains the information about shared secret key, encryption algorithm used, hash algorithm used, hash code, list of DUs to whom the access rights issued etc. for every file, locally. DU is the Cloud data user who wishes to utilize the data file that was generated by DO. It requests to DO for accessing a file with required rights. After getting permission from DO, DU requests to CSP for required file. CSP responds to DU by providing encrypted file, which in turn decrypted by CDU at its own premise locally.

B. Algorithm Steps

Table1: Synonym

PK/SK	Public Key/ Symmetric Key	H_S	Hash at server
PR_K	Private Key	DO_ID	Data Owner ID
E/D	Encryption/Decryption	DU_ID	Data User ID
DO/DU	Data Owner/ Data User	OWN_FL	File List
EFL	Encrypted File	US_LST	User List
CSP	Cloud Service Provider	FL_NM	File Name
H_C	Hash code at Client	FL_BITS	File Bits

To achieve proposed scheme we divide our model in 9 different phases.

During Phase 1 for Encryption purpose the Cloud users(Owner/User) both Generate the Encryption key.

Step 1: DO/DU Generate Key pair.

Aim of Phase2 is to make registration on Cloud and to get ID from CSP which used to perform all the operations. Following steps together work in Phase2. First Owner/User send key to Cloud Server and Server Process request Generate ID and send it back to Requester. In After Receiving the ID now user send its Personal Details like Email Name Etc. which store by Server and send Confirmation after verifying all details.

Step 1: Send {K} -> CSP Step 2: CSP - > DO/DU. (Process Request and send {ID}). Step 3: DO/DU -> CSP. (Send Registration Details). Step 4: CSP -> DO/DU. (Verify and Process request).

Aim of Phase 3 Data are need to process before actually sent on Cloud. First DO choose algorithm need to use for secure his data from available algo. Key according to algo and Encrypt the file.. DO can apply Authentication if need on Encrypted file. DO also store Hash of encrypted file in local dataset before send to CSP. During last step Cloud server check existence of uploaded file and if user need to maintain older version then store it by providing version numbers and does necessary modification in Database.

Step 1: DO Choose file, Algo, Key size and generate key. Step 2: E(SK(File)) => EFL Calculate C_H and store in local Database. (step 3 is Optional) Step 3 (PR_K(EFL)) => Ath_FLE ; Send {Ath_FL} - > CSP Step 4: If (Exist(Ath_FL)) CSP store {Ath_FL_Version}, Modify Database. Else CSP store {Auth_file}, Modify Database

In phase 4 Owner sends request to share its file to Group of users (Group Policy). In first step Client send request to CSP which return list of files of Owner as well List of users available. In next step Owner choose file and user with whom it wants to share its file. In last step CSP get details and make Changes in Database accordingly.

Step 1: DO => CPS. Request {DO_ID}. CSP Generate{OWN_FL}, and user list{US_LST} CSP{FL_LST,US_LST} -> DO Step 2: Send {Fl_NM,US_LST} => CSP ; CSP Modify D/B

During Phase 5 our Data owner Verify its file stored on Cloud Premises. During first step Owner get their file list by sending its ID, CSP find files stored on his premises and send list to requester. In next step Owner Choose the file wants to verify and gives details about random bits which user need to verify and send to CSP. At CSP it verify request get record based on

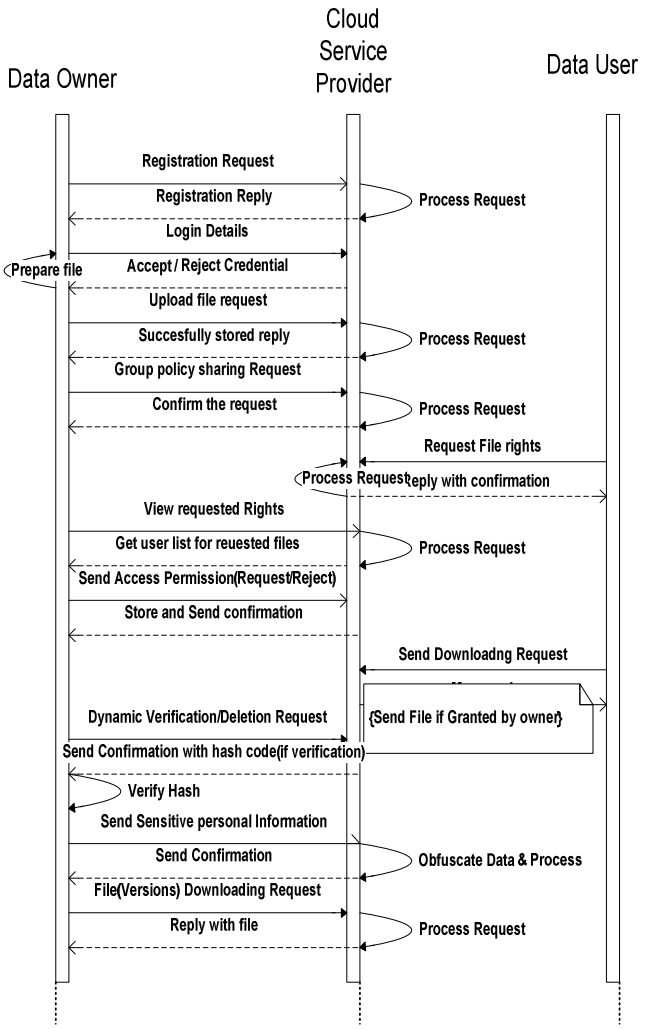

Fig. 3. Proposed Model Work Flow

request and after calculating hash(if needed) send it to User. In last step Requester get data and verify on his premise.

Step 1: DO/DU => CPS. Send ID.; Find and send {OWN_FL}. Step 2: DO/DU => CS. File and Random Bits. Step 3: CSP Find bit from file. Generate Hash(if required) CSP=> DO/DU. Send H(FL_BITS) Step 4: DO/DU Locally check {S_H, C_H}.

Aim of Phase 6 is about Rights management. Once individual DU wants to request owners file which stored on Cloud premises It send request using name of Owner and CSP send list of files. User choose file with required rights and send request on CSP, who modified database accordingly.

Step 1: DU=> CSP. Send request for Owner's file. Step 2 CSP => DU. List of requested owner's file. Step 3: DO=> CSP, FL_NM, RGHTS(R/W).; CSP Manage Database

In Phase 7 Owner check the request come from Users during Previous Phase and Can Grant and Deny the request which come from Users.. In first Phase Owner get all he request which is pending and available on CSP's Database . In next step based on Details Owner Grant or deny the request and Make CSP aware so it makes necessary changes in his database. Here if owner Grant the rights then the key is sent to requester

Step 1: DO=> CSP. Fetch Request details. Step 2: CSP=> DO; Receives {FL_LST} Step3: DO => CSP. ; Send confirmation(Grant/Reject) Step 4: DO=>DU. {SK} sent In case of Grant.

During Phase 8 our wish is to handle sensitive data which is uploaded by DO/DU and protect them against misuse. In step 1 user provides necessary encrypted information and in 2 step CSP obfuscate incoming data and store it in Database

Step 1: Send(Enc(Data)) Step 2: CSP Apply obfuscation; Store Data in Database.

Phase 9 is about Decrypting/Downloading file from CSP. User send request to check list of files which is granted by Owner's. In next step User can download file from Cloud premises. After user can download file and decrypt locally.

The obfuscation/De-Obfuscation is normally always applied in some phases where data will be stored and retrieved from the database.

The below figure 4 gives information about the implementation part. Here user send information on the cloud which will be obfuscated before storing on the cloud which free CSP from worry about theft of the data. Here the Owner manages all the rights may be to assign or to request at file rights option. Once user has access to owners file it can download and decrypt the file locally. User can verify the files anytime from anywhere.

Fig. 4. Model Implementation

C. *Proposed Model Analysis*

Storage Correctness: DO (or DU) can anytime request CSP for data correctness. DO issues a Dynamic random bit request to CSP regarding to the file he created, and CSP gives in form of hash of those bits having size is almost in KB. After receiving hash value from CSP, DO (or DU) compares it with new calculated hash code. If both found same, it is concluded that the integrity of data is verified.

B. Lightweight: Confidentiality and integrity are to be achieved through encryption and hash algorithms. These two cryptographic primitives consume significant computational and hence we recommend these two operations to be performed offline on the premise of DO or DU. To check integrity of data i.e. storage correctness, the whole file is not transferred, but only a small sized data is exchanged between CSP and DO/DU, which is independent of the file size.

C. Encryption based on sensitivity of data: As discussed earlier, data is divided in three categories based on its sensitivity viz. (i) Less sensitive, (ii) Adequate sensitive and (iii) highly sensitive. DO selects encryption algorithm based on data sensitivity, if the data is not sensitive and data is stored without encryption on Cloud.

D. Dynamism: Granting/revoking access rights to/from DU or with the group of users is done through executing SQL query and updating the required Database entry.

E. Versioning: DO/DU is able to store multiple version of their file on CSP and can able to get it as required.

F. Data Obfuscation: The sensitive details like Credential information, Account information Etc. are obfuscated and stored on CSP Database which ensure CSP that DO/DU data are safely available on premises and no chance to tempered or misuse.

Cryptographic operations take considerable execution cost on overall operation of the proposed scheme. So, Here we counted number of cryptographic functions required (E.g. Asymmetric Encryption, Symmetric encryption, Encrypted file sending/Receiving, Hash function Etc) for each phase of the model. Following figure 5 illustrates total number of different cryptographic functions/Obfuscation techniques to be executed for all phase mentioned above.

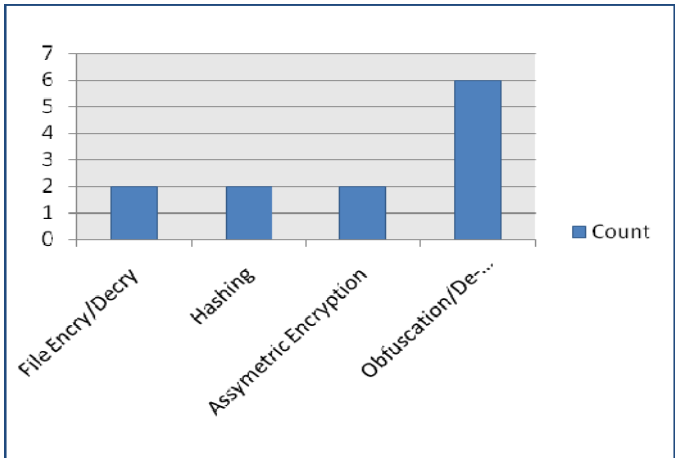

Fig. 5. Overall Number of Cryptographic Operations

Figure 6 below shows phase wise cryptographic/obfuscation operations required. All the hash functions are performed offline and they are quite faster.

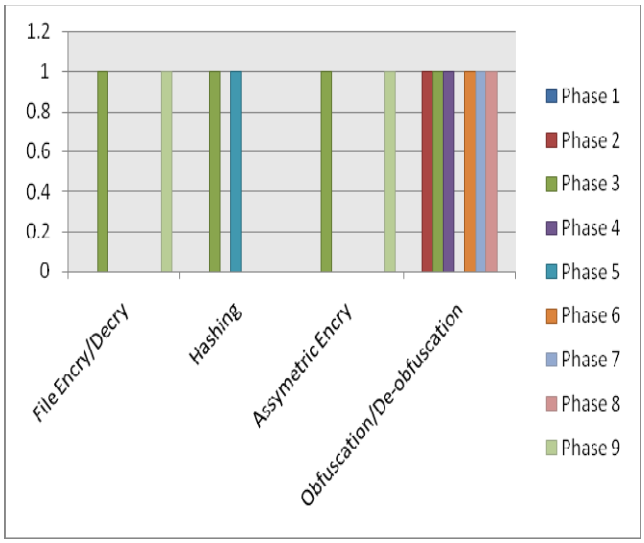

Fig 6. Cryptographic Operations/obfuscation(Phase wise)

By using SHA hash function which executes in few milliseconds to compute a hash of even 1 MB file. So, overall, the overhead occurred by the cryptographic operations involved in EncryScation is very low.

CONCLUSION

Cloud computing provides "pay as you go" services to an individual and enterprise customers with very least cost. But due to lack of security many of the users are beware to adopt it. With this providing enough security to stored important information or a file to publicly available Cloud environment is a burning issue for Service providers today. Data integrity or correctness in the cloud is achieved by providing security to sensitive information. To address the problem of both Cloud user as well service provider, we proposed a new scheme by putting encryption and obfuscation technique works together. Data will be encrypted before sending on Cloud server based on sensitivity of data and user kept key secret gives security to data in transition. Even key is not shared with any one and data available in encrypted format on cloud machine makes user ensure about confidentiality.

Along with above benefits to user, we used obfuscation technique for security purpose at Cloud server side by which there is very less chance of tempering the data. We proposed an algorithm which supports all this operations and proving that user centric and server centric control together which provide adequate security. The proposed scheme also provides other benefits like by implementing Group sharing policy there is no need for every individual to ask for a rights to owner decrease the network traffic significantly. For the purpose of no data lost User can able to maintain multiple versions of file on cloud server which. Data owner can verify files stored without downloading on local premises works fine for low processing power machines. From the Model analysis, it is observed that proposed scheme provides better protection to stored information on a cloud than the existing techniques which are based on encryption, obfuscation technique alone from Cloud users as well Service providers view.

REFERENCES

[1] Arockiam, L.; Monikandan, S., "Efficient cloud storage confidentiality to ensure data security," *International Conference on Computer Communication and Informatics (ICCCI)*, 2014, vol., no., pp.1,5, 3-5 Jan. (2014)

[2] Halder, R.; Cortesi, A., "Obfuscation-based analysis of SQL injection attacks," *Computers and Communications (ISCC),IEEE* Symposium on , vol., pp.931,938, 22-25 June (2010).

[3] Atiq, R.; Hussain, M..: " Efficient Cloud Data Confidentiality for DaaS" *International Journal of Advanced Science and Technology* Vol. 35, October(2011).

[4] Hataba, M.; El-Mahdy, A.; "Cloud Protection by Obfuscation: Techniques and Metrics," *P2P, Parallel, Grid, Cloud and Internet Computing* (3PGCIC), 2012 Seventh International Conference on , vol., no., pp.369,372, 12-14 Nov. (2012).

[5] Suthar, K., Patel, J..: "Security of Cloud IAAS, DAAS Services using Encryption, Obfuscation Techniques: A Review" *Technix International Journal for Engineering Research,* Volume 1 Issue 6, Jan (2015).

[6] Ikechukwu, U.; Omenka. U;, "Building Trust and Confidentiality in Cloud computing Distributed Data Storage" *West African Journal of Industrial & Academic Research*, Vol. 6 No.1 March, pp78-83.(2013).

[7] Xiaojun Yu, Qiaoyan W.; "A View about Cloud Data Security from Data Life Cycle" *International Conference on Computational Intelligence and Software Engineering (CiSE*), pp 1-4, IEEE, Dec.(2010).

[8] Patel H. B.,; Patel D. R.; Borasaniya B.; Patel A. ; "Data Storage Security Model for Cloud Computing" *Advances in Communication, Network, and Computing Lecture Notes of the Institute for Computer Sciences*, Social Informatics and Telecommunications Engineering Volume 108, 2012, pp 37-45.(2012).

[9] Yvette E. Gelogo, Sunguk L.,; "Database Management System as a Cloud Service" *International Journal of Future Generation Communication and Networking* Vol. 5, No. 2, pp 71-76 June (2012).

[10] Hyun-Suk, Yu.; Yvette, E.; Kyung K,; "Securing Data Storage in Cloud Computing" *Security Engineering Research Institute (Journal of Security Engineering),* No. 9, No. 3, June, pp 251-260(2012).

[11] el-Khameesy, N.; Hossam R., "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems" *Journal of Emerging Trends in Computing and Information Sciences*, VOL. 3, NO. 6, June, pp 970-974(2012).

[12] Anitha, R.; Pradeepan, P.,; Yogesh, P.; Mukherjee, S.; "Data Storage Security in Cloud using Metadata" *2nd International Conference on Machine Learning and Computer Science(IMLCS'2013*), Kuala Lumpur (Malaysia), August pp 26-30(2013).

[13] Raja B.,; Kumar S, B., Reddy S., L.; Chandar P, V. ; "CP-ABE Based Encryption for Secured Cloud Storage Access" *International Journal of Scientific & Engineering Research*, Volume 3, Issue 9, September, pp 1-5.(2012).

[14] Wang, C.; Wang, Q.; Ren, K.; Lou, W.; "Ensuring data storage security in Cloud Computing" Quality of Service, 2009. IWQoS. 17th International Workshop on , vol., no., pp.1,9, 13-15 July.(2009).

[15] Mathew, A.; "Survey Paper on Security & Privacy Issues in Cloud Storage System", EECE, Term Survey Paper, April, pp 1-13(2012).4

[16] Mahajan, P.; Setty, S.; Lee, S.; "Depot: Cloud storage with minimal trust" *9th USENIX Symposium on Operating System Design and Implementation*, pp 1-26.(2010).

[17] Mather, T.; Kumaraswamy, S.; Latif, S.; "Cloud Security and Privacy" O'Reilly Media, Inc.,chapter 4, September, pp 61-71(2009).

[18] Kamara S,; Lauter K,; "Cryptographic Cloud Storage" IFCA/ LNCS 6054, Springer-verlag, Berlin Heidelberg, pp 136-149.(2010).

View publication stats