Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 7, July -2017

Public Integrity Auditing With Regenerating Code & Dynamic Group User Revocation

[1]Sanyogita Kamble, [2]Prof. Arti Mohanpurkar

[1,2]*Department of Computer Engineering, Dr D.Y. Patil School Of Engineering ,Lohgaon,Pune,Maharashtra,India*

Abstract--- *Benefited from cloud computing, end users can achieve an efficient and economical technique for information sharing between group members in the cloud with the characters of reduced maintenance and small management cost. Meanwhile, should provide offer security ensures for the sharing information files since they are outsourced. However, due to the fact of the frequent alter of the member-ship, sharing information although providing privacy-preserving is still a challenging issue, particularly for an untrusted cloud due to the collusion attack. Furthermore, for existing schemes, the security of key distribution is primarily based on the secure communication channel, even so, to have such channel is a strong assumption and is difficult for practice. In this paper, propose a secure information sharing scheme for dynamic members. Firstly, suggest a safe way for key supply wanting any safe message stations, and the finish operators can strongly find their isolated solutions after collection director. Secondly, our system can realize fine-grained convenience regulator, some operator in the collection can effort the basis in the cloud and retracted users can't access the cloud over afterward they are rescinded. Thirdly, it can defend the system from collusion attack, which suggests that withdrawn users cannot get the unique information file even if they combine with the untrusted cloud. In this approach, by leveraging polynomial purpose, can attain a secure user revocation scheme. Finally, our arrangement can attain fine efficiency, which suggests preceding workers essential not to inform their isolated solutions for the national either a novel user joints in the cluster or a worker is retracted from the set.*

Keywords-- *Cloud Computing, Encryption, Decryption, Auditing, recovery Server*

I. INTRODUCTION

The progression of cloud computing inspirations attempts what's more, relationship to outsource their data to outsider cloud administrations provider(CSPs), which will upgrade the limit obstacle of advantage accommodate close-by mechanisms. With the qualities of data sharing gives better use of administrations and assets Provides security over client data by hiding their data refined elements. Giving security to end clients data put away in cloud is turned out to be principle requirement since end clients outsource their data. End clients data is ensured as it will be put away in encoded arrange however it is difficult for cloud to give a safe stockpiling structure to dynamic gathering of client in cloud as it is difficult to give verifications.[1] Many plans have been proposed to give a safe data stockpiling and recovery conspires in framework and gives confirmation and secure gathering administration framework for cloud. In any case, any arrangement of them can't give security and efficient assemble client administration. A cryptographic stockpiling framework that empowers secure data sharing on dishonest servers basically in light of the procedures that partitioning files into file gatherings and scrambling each file bunch with a file-piece key. The author abused and consolidated strategies of key approach property based encryption, intermediary re-encryption and languid re-encryption to accomplish fine-grained data get to control without uncovering data substance. For giving the respectability and openness of remote cloud store, a couple of courses of action, and their varieties, have been proposed.[3] In these courses of action, when an arrangement reinforces data modification, call it element arrange, for the most part static one. So propose safe information sharing plan and key conveyance and gathering administration. This framework give following component to bunch partaking in cloud Secure information sharing plan gives successful key dispersion with no safe channel client will get their mystery keys from aggregate director. Client in gathering can get to all assets accessible in cloud yet repudiated client cannot get to files or any assets in cloud. Private Key of that client doesn't have to refresh or recomputed. In this give a security examination to demonstrate the security. Many schemes are planned to supply a secure information storage and retrieval schemes in system and provides authentication and secure cluster management system for cloud, however any system of them cannot give security and economical cluster user management.. This system given a science storage system that allows secure information sharing on untruth servers supported the techniques that dividing files into file teams and encrypting every file cluster with a file-block key. Author Exploited and combined techniques of key policy attribute-based coding, proxy re-encryption and lazy re-encryption [4] to realize fine-grained information access management while not revealing information contents. For giving the honorableness and accessibility of remote cloud store, a number of arrangements, and their variations, are planned. In these arrangements, once an idea supports data alteration, decision it component arrange, typically static one (or restricted component arrange, if an idea might simply effectively bolster some planned operation. Thus propose secure information sharing theme and key distribution and cluster management. This system give following mechanism for cluster sharing in cloud: Secure information sharing theme provides effective key distribution with none secure channel user can get their secret keys from cluster manager [6].User in cluster will access all resources on the market in cloud however revoked user cannot access files or any

@IJAERD-2017, All rights Reserved

resources in cloud. Personal Key of that user doesn't got to update or recomputed. So give a security analysis to prove the protection of this theme.

II. LITERATURE SURVEY

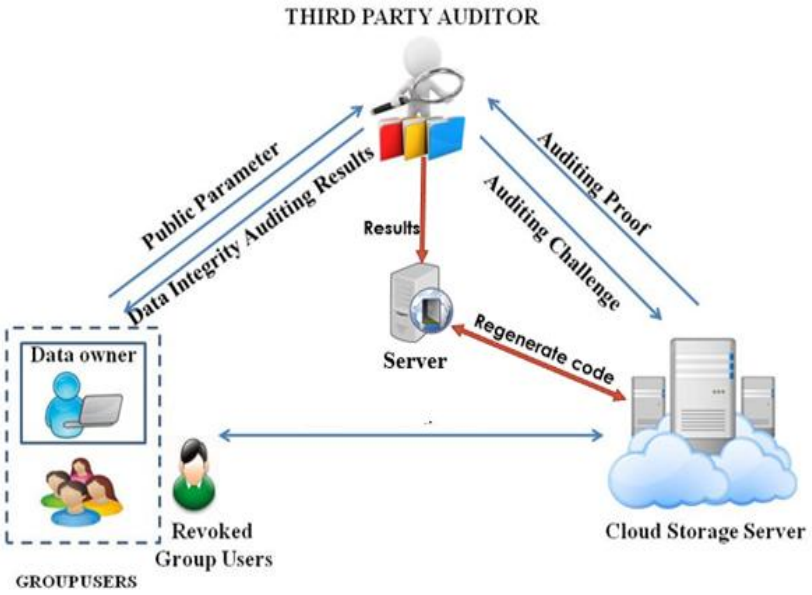
Exploited and mixed strategies of important policy attribute-primarily based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained information access control without disclosing information contents. It is also difficult to share files or resources among group members and also it is costly and requires high maintenance. Re-encryption is based on the attributes of the files .In this paper proxy re-encryption scheme and Secure Distributed Storage. And In this paper key server need not be fully trusted with all the keys of the system and the secret storage [1].
Author provide following mechanism for group sharing in cloud that secure information sharing scheme provides effective important distribution without any secure channel user will get their secret keys from group manager. Once owners file on cloud is lost then this file is lost permanently also there is no authentication of any important provider is provided to manage file uploads and file downloads. Providing security to end users information stored in cloud is become main constraint because end users outsource their information. Also an important issue is raise as how to control and prevent unauthorized accessibility to information stored in the cloud. In this paper Revoke user can access file or resources on cloud after revoke [2].
Sharing information while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Many schemes have been proposed to provide a secure information storage and retrieval schemes in system and provides authentication and secure— group management system for cloud. System also does not have any efficient encryption strategy to protect information of files on cloud. A secure information sharing scheme for dynamic members. Propose a secure way for important distribution without any secure communication channels, and the end users can securely obtain their private keys from group manager. In this system files are divided into groups and each file group is encrypted with a file-block key, and As cloud server is not trusted authority then, So this system cannot verify integrity of files[3].
A new technique for recognizing Cipher text-Policy Characteristic Encryption (CP-ABE)[11] under concrete and no interactive cryptographic assumptions in the standard model.[9] System give option to permit any kind of encrypted to defined access control in terms of any access formula over the features in the system. In this system, cipher text size, file encryption, and also decryption time scales linearly with the intricacy of the access formula. The only previous work to accomplish these criteria was restricted to evidence in the generic group model. In this paper Broadcast group. key management (BGKM) and prove security of BGKM. and Integrity of Files on cloud cannot be verify and if file is loss it cannot be regenerated[4].It will simply suffer from the collusion attack, which might result in the revoked users obtaining the sharing knowledge and revealing different legitimate members' secrets. additionally, there's another security shortage within the user registration part, that is the way to shield the non-public key when distributing it within the unsecure communication channels. Author puts forward new economical constructions for public-key broadcast coding that at the same time relish the subsequent properties: receivers area unit stateless; coding is collusion-secure for indiscriminately large collusions of users and security is tight within the commonplace model; new users will be a part of dynamically i.e. while not modification of user cryptography keys nor cipher text size and tiny or no alteration of the coding key[3].
An important downside publicly clouds is a way to by selection share documents supported fine-grained attribute primarily based access management policies. associate degree approach is to encipher documents satisfying totally different completely different} policies with different keys employing a public key crypto system like attribute primarily based cryptography (ABE), and/or proxy re-encryption (PRE). However, such associate degree approach has some weaknesses: it cannot expeditiously handle adding/revoking users or identity attributes, and policy changes; it needs to stay multiple encrypted copies of constant documents; it incurs high process value. a right away application of a original key cryptosystem, wherever users square measure sorted supported the policies they satisfy and assignment distinctive keys for every cluster, conjointly has similar weaknesses. It tend to observe that, while not utilizing public key cryptography and by permitting users to dynamically derive the original keys at the time of cryptography, one will address the higher than weaknesses. supported this concept, to formalize a brand new key management theme referred to as broadcast cluster key the thought is to present to convey to grant to resign some secrets to users supported the identity attributes they need and later allow them to derive actual original keys supported their secrets and a few public info.[7]A key advantage of the BGKM theme is that adding users/revoking users or change access management policies will be performed expeditiously by change just some public info. Victimization BGKM construct, to propose associate degree economical approach for fine-grained cryptography primarily based access management for documents hold on in associate degree untreated cloud file storage.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

