iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8336

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Encryption & Fingerprint Based Security in Cloud Computing

Ruchi[1], Ms. Kompal Ahuja[2]
Department of Computer Science, Delhi Institute of Technology and Management (DITM), (DCRUST), Sonepat

Abstract*— A cloud user can utilize different computing resources such as storage, application etc. By using cloud-based solutions, companies do not need to have their own hard ware infrastructure to host their application. Thereby the organization or company need not to invest huge amount on the infrastructure. Cloud computing can be considered as a service provided by a service provider. The user is only concerned that the service is available whenever the user needs this service. The main concern on cloud computing is that of security. Because our data and other applications reside on the cloud server. Therefore we must concern about the security of our personal data. There are different security mechanisms available in literature. But none of the methods are full poof method. In this paper, we propose a new security mechanism based on biometric fingerprint and cryptography for security of clients data on the cloud environment.

***Keywords*— Cloud computing Security, Blowfish Algorithm, Cryptography**

I. INTRODUCTION

Cloud computing [1] can be considered as a service provided by a service provider. The user need not take care how these services are obtained. Instead, the user is only concerned that the service is available whenever the user needs this service.

Cloud computing is a growing area of concern in the IT security community because cloud architectures are literally popping up all over [2]. Public clouds are available from Google, Amazon, Microsoft, Oracle, Eucalyptus, and many other vendors. The basic concerned with cloud computing is about security. here are different security mechanisms available in literature. But none of the methods are full poof method. Although they have tried to minimize security risk as much as possible, cloud computing still possesses many security risks. Some of these security risks are well known and some of them are new. Confidentiality, integrity, and availability are the three key aspects of security [3]. Ensuring confidentiality means that no one can read our data unless we want them to read it, integrity ensures that no one can modify our data without the modifications being detected, and availability means that we can access our data at any time. Cloud computing also needs to deal with security risk/threats just as any other service. In this work a security solution for data storage in cloud computing is examined. The solution encompasses confidentiality and integrity of the stored data, as well as a secure data sharing mechanism in the cloud storage systems. In this paper, we propose a new security mechanism based on biometric fingerprint and cryptography for security of clients data on the cloud environment.

II. SECURITY ISSUES FACED BY CLOUD COMPUTING

Cloud allows users to achieve the power of computing which beats their own physical domain. Different issue related to security in cloud environment are explained below [4][5].

A. Data Access Control

Sometimes confidential data can be illegally accessed due to lack of secured data access control. Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Data exists for a long time in a cloud, the higher the risk of unauthorized access.

B. Data Integrity

Data integrity comprises the following cases, when some human errors occur when data is entered. Errors may occur when data is transmitted from one computer to another otherwise error can occur from some hardware malfunctions, such as disk crashes. Software bugs or viruses can also make viruses. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing.

C. Data Theft

Cloud computing uses external data server for cost affective and flexible for operation. So there is a chance of data can be stolen from the external server.

D. Data Loss

Data loss is a very serious problem in Cloud computing. If banking and business transactions, research and development ideas are all taking place online, unauthorized people will be able to access the information shared. Even if everything is secure what if a server goes down or crashes or attacked by a virus, the whole system would go down and possible data loss may occur. If the vendor closes due to financial or legal problems there will be a loss of data for the customers. The customers won't be able to access those data's because data is no more available for the customer as the vendor shut down.

E. Data Location

Consumers do not always know the location of their data. The Vendor does not reveal where all the data's are stored. Cloud Computing offers a high degree of data mobility. The Data's won't even be in the same country of the Customer, it might be located anywhere in the world. They may also wish to specify a preferred location (e.g. data to be kept in the USA) then requires a contractual agreement between the Cloud service provider and the consumer that data should stay in a particular location or reside on a given known server.

F. Privacy Issues

Security of the Customer Personal information is very important in case of cloud computing. Most of the servers are external, so the vendor should make sure that is well secured from other operators.

G. Security issues in provider level

A Cloud is good only when there is a good security provided by the vendor to the customers. Provider should make a good security layer for the customer and user and should make sure that the server is well secured from all the external threats it may come across.

H. User level Issues

User should make sure that because of its own action, there shouldn't be any loss of data or tampering of data for other users who are using the same Cloud.

I. Infected Application

Service provider should have the full access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

III. PROPOSED WORK

The cloud storage providers claim that they supply the stored data with necessary security solutions. In this paper a cryptographic access control mechanism [10][11] is applied for data confidentiality and integrity. In order to provide the needed security for the stored data in the cloud, we ensure that the data is provided with cryptographic protection in terms of client centric solution.

For confidentiality of data, encryption of the data at the client side is carried out. We propose one of famous symmetric cryptography algorithm namely Blowfish for encryption and decryption of user's data.

Blowfish a public domain encryption algorithm with a block size of 64 bits, and it uses a variable key length. Blowfish was invented by an American cryptographer, Bruce Schneier, and it was introduced in 1993. It is mainly designed for large microprocessors. Its main design criteria are to be fast, compact, simple and having variable security. Its key length can be op to 448 bits long. Blowfish makes use of cycles/rounds. It consists of 16 rounds, and in each round transpositions and substitutions are used. However it is said to suffer from weak key problem, but with a full 16 rounds implementation, no ways are known to break the security of the algorithm until now. For integrity of the data, we use finger print based security mechanism.

IV. PROPOSED ALGORITHM

In this work, we applied two algorithms for providing security of client's data on the cloud server. The authentication security is provided by biometric traits with fingerprint and a cryptographic access control mechanism is applied for data confidentiality and integrity. Both these security concepts are applied for the security of client data.

A. Authentication security using Biometrics traits (Fingerprint)

Biometrics refers to the use of unique physiological characteristics to identify an individual. A number of biometric traits have been developed and are used to authenticate the person's identity. The idea is to use the special characteristics of a person to identify an individual. In this dissertation we use fingerprint biometric traits. A general impression of fingerprint is shown in figure 1 below.

Figure 1: Impression of Finger Print [6]

When using biometrics as an authentication tool, a cloud user, during Enrollment for a service, registers with his unique traits (fingerprints, tongue, face, iris).

B. Confidentiality and Integrity security using Cryptography Technique

Cryptography uses encryption and decryption concepts for providing confidentiality and integrity related security [12]. By doing so, even if a hacker gains access to an image/text, he may not be able to decrypt it back to the original image, provided, the underlying encryption algorithm is very complex to decrypt. There are number of encryption algorithms that are used for the finger print images. One such algorithm is Blowfish algorithm that is used in this thesis.

Blowfish is one of the most public domain encryption algorithms [7]. Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length. It takes a variable-length key from 32 bits to 448 bits. Blowfish has variants of 14 rounds or less. Blowfish is one of the fastest block ciphers which has developed to date. No attack is known to be successful against it, though it suffers from weak keys problem.

The algorithm has two parts, key expansion and data encryption. Key expansion consists of generating the initial contents of one array (the P-array), namely, eighteen 32-bit sub keys, and four arrays (the S boxes), each of size 256 by 32 bits, from a key of at most 448 bits (56 bytes). Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. Blowfish can have a key that ranges from 32 to 448-bits. It is suitable and efficient for hardware implementation and no license is required. Blowfish is a cipher based on Feistel rounds. No attack is known to be successful against this. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor.

Algorithm:

The basic algorithm for Blowfish is illustrated as follows:

1. Divide X into two 32-bit halves XL and XR
2. For i=1 to 16:
3. XL = XL ⊕ Pi
4. XR = F (XL) ⊕ XR
5. Swap XL and XR
6. End for
7. Swap XL and XR
8. XR = XR ⊕ P17
9. XL = XL ⊕ P18
10. Recombine XL and XR
11. Output X (64-bit data block: cipher text)

For decryption, the same process is applied, except that the sub-keys Pi must be supplied in reverse order. The nature of the Feistel network ensures that every half is swapped for the next round.

The flowchart for above algorithm is shown in figure 2 below [9].

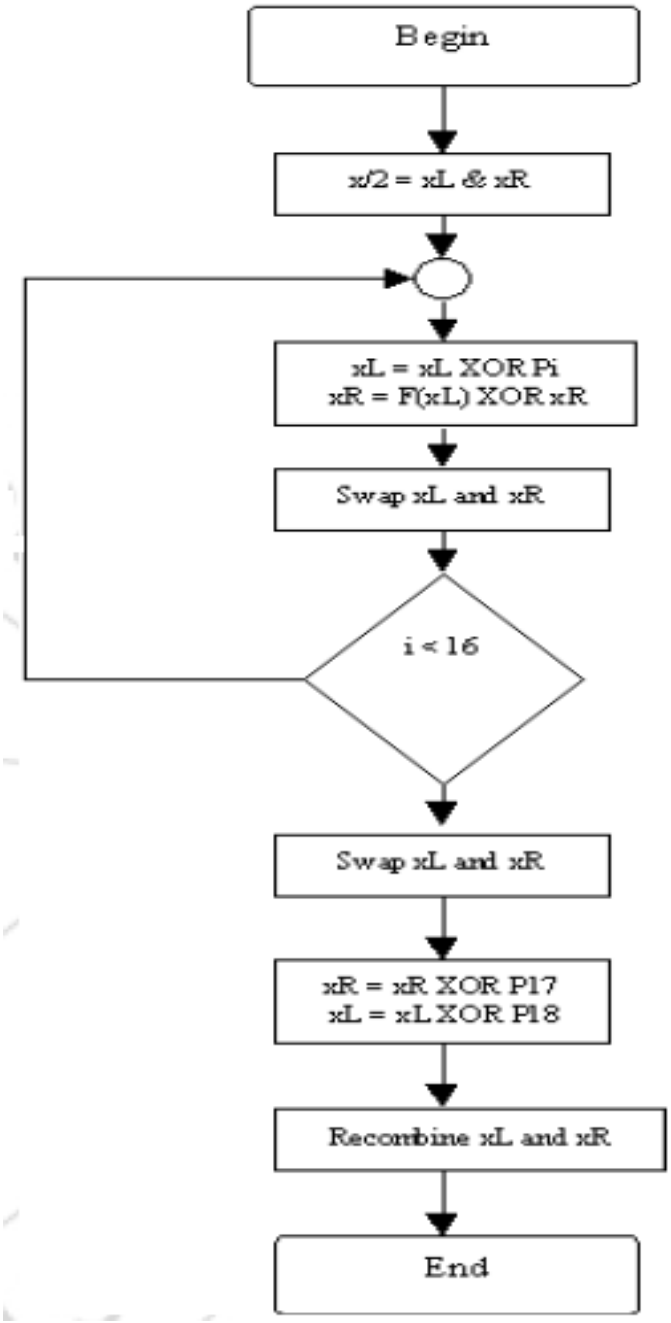


Figure 2: Flowchart for Blowfish Algorithm

V. IMPLEMENTATION & RESULTS

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

The main screen of our implementation i.e. cloud storage server will display as shown in figure 3 below.

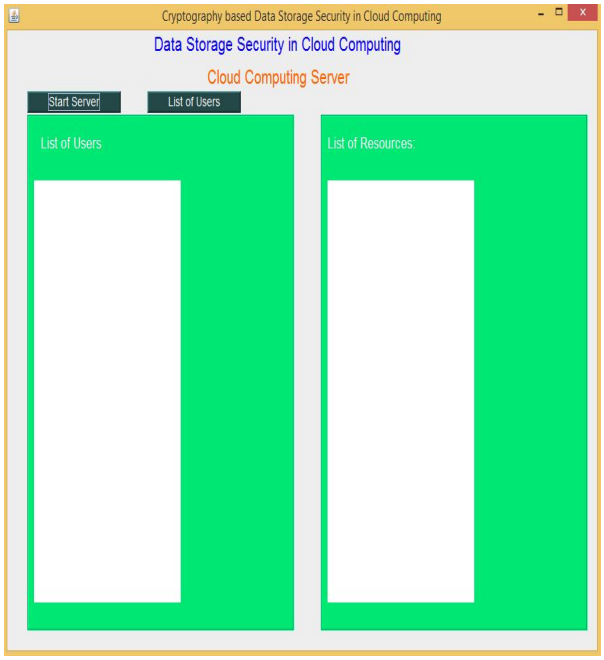


Figure 3: The main screen of Cloud Storage Server

The admin main screen contains multiple options such as Start Server, list of users and list of available resources. Press the List of users' button to view list of registered users/clients as shown in figure 4 below.

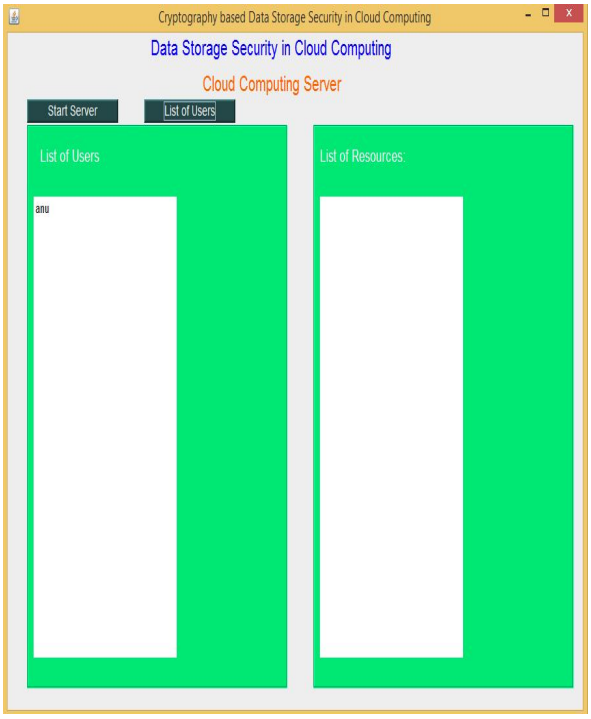


Figure 4: List of registered users

To display the corresponding resources of registered users, click on the user name and the list of available resources of that user will display. Click on the start server button to start the cloud data storage service for the different clients. Now the server is started and waiting for client.

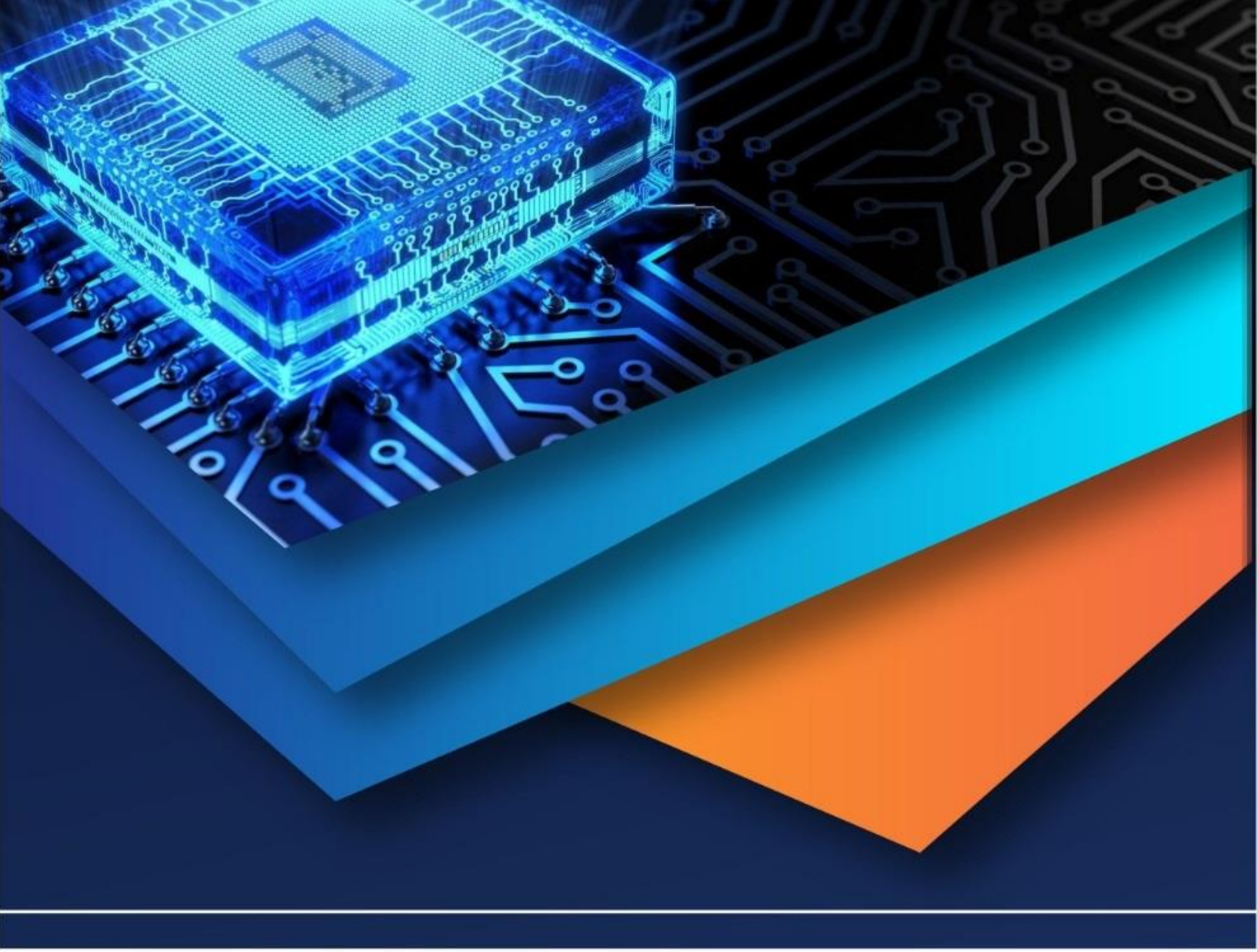
Start the client process. Type the client's authentication information and submit the information. After successfully authentication, the list of resources will display to the client.

VI. CONCLUSION

Cloud computing can be considered as a service provided by a service provider. By using cloud-based solutions, companies do not need to have their own hard ware infrastructure to host their application. Thereby the organization or company need not to invest huge amount on the infrastructure. Cloud computing can be considered as a service provided by a service provider. The user is only concerned that the service is available whenever the user needs this service. The main concern on cloud computing is that of security. Because our data and other applications reside on the cloud server. Therefore we must concern about the security of our personal data. There are different security mechanisms available in literature. But none of the methods are full poof method. In this paper, we propose a new security mechanism based on biometric fingerprint and cryptography for security of clients data on the cloud environment.

REFERENCES

[1] J. W. Rittinghouse, Cloud computing: implementation, management, and security. Boca Raton: CRC Press, 2010.
[2] P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST special publication, vol. 800, no. 145, p. 7, 2011.
[3] G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, p. 16, Nov. 2010.
[4] M. E. Whitman, Principles of information security, 4th ed. Boston, MA: Course Technology, 2012.
[5] ZiyuanWang, "Security and privacy issues within the Cloud Computing", International Conference on Computational and Information Sciences, 2011.
[6] D.Pugazhenthi, B.Sree Vidya, "Multiple Biometric Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.
[7] Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish", Journal of Global Research in Computer Science, Volume 3, No. 8, August 2012.
[8] S. S. Sudha, S. Divya, "Cryptography in Image Using Blowfish Algorithm," International Journal of Science and Research (IJSR), Volume 4 Issue 7, July 2015.
[9] Pia Singh, Prof. Karamjeet Singh, "Image Encryption and Decryption Using Blowfish Algorithm in Matlab", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
[10] A. Singh and M. Shrivastava, "Overview of Attacks on Cloud Computing," International Journal of Engineering and Innovative Technology (IJEIT), vol. 1, no. 4, Apr. 2012.
[11] "Security and Privacy in Cloud Computing - 600.412.lecture02.pdf." [Online]. Available: http://www.cs.jhu.edu/~ragib/sp10/cs412/lectures/600.412.lecture02.pdf. [Accessed: 02-May-2013].
[12] Nidal Hassan Hussein, Ahmed Khalid, "A survey of Cloud Computing Security challenges and solutions", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 1, January 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY