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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

An Efficient Approach to Usage of Cloud Storage by Sharing Multi-Owner Data in Cloud Computing

George Fernandez.I[1], Dr. A. Kumaravel*[2,]

Assistant Professor, Dept. of IT, Jerusalem College of Engineering, Chennai, Tamil Nadu, India[1]

Dean& HOD, Dept. of IT, Bharath University, Chennai, Tamil Nadu, India[2]

* Corresponding Author

ABSTRACT: Cloud Computing has added an advantage when compared to Grid computing and Cluster computing by providing an efficient and economical solution for sharing group resources among the cloud users. Preserving data and Maintaining privacy in an untrusted cloud is still a demanding issue. In this Paper we propose a secure Multi-Owner data sharing using the techniques such as dynamic broadcast encryption and group signature so that any cloud user can anonymously share data with others. A new revocation technique will be proposed in this paper. In our scheme a separate revocation list will be constructed by the group manager which helps to identify the revoked user. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

KEYWORDS: Cloud Computing, Data Sharing, Dynamic Groups, Revocation.

1. INTRODUCTION

The growth of internet access with high speed network for industrial, commercial and entertainment purpose comprised of thousands of concurrent ecommerce transaction in every day. To handle this demand to access high speed network it needs large scale data-center, thousands of servers, large infrastructure.[2] So many organizations such as Google, eBay, salesforce.com, HP, IBM, operating huge datacenter to whole world. Many organizations invest huge amount of capital, time, infrastructure, large datacenter. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application, A organization allows its workers in the same group to store and share files in the cloud.

By making use of cloud[2], the worker can be completely freed from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. The cloud service provider or third party may not fully trusted by the users. While the data files stored in the cloud may be sensitive and confidential. The basic solution is to encrypt the data and then upload the encrypted data into the cloud.

Designing am efficient and secure sharing scheme for groups in cloud is a difficult task due to the following reason:
First, privacy is the most significant obstacles for the wide deployment of cloud computing. On the other hand, unconditional identity privacy may incur the abuse of privacy. Second, it is highly recommended that any member in a group should be able to fully use the data storing and sharing services provided by the cloud, it is called as the multiple-owner manner. Finally, groups are generally dynamic in practice, e.g., new employee allocation and current employee revocation in a company. Third issue is that, the changes of membership make secure data sharing extremely difficult. Another challenging thing is that newly granted users to learn the content with the anonymous data owners, and obtain the corresponding decryption keys. Final challenging issue is that efficient membership revocation mechanism should be achieved without updating their secret keys of the remaining users and it is also desired to reduce the complexity of the key management.[3]

The draw backs of the existing system can be overcome using this proposed system[1]. The main contribution of this paper is that:The proposed system uses MONA. Any user in the group can store and share data files with others by the cloud. This schema is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. It provides the secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resources The real identities of data owners can be identified or revealed by the group manager when dispute occur. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. We demonstrate the efficiency of our schema in terms of storage and computation head by security analysis.[4]

2.1 Group Signature

Chaum and Van Heyst introduced the concept called group signature[6].In this paper we present a new type of signature for a group of person called a group signature which has the following properties:Any members of the group can sign messages. Keeps the identity secret from the verifiers.[5] Only the group manager can reveal the real identity, when the dispute occurs which is called as traceability.

2.2 Dynamic Broadcast Encryption

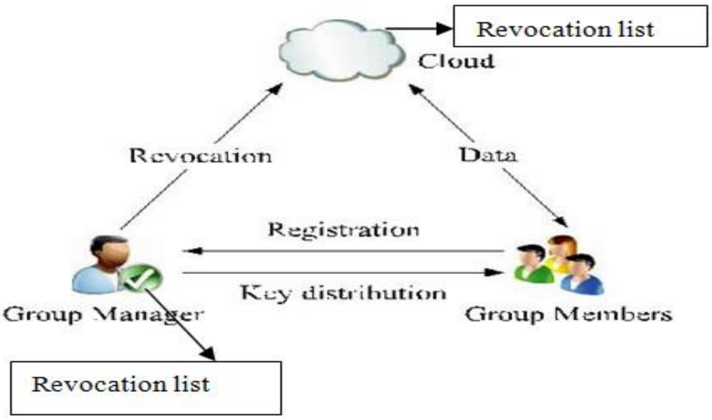
Broadcast encryption allows a user to distribute message securely to a set/group of users in an in secure environment [7] so that only a privileged subset of users can decrypt the data. Apart from this Dynamic broadcast encryption also allows the group manager to dynamically include new members while preserving previously computed information, i.e., user decryption keys need not be recomputed, the morphology and size of cipher texts are unchanged and the group encryption key requires no modification.[8] The first formal definition and construction of dynamic broadcast encryption are introduced based on the bilinear pairing technique, which will be used as the basis for file sharing in dynamic groups.[9]

2.3 Revocation List

It is list of the revoked users, who tries to attack the data The revoked list should be updated frequently [8]. The revocation list will be monitored by the group manager and even updates in the cloud, so that revoked user cannot access or share the data in the cloud.[10]

III. SYSTEM MODEL

The system model consists of different entities as illustrated in the below figure.[11]



- Data Owner(Group member)
- Cloud Server.
- Data Integrity.
- Group Manager.
- Data Consumer(End User / Group Member

Data Owner (Group Member)
In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud.[12] The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.[13]

Cloud Server
The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers.[14] To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.[15]

Data Integrity
Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.[16]

Group Manager
The Group Manager who is trusted to store verification parameters and offer public query services for these parameters. In our system the Trusted Third Party, view the user data and uploaded to the distributed cloud. In distributed cloud environment each cloud has user data. The Group Manager will perform the revocation and un revocation of the remote user if he is the attacker or malicious user over the cloud data.

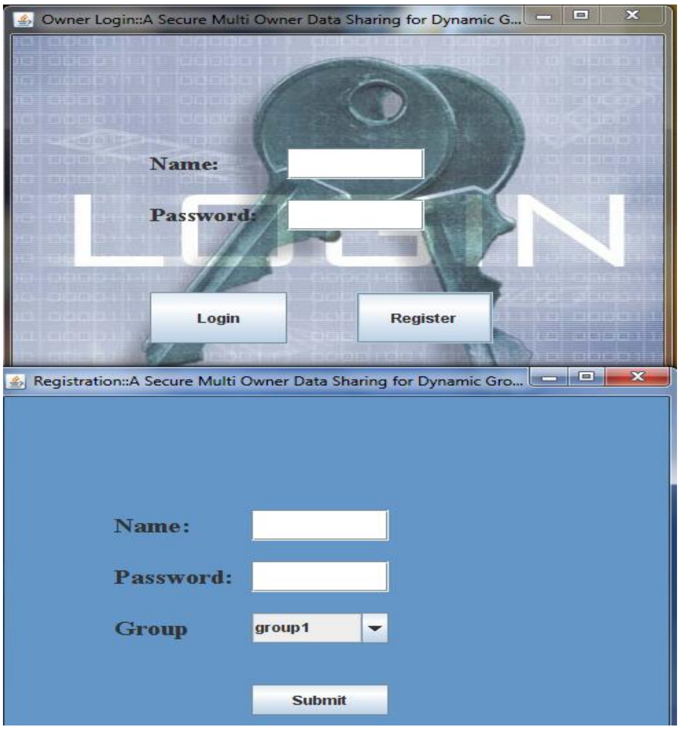
Data Consumer (End User / Group Member)
In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the GM authority and the Data user's are controlled by the GM Authority only. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges

IV. IMPLEMENTATION WORK

Group Member: Initially, if the member is new to the group, he has to get registered by entering the name and his password, and also he needs to select to which group he need to go. If he is already registered than he can Login as shown in the snap shot Once the user or the group member logins, a group signature will be generated, for each and every group different signature will be generated using a signature generation algorithm. Some of the task of the group member is that:

- Upload a file
- Download a file
- Delete a file
- Change the group

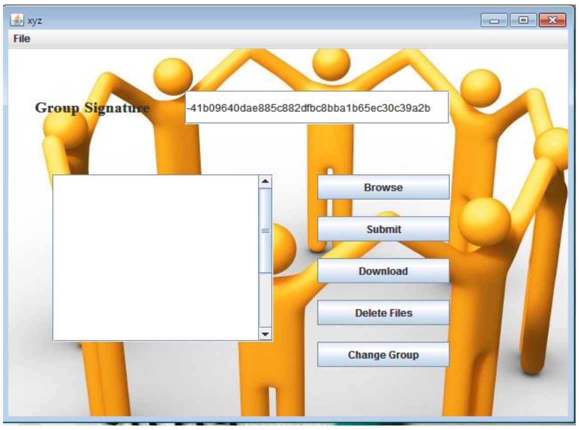
The uploaded file will be in the encrypted format , by using the dynamic broadcast encryption technique, the file upload can be accessed only by their group members .The uploaded file can be downloaded or decrypted by using a secret key, which will be generated for each and every file. The group member can delete the files of only which he is uploaded or of his own group file. He cannot delete the other group files. The group member as all the rights to change from one group to another, on request to group manager.


Owner Login::A Secure Multi Owner Data Sharing for Dynamic G...
Name:
Password:
LOGIN
Login
Register
Registration::A Secure Multi Owner Data Sharing for Dynamic Gro...
Name:
Password:
Group
Submit

Group: group1

Fig 1 member registration and login

As shown in the snap shot



Group Signature: -41b09640dae885c882dfbc8bba1b65ec30c39a2b

Fig 2 generation of group signature

Group manager:

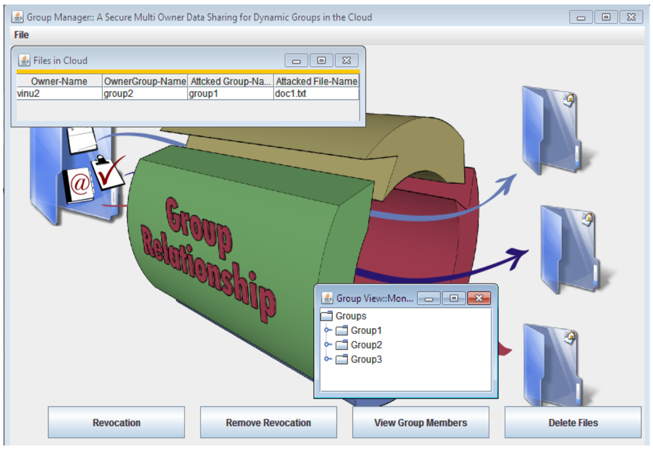
Group manager controls the overall operations of the group. All the details of the group and the files stored in the cloud will be available in the group manager.

Some of the task performed by the group manager is that:

- Revocation
- Remove revocation
- Group member details
- Delete files

As shown in the snapshot

10.15680/ijircce.2015.0304229



Group Manager:: A Secure Multi Owner Data Sharing for Dynamic Groups in the Cloud

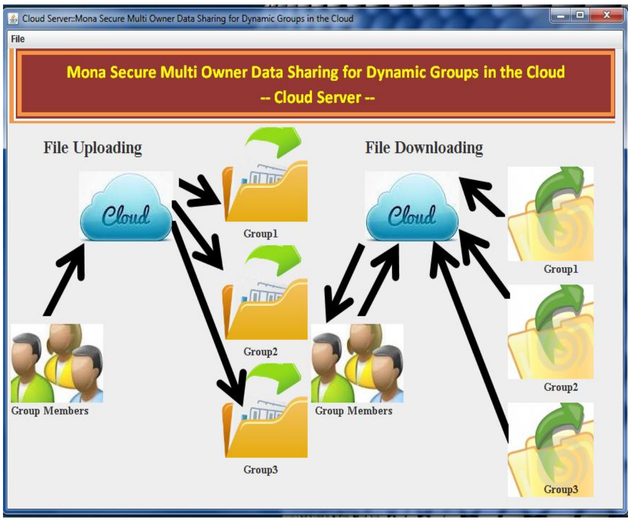
Files in Cloud

Owner-Name	OwnerGroup-Name	Attcked Group-Na...	Attacked File-Name
vinu2	group2	group1	doc1.txt

Fig 3 group manager

Revocation can be achieved by the group manager, if group members of one group is trying to access the file of the another group then he needs to be revoked, a blocked list will be maintained by the group manager, based on that user can be revoked. Revocation can be removed, if the revoked user request for the group manger. Once the user has been revoked, he would not be able to upload or download the file, even from his own group.Group member details such as , how many groups are there, the group members name will be present.Finally he can delete all the files of the groups.

Cloud server:



Cloud Server::Mona Secure Multi Owner Data Sharing for Dynamic Groups in the Cloud

Mona Secure Multi Owner Data Sharing for Dynamic Groups in the Cloud
-- Cloud Server --

Fig 4 cloud server

The file can be uploaded into the cloud server by the group members, the cloud server just acts as storage. The files stored in the cloud will be in the encrypted format. The files can be downloaded from the cloud server by only the valid group members.

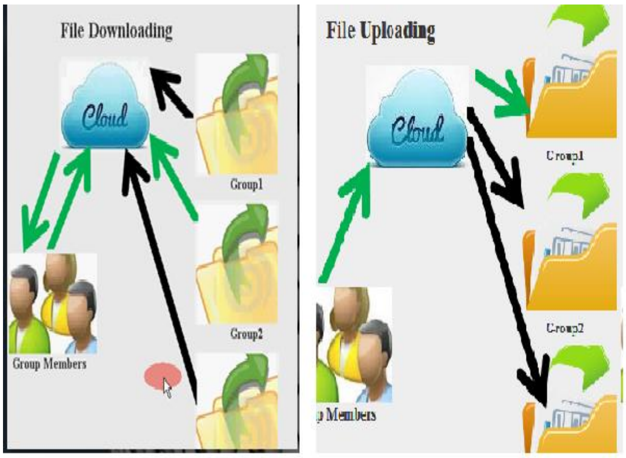


Fig.5 file uploading and downloading

If the group member of one group is trying to access the files of the other groups, he will be revoked by the group manager. Once he has been revoked he will not be able to upload or download any file from the cloud, this can be shown through the snapshot:

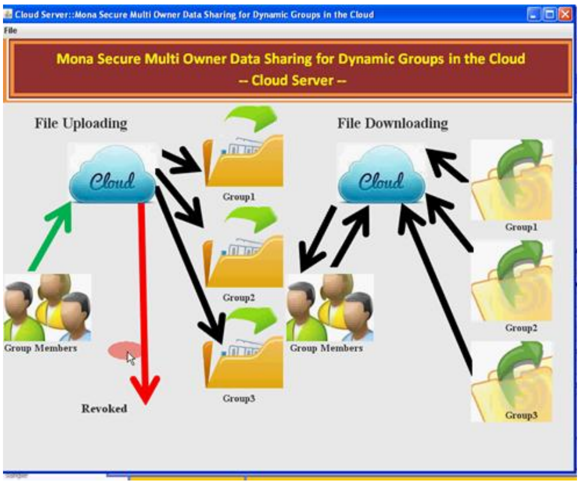
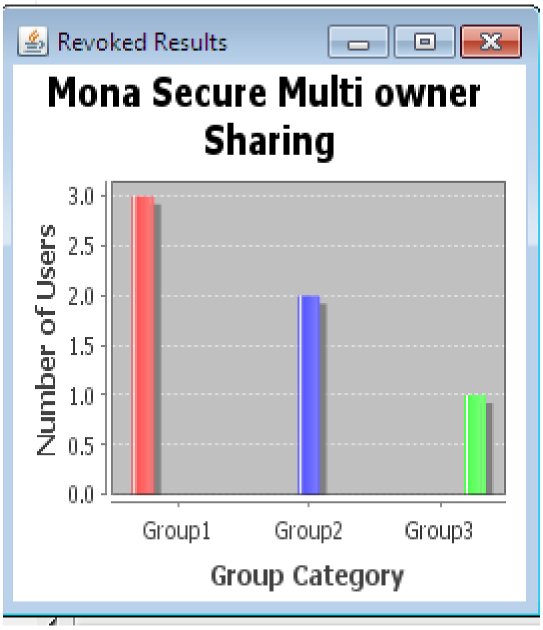

Cloud Server::Mona Secure Multi Owner Data Sharing for Dynamic Groups in the Cloud
File
Mona Secure Multi Owner Data Sharing for Dynamic Groups in the Cloud
-- Cloud Server --
File Uploading
Cloud
Group1
Group2
Group3
Group Members
Revoked
File Downloading
Cloud
Group Members
Group1
Group2
Group3

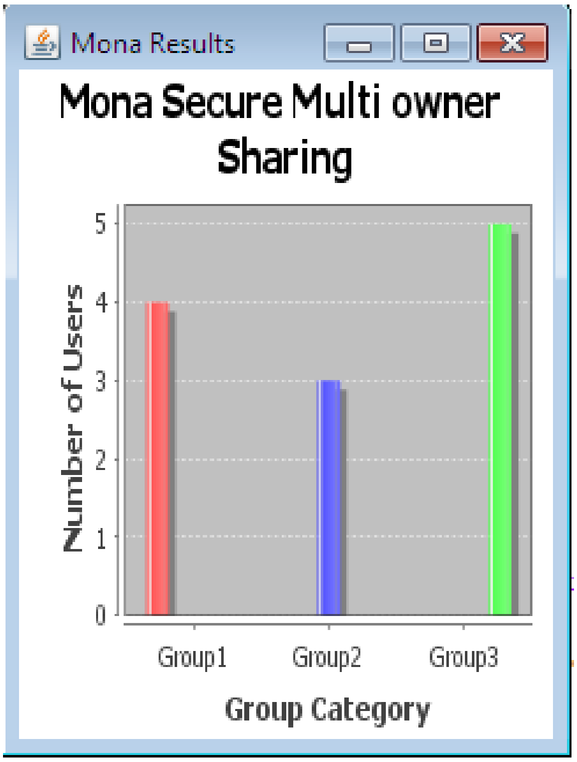
Fig.6 revocation

V. RESULTS DISCUSSION

The below graph represents the number of revoked users present in each and every group, the revoked user in the group1 are represented in red. The revoked users in the group2 are represented in blue whereas the revoked users in group3 are represented in green as seen in the graph. The numbers of revoked users in group1 are more when compared to the group 2 and group3.



The below represented graph represents the number of users present in each and every group, the user in the group1 are represented in red. The users in the group2 are represented in blue whereas the users in group3 are represented in green as seen in the graph. The numbers of users in group3 are more when compared to the group1 and group2.



VI. CONCLUSION

In this paper design a secure data sharing scheme and achieves the revocation using the revocation list for dynamic groups in an untrusted cloud .A user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, it supports efficient user revocation and a new user joining More specially, user revocation can be achieved through a public revocation list without updating the private keys of the remaining users , and the new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

REFERENCES

1. X. Liu, Y. Zhang, B. Wang and J. Yan, “Mona: Secure Multi-Owner Data Sharing for Dynamic Group in the Cloud,” IEEE Tran. On Parallel and Distributed System,vol. 24, no. 6 June 2013.
2. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph R.H Katz,A. Konwinski, G. Lee, A.D Patterson, A. Rabkin, I Stoica, and M. Zaharia “ A View of Cloud Computing,” comm.ACM vol. 53, no. 4, pp. 50-58, April 2010
3. Sree Latha R., Vijayaraj R., Azhagiya Singam E.R., Chitra K., Subramanian V., "3D-QSAR and Docking Studies on the HEPT Derivatives of HIV-1 Reverse Transcriptase", Chemical Biology and Drug Design, ISSN : 1747-0285, 78(3) (2011) pp.418-426.
4. S. Yu, C. Wang, K. Ren, and W. Lou “Achieving Secure Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM, pp. 534-542, 2010
5. S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” proc. Int’l Conf. Financial Cryptography and Data Security (FC), pp. 136 149, Jan. 2010
6. Masthan K.M.K., Aravindha Babu N., Dash K.C., Elumalai M., "Advanced diagnostic aids in oral cancer", Asian Pacific Journal of Cancer Prevention, ISSN: 1513-7368, 13(8) (2012) pp.3573-3576.
7. M. Kallahalla, E. Riedel, R. Swaminathan, Q Wang, and K. Fu, “Plutus: Scalable Secure File Sharing on Untrusted Storage,” proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003
8. D. Chaum and E. van Heyst, “Group Signatures,” Proc Int’l Conf.Theory and Applications of Cryptographic Technique (EUROCRYPT),p p. 257-265, 1991
9. Tamilselvi N., Dhamotharan R., Krishnamoorthy P., Shivakumar, "Anatomical studies of Indigofera aspalathoides Vahl (Fabaceae)", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384 , 3(2) (2011) pp.738-746.
    A. Fiat and M. Naor, “Broadcast Encryption,” Proc. Int Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993
10. D. Naor, M. Naor, and J.B. Lotspiech, “Revocation and Tracing schemes for Stateless Receivers,” Proc. Ann. Int’l Cryptology (CRYPTO), pp. 41-62, 2001
11. Devi M., Jeyanthi Rebecca L., Sumathy S., "Bactericidal activity of the lactic acid bacteria Lactobacillus delbreukii", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384 , 5(2) (2013) pp.176-180.
12. B. Wang, B. Li, and H. Li, “Knox: Privacy Preserving Auditing for Shared Data with Large Groups in the Cloud Proc. 10th Int Conf. Applied Cryptography and Network
13. B. Waters, “Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,” proc. Int’l Conf Pratice and Theory in Public Key Cryptography Conf. Public Key Cryptography pdf.2008
14. G. Ateninese, K. Fu, M. Green, and S. Hohenberher Improved Proxy Re-Encryption Schemes with Applications to Secure distributed Storage,”.
15. Reddy Seshadri V., Suchitra M.M., Reddy Y.M., Reddy Prabhakar E., "Beneficial and detrimental actions of free radicals: A review", Journal of Global Pharma Technology, ISSN : 0975-8542, 2(5) (2010) pp.3-11.
16. B Karthik, TVUK Kumar, A Selvaraj, Test Data Compression Architecture for Lowpower VLSI Testing, World Applied Sciences Journal 29 (8), PP 1035-1038, 2014.
17. 17.M.Sundararajan .Lakshmi,”Biometric Security system using Face Recognition”, Publication of International Journal of Pattern Recognition and Research. July 2009 pp. 125-134.
18. 18.M.Sundararajan,” Optical Sensor Based Instrumentation for correlative analysis of Human ECG and Breathing Signal”, Publication of International Journal of Electronics Engineering Research, Research India Publication, Volume 1 Number 4(2009). Pp 287-298.
19. 19.C.Lakshmi & Dr.M.Sundararajan**, “**The Chernoff Criterion Based Common Vector Method: A Novel Quadratic Subspace Classifier for Face Recognition**”** Indian Research Review, Vol.1, No.1, Dec, 2009.
20. 20.M.Sundararajan & P.Manikandan,” Discrete wavelet features extractions for Iris recognition based biometric Security”, Publication of International Journal of Electronics Engineering Research, Research India Publication, Volume 2 Number 2(2010).pp. 237-241.
21. 21.M.Sundararajan, C.Lakshmi & .M.Ponnavaikko, “Improved kernel common vector method for face recognition varying in background conditions”, proceeding of Springer – LNCS 6026- pp.175-186 (2010).ISSN 0302-9743**.(Ref. Jor – Anne-II)**