Any user is part of a gaggle with a time stamp before completed time used extends a time stamp, and additionally time stamp over user mechanically revoke from the cluster and once revoke cluster user be part of the cluster once more utilizing the re-registration technique. One member be part of the many group with completely different username

however same email ID. And additionally user sent verification request to TPA for file verified and if get outcome is file is hack or corrupt on cloud then file is regenerated from the server and send to regenerated file to requested user. System design cluster of user transfer files and use resources among cluster. within the System new member need to hitch cluster, then these are 1st send cluster be part of request with specific time stamp i.e. They mansion fundamental quantity sent to requested cluster Owner if cluster owner settle for the user request then requested user be part of the cluster. So user are member of cluster just for that specific fundamental quantity. When time completes member of that cluster are mechanically revoked from the cluster. Within the cluster there are several users and there's information owner for every cluster World Health Organization transfer file on cloud and cluster member World Health Organization need to transfer files and information owner of cluster provides keys to member for downloading files. Information owner will send request to TPA for check verify integrity of file store on cloud. Then TPA verify the files requested by information Owner send Integrity verification response to Server (Proxy) and information Owner, if requested file information corrupt or hack then file is regenerate from server on cloud, send response to the data Owner.

IV. SYSTEM ARCHITECTURE



V. MATHEMATICAL MODEL

This system approach contains below procedures.
A Group Owner creates the group in cloud. User sends request to the group owner to become member of particular group.
After creating group user will be the member of group until owner accept the request.
S1= {I, P, O}
Input:
F= {f1, f2, f3}

Procedure (P)
P= {create_grp, sent_req, accept_req, revoke_user}

Input(I)=Create group(Owner):
Procedure(P1):
This is the first step i.e. to perform a group in the cloud.
Owner=Create_grp(User)
Where,
Owner=Group Owner
User=Group user.
Output(O1):Group is created.

Input(I2) = Send_req(User)
Procedure(P2):

User send request to the owner to become a part of the group and user can easily share data between group.
User needs to provide details like group name in which he wants to take membership.
User needs to give the time duration in days, how much days user wants to be a member of group.

User=Send_req(Owner)
Output(O2): User is the member of group with the duration. User can upload file and request to TPA for auditing.

After creating the group user perform below operations on uploaded file.

S2= {I, P, O}
Input:
F = {f1, f2,…..,fn}
Procedure (P)
P={ uploadf, proxyup,verfpp,Ac,Af+reg_s, usr_{req} }

Input(I1): Upload file(uploadf):
Procedure (P1):
In this step first user select file to upload on cloud so input to this step is plaintext file is select for uploading procedure and converted to encrypted format and upload on cloud.
F=F(encr)->E_F
Where,
encr=encryption.
E_F=Encrypted File.
Output (O1): Output of this process is file in encrypted format.

Input 2:proxyup(p_{up})
Procedure (P2):In this step copy of file upload on cloud are store on server (proxy) to generate file on request.
Pr= E_F (p_{up})
Wher
pr =proxy.
E_F=Encrypted files.
Output (O2):All files copied to server.

Input (I3) Public parameter(PP):
Procedure (p3):[verfpp]
In this step data owner sends public parameter to third party auditor for verification of files on cloud.
Do(pp)->TPA
Do=Data Owner.
pp=public parameter.
TPA=Third part auditor.
Output(03):
Verification request is send to TPA by data owner.

Input(I4): Auditing challenge(Ac)
Procedure(P4):
In this step TPA send auditing challenge to cloud with parameter of owner file.
TPA_c =audit(pp)->cloud.
audit(pp)=auditing challenge
Output(o4): Auditing challenge is send to cloud for file verification.

Input(I5):Auditing proof and regenerate if file corrupt (Af+reg_s)
Procedure(p5):
In this step cloud gives verification proof to Third party auditor.
$cloud_{(prof)}$->TPA=reg_s(E_F) if file courrept.
Where,
reg_s=regenerate from server(proxy)
Output(o5):cloud gives verification proof and regenerate file from server if file is corrupt.
Input(I6): User rerequest to join group.(usr_{req})
Procedure(P6):
In this step user who send revoke can send request to join group again.
U_{revoke}=req_{join}->grp

@IJAERD-2017, All rights Reserved

Where,
U_{revok}=Revoked User.
Req_{join}=Request to join group.
Output (O6): User request for join group.
Output (O) - Finally, the security and experimental analysis show that, compared with its relevant schemes .this scheme is also secure and efficient

VII. RESULT

Result analysis is grounded on the size of file uploaded by user and also the revoked users in group.
In general, this scheme can achieve secure key distribution access control and secure user revocation.
The computation cost for members in this scheme is irrelevant to the number of revoked users.
System listed the comparison on computation cost of member for file upload having different size. It differs in encryption and decryption time as per the file size uploaded by each user. It also consider auditing time and also regeneration file if original file is corrupted.
The calculation cost of members for downloading the file with size of files in KB(like50,100 etc) is given in below Table I and graphically represent in Fig.2 and Fig. 3 (Graph of File Size with Time)

Security performance:

In general our scheme can achieve secret key distribution, fine access control and sure user revocation.
For clearly, seeing the advantages of security of proposed system are listed the below with respect to given factors.

Access Control	Secure user revocation	Anti-collusion attack	Data confidentially
Yes	Yes	Yes	Yes

Table 1: Security performance factors

Performance evaluation of the original file i.e. when group user send for the file auditing request and it confirmed that after third party auditor's evaluation file is not hacked.

File Size	Upload Time	Download Time
10 KB	0.4	0.3
50 KB	1.4	1.3
100 KB	2.7	2.5
200 KB	5.4	5

Table 2.Performance of file size in KB with time

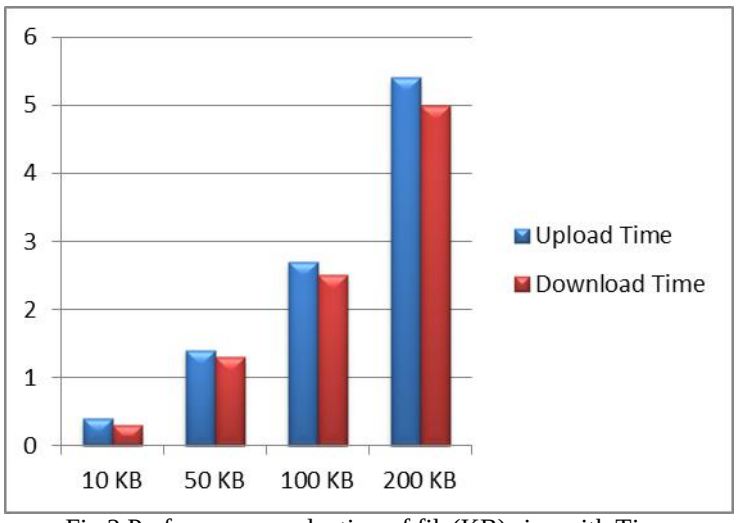


Fig 2.Preformance evaluation of file(KB) size with Time

@IJAERD-2017, All rights Reserved

File Size	Upload Time	Download Time
10 MB	0.8	0.7
50 MB	2.8	2.5
100 MB	4.0	3.7
200 MB	7.0	6.4

Table 3. Performance of file size in MB with time

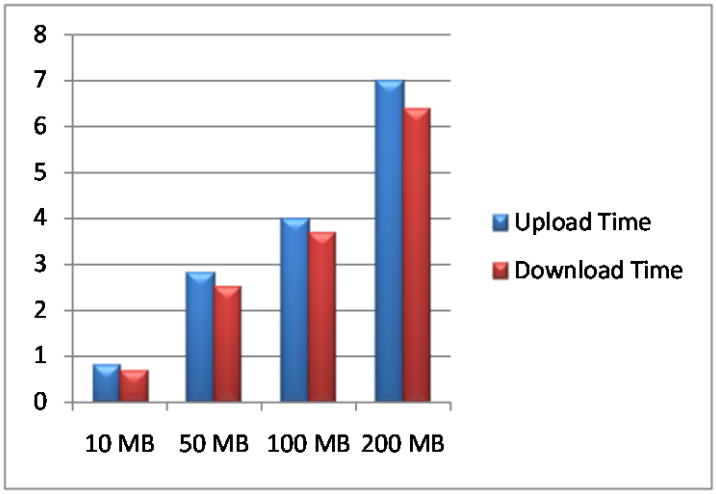


Fig 3.Preformance evaluation of file (MB) size with Time

Performance evaluation of the hacked file with compare to original file. That after auditing user wants to regenerate the file which is hacked.

File Size	Upload Time (Original File)	Download Time (Original File)	Download Time (Hacked File)
10 KB	0.4	0.3	0.5
50 KB	1.4	1.3	1.7
100 KB	2.7	2.5	3.0
200 KB	5.4	5	5.4

Table 4. Performance of regenerated file size in KB with time

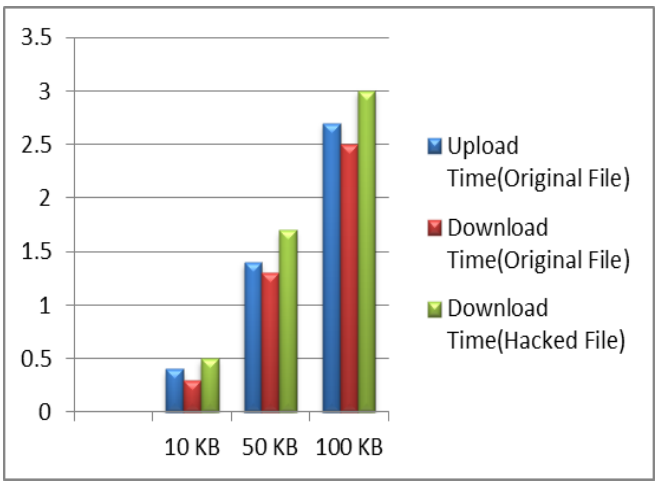


Fig 4.Preformance evaluation of regenerated file(KB) size with Time

@IJAERD-2017, All rights Reserved

File Size	Upload Time (Original File)	Download Time (Original File)	Download Time (Hacked File)
10 MB	0.8	0.7	1.1
50 MB	2.8	2.5	3.2
100 MB	4.0	3.7	4.3
200 MB	7.0	6.4	7.5

Table 5. Performance of file size in MB with time

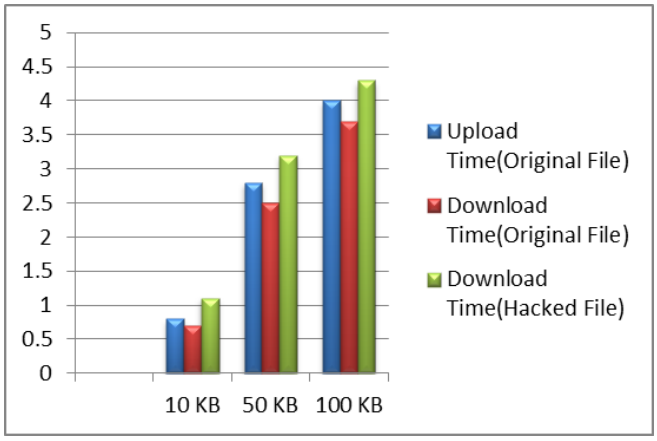


Fig 5.Preformance evaluation of regenerated file(MB) size with Time

VIII. CONCLUSION

Implementation of system to verify integrity of files on cloud of cluster of user and managing cluster of user with user adding in cluster and user take away from cluster with timestamp related to user. In this paper, design a secure anti-collusion information sharing scheme for groups in cloud, in this scheme group end users can securely get key from information owner and can upload files on cloud in encrypted format using AES Algorithm. Also information owner can send uploaded files verification request to third party auditor for verification. If file is hacked or corrupt then file will regenerate from server. Scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, and single user join the more than one group, group member extends the group last date and Also revoked user can re-reregister in group of cloud.

REFERENCES

[1]Zhongma Zhu and Rui Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud" VOL. 27, NO. 1, JANUARY 2016

[2] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

[4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp, 2005, pp. 29–43.

[5] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[7] Z. Zhu, Z. Jiang, and R. Jiang, "The attack on mona: Secure multi owner data sharing for dynamic groups in the cloud", in Proc. Int. Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185189

@IJAERD-2017, All rights Reserved

[8] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.
[9] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 2602–2614, Nov. 2013.
[10] X. Zou, Y.-S. Dai, and E. Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," in Proc. IEEE Conf. Comput. Commun., 2008, pp. 1211–1219.
[11] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.
[12] B. Dan and F. Matt, "Identity-based encryption from the weil pairing," in Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol., 2001,vol. 2139, pp. 213–229.
[13]Arti Arun Mohanpurkar, Madhuri Satish Joshi, "A Traitor Identification Technique for Numeric Relational Databases with Distortion Minimization and Collusion Avoidance" International Journal of Ambient Computing and Intelligence Volume 7, Issue 2 , July-December 2016

@IJAERD-2017, All rights Reserved