iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** V **Month of publication:** May 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Effective User Revocation and Anti - Collusion System for Dynamic Groups in Cloud

K. Vijayakumar[1], N. Divya Sri[2], M. Vijayashree[3]
[1]Associate Professor, [2,3]Computer Science and Engineering
St. Joseph's Institute of Technology, Chennai, India

Abstract— The objective of the project is to develop a simple and effective collusion resistant dynamic group model for cloud. The workloads in cloud often contain sensitive information. The major problem in public clouds is to securely share the data in dynamic groups while also conserving data and uniqueness. This is because, revocated users from the group should not able to access the original data as well as the data being shared in the group. This problem is called collusion attack. The existing systems use few encryption techniques such as ECC to prevent the collusion attacks but when implementing such a system, the drawback is actually in choosing which curve or family of curves to deal with, because every application will have diverse requirements and also no elliptic curve can be optimal for every other application thus making the ECC algorithm complex and difficult to the core. Hence we present a new secret sharing scheme which is comparatively simpler, efficient and easier to implement. This scheme has an efficient membership re-vocation method by avoiding the overhead of updating the secret keys of the users every time thus minimizing the complexity of key management, and also the computational cost.
Keywords— Cloud computing; dynamic groups; encryption; user revocation; secret sharing; blowfish algorithm;

I. INTRODUCTION

Cloud computing is a computing model, where a pool of workstations or computers are inter connected in private, public or hybrid networks, to provide dynamically accessible setup for data storage. With the dawn of cloud computing, the cost for hosting, storage, computation has reduced significantly. The sole goal of this technology is to reuse the IT capabilities and to put them to efficient and worthy usage. Data storage is the most basic and widely used service offered by the cloud. In order to preserve data privacy, the files are encrypted even before storing into the cloud. There exists many dynamic groups in the cloud where user members share data accordingly with each other. This scenario is seen in many organizations wherein the employees step into the shoes of group members. However, scheming an efficient data sharing system for dynamic groups in the cloud has few challenges. First issue is that it should support multiple data owner manner which means that any member in a group should be able to practice data storing as well as data sharing services in cloud. Another downside is that, groups are typically dynamic in practice. Thus the user management and associated data management is very challenging. Hence to resolve these challenges, we propose a secret key sharing scheme and our contribution includes:

A user is added to the group by group admin and is given a secret key.

Any user in the group can securely share their data with others. The public file sharing helps the users to share the file with all the members in the group.

The private file sharing helps the users to share the file with selected members of the group.

The proposed scheme also supports dynamic groups efficiently. The newly joined users can also decrypt the files.

User revocation also easily achieved. There is no need to update the secret keys of the remaining users. Once the user is revocated from the group, he will not be able to access any file shared in the group even if he conspires with other untrusted cloud servers.

II. RELATED WORK

M. Ali et al. a cloud storage security scheme for group data named the SeDaSC methodology. This methodology delivers forward and backward access control, secure data sharing without reencryption, access control for malicious insiders, and. Also, it provides assured deletion as it deletes the details required to decrypt a file. However, the response of this method with varying key sizes seems to a downside and has to evaluated [3].

Zhou et al. proposed a secure access control scheme for encrypted data in cloud using a role based encryption technique. According to Zhou et al. the scheme is said to achieve well organized user revocation by combining role based access control policies with encryption to protect huge data storage in the cloud. However, the authentications between entities are not taken into consideration,

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

and hence, the scheme is prone to attacks such as collusion attack which can disclose sensitive data files [15].

Ning Shang et al. proposed a new scheme for choosy dissemination of content that claims to preserve the privacy of the users to whom the data files are sent and is based on a group key management scheme. This method is privacy preserving which means that the users are given access to file based on the policies given by the data owner. However, there is this scalability and optimization problems. Thus, further a proper criteria for grouping subscribers depending on different requirements of broadcasting has to be developed. The performance of the system is also affected due to the matrix. Thus the optimization of the matrix should also be considered [16].

Zhongma Zhu et al. found that there exists collusion attack on Liu et al.'s protocols. Due to the presence of the collusion attack, the secure data access control has not been achieved and the sharing of data has not been taken into consideration and therefore poorly protected. Also, another security loophole existing user registration phase because of the unsecure communication channels. Thus the private key has to be securely given to users in this channel. This can also lead to unveiling the secret data of the users. Thus, the scheme will easily suffer from the collusion attack by the revoked user and the cloud. The revoked user will be able to use his private key to get the secret data and will also be able to decrypt it after his revocation by conspiring with the cloud [17].

Kallahalla et al. came up with a scheme named Plutus. It makes novel use of cryptographic functions to provide security. Plutus divides the files into chunks called filegroups and encrypts every filegroup with the help of unique block key, the data owner will be able to share the filegroups with others through providing the equivalent lockbox key. The lockbox key is used to encrypt the file-block keys. However, the file block keys requires to be updated and disseminated for a user revocation or also a new user addition, therefore, the system has a heavy key distribution overhead [25].

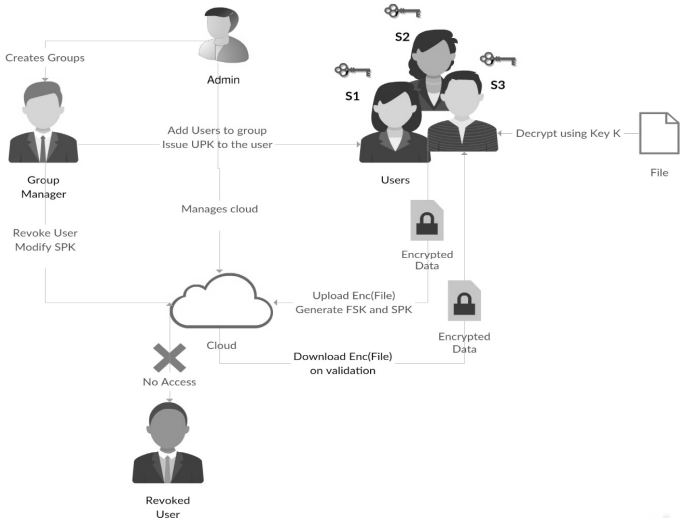
III. SYSTEM ARCHITECTURE

A. *Abbreviations And Acronyms*

IP - Internet protocol
ECC - Elliptic Curve Cryptography
FSK - File Secret Key
UPK - User Private Key
SPK - Shared Private Key

B. *Overview*

The overall system architecture consists of group manager, group members, an administrator, and cloud. The cloud is the cloud service provider (CSP) like amazon, Microsoft etc. The cloud is the place where the members upload and store data. The admin is the person who manages the overall system. Administrator will be able to view all the groups present and all users. Within a group, the members are allowed the share the data files in two different modes viz., private and public.



During the creation of group, a user private key is given to the members being added to the group. When a file is uploaded by the data owner in the group in public mode, anyone in the group will be able to download and decrypt the encrypted file. If a file is

uploaded privately, then the file is accessed only ny specific people. The authentication is checked using the shared private key generated every time a private file is uploaded. The verification with shared private key is done by the group manager.

Adding User to Group: A group admin is created by the Admin and controls the overall architecture of this model. A group admin is capable of creating secure groups by adding trusted members to the group. When a user is added to the group all the user details are collected and the user is provided with the UPK. The key thus generated is stored in the database after encryption to improve reliability.

Public File Upload / Download: A group user can share the files publicly as well as privately. The public file sharing helps the users to share the file with all the members of the group. Any other user of the group can download the file uploaded publicly. To ensure security from the non-group users, the file is encrypted and then stored in the cloud. The file upload process is done using the multi part file upload scheme. The owner and the file details are stored in the database.

Private File Upload / Download: User of the group is given the choice of sharing the file with selected members of the group. The user provides the email of the selected users and share them the file. In this process, a SPK is generated. This SPK is generated with the help of the UPK's of the users to whom the file is shared and then encrypted before storing it to the database. Whenever any other user tries to download the file, he will not be given access.

Revoke User: A user is revoked from the group by the group admin. Once the user is revocated he will not be able to access any file from the cloud even if he conspires with other untrusted cloud. The database is modified by deleting all the user information. The SPKs of all the files are modified. The user will not be able to login to the application. System eliminates complex solutions and considers modifying a single key modification at the time of user revocation. This key need not be distributed among the users or to be recomputed as a whole. Thus this process is computationally very efficient compared to previous processes.

C. Algorithm

UserPrivateKey_Gen(): A UPK(User Private Key) is generated when the user is registered to a group. This key is unique for each user and is based on the three parameters.

$$UPK = a + b + c \quad (1)$$

where,

a - Substring of one of the user credentials.

b - A random PIN.

c - Substring of the Email of the user.

File_Upload(): Files are uploaded by the users of the group. During the file upload, a FSK (File Secret Key) is generated. This FSK is used to maintain the uniqueness of the file and provide more security by making the files private.

$$FSK = \alpha + \beta + \gamma \quad (2)$$

where,

α - A random character from the provided filename.

β - A random number.

γ - A random character from the provided filename.

Private_Upload(): For the purpose of uploading the files privately, the user can select the visibility of the file. An SPK is generated, which checks the authorization of the user.

$$FSK = g(UPK[n]) \quad (3)$$

where,

g(a[n]) - A function which does the concatenation of the

elements of the array

a[] - An array of user private private keys.

n - The number of users to whom the file is shared.

File_Encrypt(): A file is encrypted before storing it in cloud. Blowfish algorithm is used to encrypt the files [3]. No user or any other person cannot access the file without proper authorization.

Revoke_User(): An untrusted user can be revoked by the group admin. The user details are removed from the database in this method. And, the shared private key of the files are modified by removing the keys of the revoked users.
We have used a symmetric encryption technique called blowfish algorithm.

- Divide x into two 32-bit halves: xL, xR
- For i = 1 to 16:
- xL = XL XOR Pi
- xR = F(XL) XOR xR
- Swap XL and xR
- Swap XL and xR (Undo the last swap)
- xR = xR XOR P17
- xL = xL XOR P18
- Recombine xL and Xr

where,

x - The data to be encrypted.

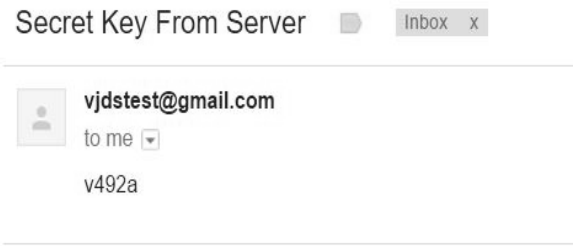
xL - Left part of the data.

xR - Right part of the data.

The function in the algorithm iterates 16 times of the network. Every round will consist a permutation dependent on a key and a substitution that is a key and data dependent. The operations in this algorithm are XORs and additions on 32 bit words. It also includes few additional operations for every round that are four indexed array data lookup tables. This block cipher algorithm encrypts a block data of 64 bits at once. It obeys the feistel network [3].

IV. IMPLEMENTATION AND RESULTS

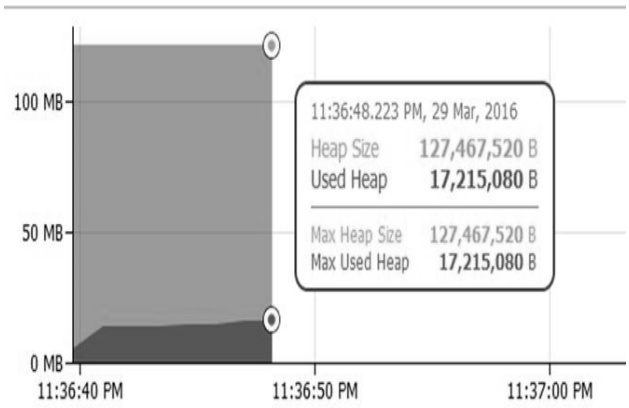
The file upload page of the application allows the user to browse a file from their personal computers and upload it to the cloud. For a private upload of the file the user can specify the Share With details. The download page helps the users to download the files uploaded by other users of the group. The select input box will also prompt the users with the file names that are uploaded to the server.



When a user requests for the download of the private file, the server verifies whether the current user is eligible to access the file or

not by authorizing the shared private key, and if he is eligible then the secret key of the file is sent to the user's mail id from the server mail id. This secret will only takes the user to the next step of downloading the private file. If the user enters a valid file secret key, which is checked with the database table file details against the column secret, then the user will be redirected to the validation page. In the validation page, the verification process will be done. The next step is File Download, the user will be given the details of the file and on clicking the download button, and the file is downloaded after being decrypted. For the public and low priority files, the user will be immediately redirected to the last page with the secret verification process.

A. Memory Usage



The heap is memory fixed separately for dynamic allocation. Unlike the stack, there is no prescribed pattern to the allocation and deallocation of blocks from the heap. One can allocate a block at any time also cannot free it at any time. The memory heap graph shows a flat usage of memory which means that:

There are very few short lived objects in the memory,

Very less garbage collection happening and

There are no memory leaks in the program.

V. CONCLUSION AND FUTURE WORK

The paper proposes a novel system called to provide efficient management of dynamic groups and elimination of collusion attacks on the data in cloud. System uses a method called the Shared Private Key Method to avoid collusion. This method allows us to modify the key without creating a overhead. Experimental results show that the method can generate much better protection than traditional methods. This method reduces the computational complexity compared to the Elliptic Encryption Method. The method also reduces the manual work and performs automatic computations without much involvement of the users. In the future, system will consider more efficient method to provide even better secrecy in sharing files to the users. System might also try to eliminate the redundancy in sharing the files in the cloud to preserve the memory and time. Furthermore, the system considers the deletion of the users from the group. Additionally the system may also consider revocation of the groups as a whole in the future by using information from other relevant papers and the citations. We can also modify this system to support dynamic wireless groups such as MANET. System may consider this issue in the future.

REFERENCES

[1] Shao Ying Zhu, Richard Hill, Marcello Trovati (2016), “Guide to Security Assurance for Cloud Computing”, Springer Publishing.

[2] Jonathan Katz, Yehuda Lindell (2015), “Introduction to modern cryptography” , CRC Press.

[3] B. Schneier “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)”, Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.

[4] M.Ali, R.Damodaran, E.Khan (2015). “SeDaSC: Secure Data Sharing in Clouds”, IEEE systems journal.

[5] U.Gupta (2015), “Survey on security issues in file management in cloud computing environment”, http://arxiv.org/abs/1505.00729

[6] Sushil Jadojia, Krishna Kant (2014), “Secure Cloud Computing”, Springer Publication.

[7] L. Wei, H. Zhu, Z. Cao, Y. Chen, and A. V. Vasilakos (2014), "Security and privacyfor storage and computation in cloud computing", Inf. Sci.

[8] M.Malarvizhi, J.A.J.Sujana,T.Revathi (2014), "Secure File Sharing Using Cryptographic Techniques in Cloud", IEEE.

[9] KaipingXue, Peilin Hong (2014), "A Dynamic Secure Group Sharing Framework in Public Cloud Computing", IEEE.

[10] P.Varalakshmi, A.R.Shajina (2014), "A Framework For Secure Cryptographic Key Management Systems", IEEE.

[11] A. Abbas and S. U. Khan (2014), "A review on the State-of-the-art privacy preserving approaches in e-health clouds," IEEE.

[12] A. N. Khan, M. M. Kiah, S. A. Madani, M. Ali, and S. Shamshir-band (2014),"Incremental proxy re-encryption scheme for mobile cloud computingenvironment," J. Supercomput.

[13] Hugo Krawczyk (2014), "Public-Key Cryptography - PKC 2014", Springer.

[14] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, Xuemin Sherman Shen (2013), "Secure provenance: the essential of bread and butter of data forensics in cloud computing", Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security.

[15] X. Liu, Y. Zhang, B. Wang, and J. Yang (2013), "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst.

[16] L. Zhou, V. Varadharajan, and M. Hitchens (2013), "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Security

[17] M Nabeel, N Shang, E Bertino (2013), "Privacy preserving policy-based content sharing in public clouds", Knowledge and Data Engineering, IEEE Transactions.

[18] Z. Zhu, Z. Jiang, and R. Jiang (2013), "The attack on mona: Secure multiowner data sharing for dynamic groups in the cloud," in Proc. Int. Conf. Inf. Sci. Cloud Comput.

[19] DinkarSitaram, GeethaManjunath (2012), "Moving to the cloud, Developing Apps in the new world of computing", Syngress Publishing.

[20] D. H. Tran, H.-L. Nguyen, W. Zha, and W. K. Ng (2011), "Towards securityin sharing data on cloud-based social networks," in Proc. 8th Int. Conf. Inf., Commun. Signal Process.

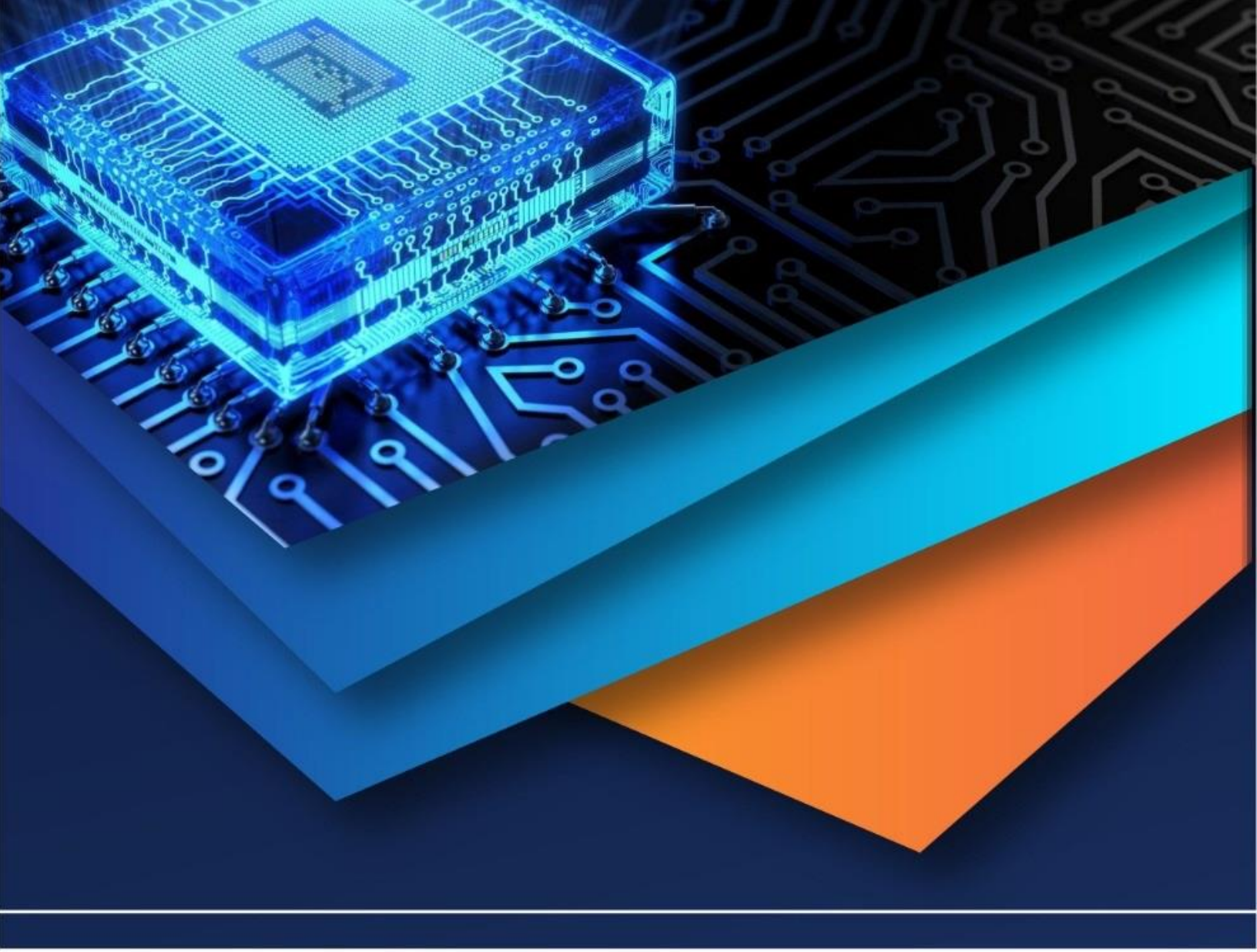
[21] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno(2010), "Cryptography Engineering: Design Principles and Practical", Wiley Publishing.

[22] Gautam Shroff (2010), "Enterprise Cloud Computing: Technology, Architecture, Applications", Cambridge University Press.

[23] BorkoFurht, Armando Escalante (2010), "Handbook of Cloud Computing", Springer Publishing.

[24] Barrie Sosinsky (2011), "Cloud Computing Bible", Wiley Publishing.

[25] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu (2003), "Plutus: Scalable secure file sharing on untrusted storage," Proc. USENIX Conf. File Storage Technol.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY