iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VI **Month of publication:** June 2018

DOI: http://doi.org/10.22214/ijraset.2018.6094

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 6 Issue VI, June 2018- Available at www.ijraset.com

Cloud Data Integrity Checking Using Third Party Auditor

Prof S R Nalamwar[1], Shweta Jagtap[2], Sneha Mahadik[3], Gauri Ranade[4], Safiya Shaikh [5]
[1, 2, 3, 4, 5]*Computer Department, Savitribai Phule Pune University*

Abstract*: Remote data integrity checking (RDIC) allows checking the data in- tegrity for the data stored on cloud. There are number of RDIC pro- tocols have been proposed in the literature, but they suffer from issue of a complex key management. In this project, we propose a new con- struction of identity-based (ID-based) RDIC protocol by making use of security key primitives to reduce the system complexity and the cost for establishing and managing the public key authentication framework in PKI based RDIC schemes. In our project there are three main concept that are cloud server, user and third party auditor(TPA). TPA gives the proof that our data integrity is maintain or not ,in addition we are also providing the security mechanisms .In case if the data is gets modified by the cloud server or unauthorized person then user get their original data from the dummy server. Third Party Auditor (TPA) is responsible for checking the integrity of the cloud data on behalf of the cloud users in case if cloud user does not have time to monitor their resources and integrity of data, and returns the auditing report to the cloud user.
Keywords*: Cloud Storage, data integrity, privacy preserving, identity based cryptography

I. INTRODUCTION

Cloud computing, that has received sizable attention from analysis communities in domain likewise as trade, may be a distributed computation model over an outsized pool of shared-virtualized computing resources, like storage, process power, applications and services. Cloud users can resources as they require in cloud computing atmosphere. This type of latest computation model represents a replacement vision of providing computing services as public utilities like water and electricity. Cloud computing brings variety of advantages for cloud users. For example, Users will scale back cost on hardware, software package and services as a result of they pay just for what they use; Users will get pleasure from low management overhead and immediate access to a good variety of applications; and Users will access their information where they need a network, instead of having to remain near their computers However, there's an enormous type of barriers before cloud computing are often wide deployed. A recent survey by Oracle referred the information supply from international data corporation enterprise panel, showing that security represents 87 of cloud users' fears. The key security considerations of cloud users is that the integrity of their outsourced files, since they do not physically possess their knowledge and so can lose the management over their knowledge. Moreover, the cloud server isn't totally trustworthy and it's not obligatory for the cloud server to report information loss incidents. Indeed, to establish cloud computing irresponsibleness

II. PROBLEM STATEMENT

To provide an efficient public integrity auditing scheme with secure group user revocation and also regenerate code through proxy. This system is been developed to provide integrity and regenerating code.

III.LITERATURE REVIEW

According to literature survey after looking at various IEEE paper, we gathered some identical papers and documents . Some of the topics are discussed here

Paper Name The improved Data Encryption Standard (DES) Algorithm

Author Name Seung-Jo Han,Heang-Soo Oh

Abstract cryptosystem which is most used in throughout the world for pro- tecting information is the Data Encryption Standard (DES).The DES must be stronger than other cryptosystems in the security. But the process time required for cryptanalysis has less, because hardware tech- nique has developed rapidly,the DES may be attacked by various kinds of cryptanalysis using parallel process. It may be especially vulnerable to attack by the differential cryptanalysis.The differential cryptanalysis was well known to the IBM team that designed the DES in 1974. A differential cryptanalysis attack against the DES requires 1015 chosen plaintext messages,an enormous amount.

Paper Name Security Analysis of Blowfish algorithm Author Name: Ashwak ALabaichi,Faudziah Ahmad

©IJRASET: All Rights are Reserved

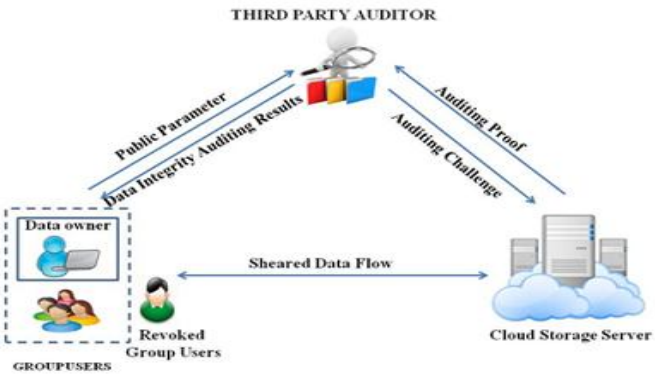
Abstract:
Blowfish algorithm (BA) is a symmetric block cipher with a 64-bit block size and variable key lengths from 32 bits up to a maximum of In order to measure the degree of security of blowfish algorithm, some cryptographic tests must be applied such as randomness test, avalanche criteria and correlation coefficient. It attempts to an- alyze the security of blowfish using avalanche criteria and correlation coefficient. It analyzed the randomness of the Blowfish output. The results obtained from the analysis of correlation coefficient showed that Blowfish algorithm gives a good nonlinear relation between plaintext and ciphertext while the results of avalanche effect indicate that the algorithm presents good avalanche effect from the second round.
Paper Name Research and Implementation of RSA Algorithm for Encryption and Decryption
Author Name: Xin Zhou,Xiaofei Tang
Abstract RSA public key cryptosystem is one of the most widely use for pub- lic key cryptography in encryption and digital signature standards.The key feature of public-key cryptosystem is that the encryption and de- cryption are done with two different keys - public key and private key, and the private key can not be derived from the public key, that enables the publication of the encryption key without the risk of leaking the secrets.The most significant approach of public key cryptography algo- rithm is RSA, which can resist almost all the known passwords attacks so far.RSA algorithm,is the first algorithm that can be used for data encryption and digital signatures.RSA algorithm's security depends on the difficulty of decomposition of large numbers. In the algorithm, two large prime numbers are used for constructing the public key and the private-key. It is estimated that the difficulty of guessing the plaintext from signal key and the cipher text equals to that decomposition of the product of two large prime numbers
Paper Name Provable Data Possession at Untrusted Stores Author Name: Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner , Zachary Peterson Dawn Song
Abstract To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation becomes critical. Recently, regenerating codes have gained popularity due to their lower repair bandwidth while pro- viding fault tolerance. Existing remote checking methods for regenerating- coded data only provide private auditing, requiring data owners to al- ways stay online and handle auditing, as well as repairing, which is sometimes impractical.
Paper Name: Remote data checking using provable data possession
Author Name: Giuseppe Ateniese , Randal Burns , Reza Curtmola , Joseph Herring , Osama Khan , Lea Kissner , Zachary Peterson , Dawn SongAbstract Consider the issue of proficiently demonstrating the uprightness of in- formation put away at untrusted servers. In the provable data pos- session (PDP) model, the customer preprocesses the information and afterward sends it to an untrusted server for capacity, while keeping a little measure of metadata. The customer later requests that the server demonstrate that the put away information has not been messed with or erased (without downloading the genuine information

IV. PROPOSED SYSTEM

We propose a replacement construction of identity-based (ID-based) RDIC protocol by creating use of key homomorphism cryptology primitive to cut back the system quality and also the value for establishing and managing the general public key authentication framework in PKI based mostly RDIC schemes.
We have a tendency to formalize ID-based RDIC and its security model together with security against a malicious cloud server and zero data privacy against a third party auditor. The planned ID-based RDIC protocol leaks no information of the kept knowledge to the auditor throughout the RDIC method.
The new construction is evidenced secure against the malicious server within the generic cluster model and achieves zero data privacy against the auditor. In depth security analysis results demonstrate that the planned protocol is demonstrably secure and sensible within the real-world applications.
We Extend this work with time span based third party auditor system and recovery of file once knowledge integrity checking fault occur.

V. SYSTEM DESIGN

©IJRASET: All Rights are Reserved



VI. ALGORITHM

A. *AES (Advanced Encryption Standard)*

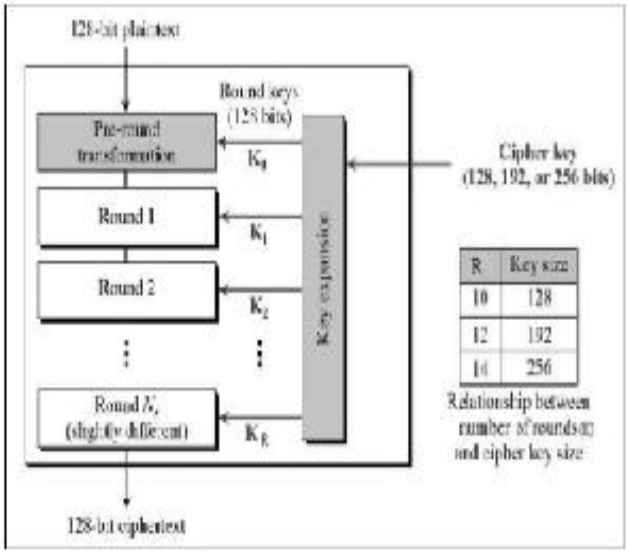
Advanced Encryption Standard The more popular and widely adopted symmetric encryption al- gorithm likely to be encountered nowadays is the Advanced En- cryption Standard (AES). It is found at least six times faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow. Operation of AES AES is an iterative rather than Feistel cipher. It is based on substitute on permutation network. It comprises of a series of linked oper- ations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permuta- tions). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. The schematic of AES structure is given in the following illustra- tion

B. *Encryption Process*

Here, we restrict to description of a typical round of AES encryp- tion. Each round comprise of four sub-processes. The first round process is depicted below

C. *Byte Substitution (SubBytes)*

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns. Shiftrows



Each of the four rows of the matrix is shifted to the left. Any entries that fall off are re-inserted on the right side of row. Shift is carried out as follows

1) First row is not shifted.
2) Second row is shifted one (byte) position to the left.
3) Third row is shifted two positions to the left.
4) Fourth row is shifted three positions to the left.

The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

D. Mix Columns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

E. Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

F. Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order

1) Add round key
2) Mix columns
3) Shift rows
4) Byte substitution Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely re- lated.

G. AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of future- proofing against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

1) Cipher(byte in[16], byte out[16], keyarrayroundkey[Nr+1])
2) begin
3) byte state[16];
4) state = in;
5) (state, roundkey[0]);
6) for i = 1 to Nr-1 stepsize 1 do
7) SubBytes(state);
8) ShiftRows(state);
9) AddRoundKey(state, roundkey[i]);
10) end for
11) SubBytes(state);
12) ShiftRows(state);
13) AddRoundKey(state, roundkey[Nr]);
14) End

H. Md5

MD5 algorithm can be used as a digital signature mechanism. This presentation will explore the technical aspects of the MD5 algorithm.

©IJRASET: All Rights are Reserved

I. Description of the MD5 Algorithm

1) Takes as input a message of arbitrary length and produces as output a 128 bit fingerprint or message digest of the input. • It is conjectured that it is computationally infeasible to pro- duce two messages having the same message digest.

2) Intended where a large file must be compressed in a secure manner before being encrypted with a private key under a public-key cryptosystem such as PGP.

3) Step 1 append padded bits: The message is padded so that its length is congruent to 448, modulo 512. Means extended to just 64 bits shy of being of 512 bits long. A single 1 bit is appended to the message, and then 0 bits are appended so that the length in bits equals 448 modulo 512.

4) Step 2 append length: A 64 bit representation of b is appended to the result of the previous step. The resulting message has a length that is an exact mul- tiple of 512 bits

5) Step 3 Initialize MD Buffer A four-word buffer (A,B,C,D) is used to compute the message digest. Here each of A,B,C,D, is a 32 bit register.

6) Step 4 cont. These registers are initialized to the follow- ing values in hexadecimal: word A: 01 23 45 67 word B: 89 ab cd ef word C: fe dc ba 98 word D: 76 54 32 10

7) Step 5 Process message in 16-word blocks. Four auxil- iary functions that take as input three 32-bit words and produce as output one 32-bit word. F(X,Y,Z) = XY v not(X) Z G(X,Y,Z) = XZ v Y not(Z) H(X,Y,Z) = X xor Y xor Z I(X,Y,Z) = Y xor (X v not(Z)

8) Step 6 Process message in 16-word blocks cont. if the bits of X, Y, and Z are independent and unbiased, the each bit of F(X,Y,Z), G(X,Y,Z), H(X,Y,Z), and I(X,Y,Z) will be independent and unbiased. – Step 7 output The message digest produced as output is A, B, C, D. That is, output begins with the low-order byte of A, and end with the high-order byte of D.

VII. ADVANTAGES

A. Remote data integrity checking for secure cloud storage.

B. It achieves soundness and perfect data privacy.

C. System proposes a protocol that is provably secure and practical in the real-world applications.

VIII. CONCLUSIONS

Identity-based remote data integrity checking protocol successfully provides secure cloud storage. The security model provides two important properties of this primitive namely, soundness and perfect data privacy. In addition to the previous work, we added time span based third party audition system and data backup. The numerical analysis demonstrated that the proposed protocol (Remote Data Integrity Checking Protocol) is efficient and practical

IX. ACKNOWLEDGMENT

It gives us great pleasure in presenting the preliminary project report on ‘Cloud Data Integrity Checking Using Third Party Auditor’. We would like to take this opportunity to thank my internal guide Prof. S. R. Nalamwar for giving us all the help and guidance we needed. We are really grateful to her for her kind support. Her valuable suggestions were very helpful.We are also grateful to Dr. D. P. Gaikwad, Head of Computer Engineering Department, AISSMS College of Engineering for his indispensable support, suggestions

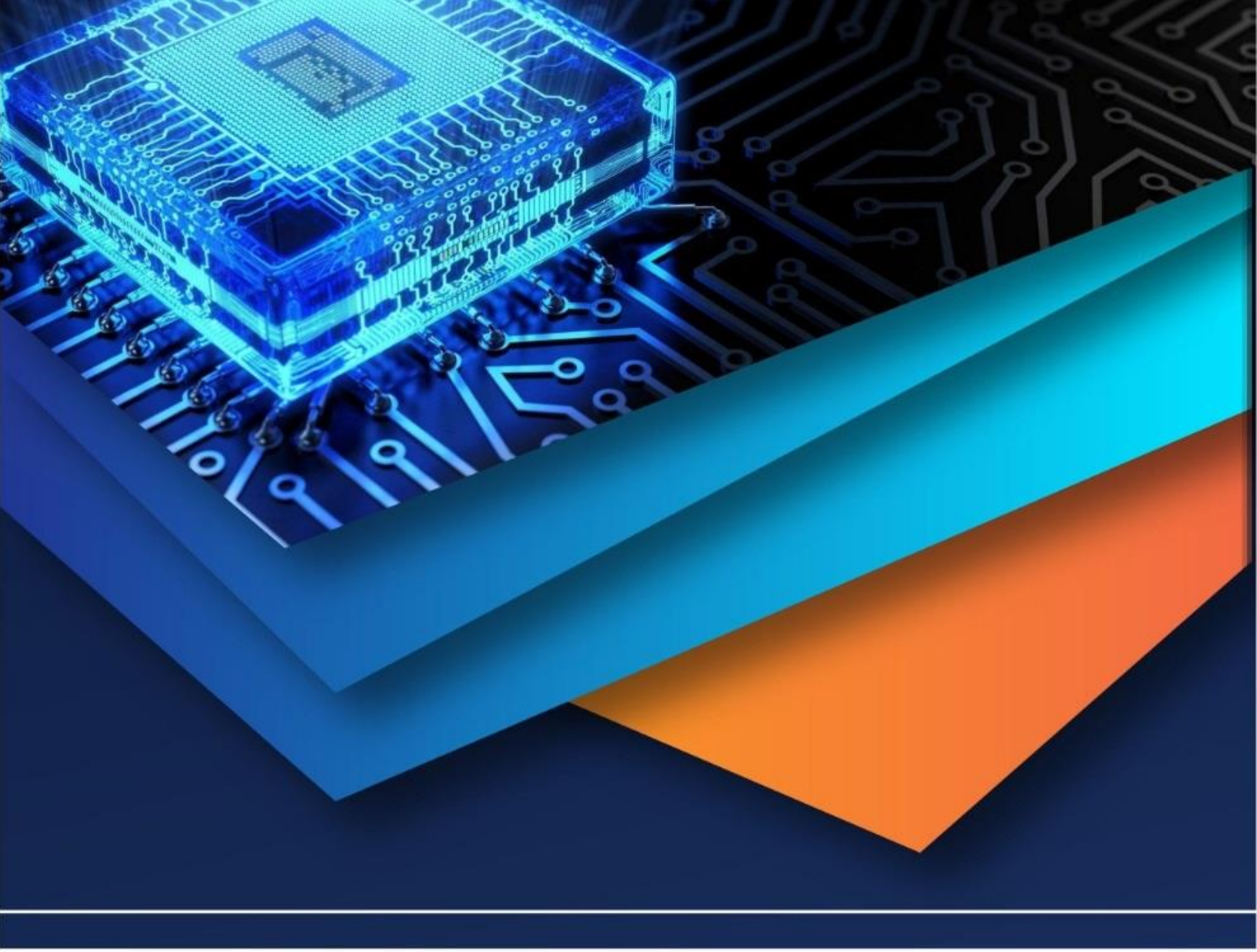
REFERENCES

[1] H. Wang, Identity-based distributed provable data possession in multicloud storage, IEEE Trans. on Service Computing, 8(2), 328–340, 2015
[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. N. J. Peterson, and D. Song, Remote data checking using provable data possession. ACM Trans. Inf. Syst. Secur., 14, 1–34, 2011.
[3] A. F. Barsoum, M. A. Hasan, Provable multicopy dynamic data possession in cloud computing systems, IEEE Trans. on Information Forensics and Security, 10(3): 485–497, 2015.
[4] D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, Proc. of CRYPTO 2001, LNCS 2139, 213–229, 2001.
[5] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. N. J. Peterson, and D. Song, Remote data checking using provable data possession. ACM Trans. Inf. Syst. Secur., 14, 1–34, 2011.
[6] A.Juels, and B. S. K. Jr. Pors, proofs of retrievability for large files.Proc. of CCS 2007, 584-597, 2007.
[7] H. Shacham, and B. Waters, Compact proofs of retrievability. Proc. Of Cryptology-ASIACRYPT 2008, LNCS 5350, pp. 90-107, 2008.
[8] G. Ateniese, S. Kamara, J. Katz, Proofs of storage from homomorphic identification protocols. Proc. of ASIACRYPT 2009, 319-333, 2009
[9] A. F. Barsoum, M. A. Hasan, Provable multicity dynamic data possession in cloud computing systems, IEEE Trans. on Information Forensics and Security, 10(3): 485–497, 2015

©IJRASET: All Rights are Reserved

[10] J. Yu, K. Ren, C.Wang, V. Varadharajan, Enabling cloud storage auditing with key-exposure resistance, IEEE Trans. on Information Forensics and Security, 10(6): 1167–1179, 2015.
[11] J. Liu, K. Huang, H. Rong, H. M. Wang, Privacy-preserving public auditing for regenerating-code-based cloud storage, IEEE Trans. On Information Forensics and Security, 10(7): 1513–1528, 2015.
[12] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing. Proc. of ESORICS2009, LNCS 5789, 355–370, 2009.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)