iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

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

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Catch You If You Lie: Search Results Verification in Cloud Computing Based on Keyword Encryption

Monika Patil[1], Sarika Bodake[2]
[1,2]PVPIT, Bavdhan, Pune Department of computer science.

Abstract: ***As an essential information use, secure Pivotal word scan again encrypted cloud information need pulled in those enthusiasm about a number scientists. This is the reason scientists expect that those cloud server is inquisitive and legitimate, where the hunt effects aren't affirmed. If cloud server act mischievously and working insincerely after that make them. Dissimilar to past scheme, recommend on novel impediment built plan. Clinched alongside verification, the cloud server can't realize which information owner, alternately the thing that amount from claiming information manager trade family information which will try for checking those cloud server's rowdiness. Intended confirmation scheme, those cloud server can't realize which information holder information are inserted in the confirmation information buffer, or what no of information Owner's confirmation information are truly used to confirmation. All servers know that, Assuming that he acts insincerely toward amount from claiming times then he must make rebuffed. Should streamline those estimation from claiming parameters used advancement of the mystery confirmation information cushion.***
Keywords- Cloud computing, dishonest cloud server, data verification, deterrent

I. INTRODUCTION

With the coming about cloud computing, an ever increasing amount individuals have a tendency with outsource their information of the cloud. Cloud registering gives colossal reductions including not difficult access, diminished costs, fast deployment, Also adaptable asset administration The greater part about existing researches would In light of an perfect gas supposition that those cloud server will be "curious Yet honest" secure Pivotal word look over encrypted cloud information need pulled in those premium from claiming a significant number specialists as of late. Likewise it may be a accepted that cloud server will never act mischievously However at times it could. Existing schemes allotment a basic assumption, i. E., information owners anticipate those request of hunt effects. However, in useful applications, various information managers need aid involved; each information manager just knows its identity or incomplete request. Without Comprehending those downright order, these information owners can't utilize the accepted schemes will check the quest comes about. A compromised cloud server might exchange false hunt outcomes should information clients for Different reasons; those cloud server might profit fashioned scan outcomes. For example, those cloud might rank a promotion higher over others, since the cloud camwood benefit starting with it, alternately the cloud might return irregular extensive files will acquire money, since those cloud adopts the 'pay as you consume' model. Those cloud server might profit inadequate quest brings about crest hours should dodge enduring from execution bottlenecks.

II. RELATED WORK

Standard searchable encryption arrangements tolerance customers on securely gander In mixed data through watchwords, these methodologies reinforce barely boolean pursuit, without getting whatever fact that data records. This approach encounters two guideline downsides The point when particularly joined with respects with cloud registering. Starting with person viewpoint, clients, who don't generally bring pre-information of the fried cloud information, requirement on post get ready every recouped archive for a particular wind objective with find ones the vast majority facilitating their enthusiasm; on the different hand, ceaseless warrant recouping every last bit records holding the doubted catchphrase also makes superfluous framework activity, which will be totally undesirable Previously, today's payment as-you-utilize cloud perspective. Will fare thee well of the issue for fruitful yet secure positioned catchphrase take a gander over mixed cloud data may be recommended. Positioned look tremendously upgrades schema accommodation.

Fluffy Pivotal word scan extraordinarily enhances framework usability by giving back the matching files when users' looking inputs

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

precisely match the predefined keywords alternately those closest time permits matching files dependent upon Pivotal word similitude semantics, At correct match neglects.

Empowering watchword gander particularly In mixed data is a engaging framework to urging use about encoded majority of the data outsourced of the cloud. Existing courses of action provide for multi watchword right pursuit that doesn't continue catchphrase spelling mistake, alternately single catchphrase feathery request that bear grammatical mistakes should certain level. The ebb What's more stream feathery request arrangements rely on upon fabricating an stretched out rundown that spreads possible catchphrase inaccurate spelling, which prompt should basically greater record record measure Also higher chase diserse caliber. Those recommended plot accomplishes feathery facilitating through algorithmic framework Likewise restricted on developing the record archive. It similarly wipes out those requirement of a predefined vocabulary and effectively bolsters various watchword feathery chase without Extending those document or pursuit many-sided nature.

III. PROPOSED SYSTEM

Proposed scheme allow data owners to construct the verification data efficiently. The cloud server should also return the verification data without introducing heavy costs. Additionally, data users can verify the search result efficiently. Deter the cloud server from behaving dishonestly. Once the cloud server behaves dishonestly, the scheme should detect it with a high probability.

Standard searchable encryption arrangements tolerance customers should securely search In mixed data through watchwords, these methodologies reinforce barely boolean pursuit, without getting any fact that majority of the data records. This approach encounters two guideline downsides when particularly associated for views will cloud registering. From person viewpoint, clients, who don't generally have pre-information of the fried cloud information, requirement will post get ready each recouped record for a particular end objective should uncover ones The majority facilitating their enthusiasm; on the other hand, ceaseless warrant recouping at records holding those doubted catchphrase Moreover reasons superfluous framework activity, which will be totally undesirable to today's recompense as-you-utilize cloud perspective. On fare thee well of the issue from claiming effective yet secure positioned catchphrase take a gander In mixed cloud majority of the data will be suggested. Positioned look for tremendously upgrades schema comfort.

Fluffy Pivotal word scan incredibly enhances framework usability Eventually Tom's perusing returning the matching files when users' looking inputs precisely match the predefined keywords alternately those closest could be allowed matching files In view of Pivotal word similitude semantics, At correct match fizzles.

Empowering watchword gander particularly again mixed data will be an alluring framework for urging use from claiming encoded data outsourced of the cloud. Existing courses of action provide for multi watchword right pursuit that doesn't continue catchphrase spelling mistake, or solitary catchphrase feathery request that bear grammatical mistakes on certain degree. The ebb What's more stream feathery request arrangements rely on upon fabricating a stretched out rundown that spreads possible catchphrase inaccurate spelling, which prompt with basically greater record record measure and higher chase diserse nature. The recommended plot accomplishes feathery facilitating through algorithmic framework Likewise contradicted with developing those record report. It similarly wipes crazy the have of a predefined vocabulary What's more effectively bolsters various watchword feathery chase without Extending those document or pursuit many-sided nature.

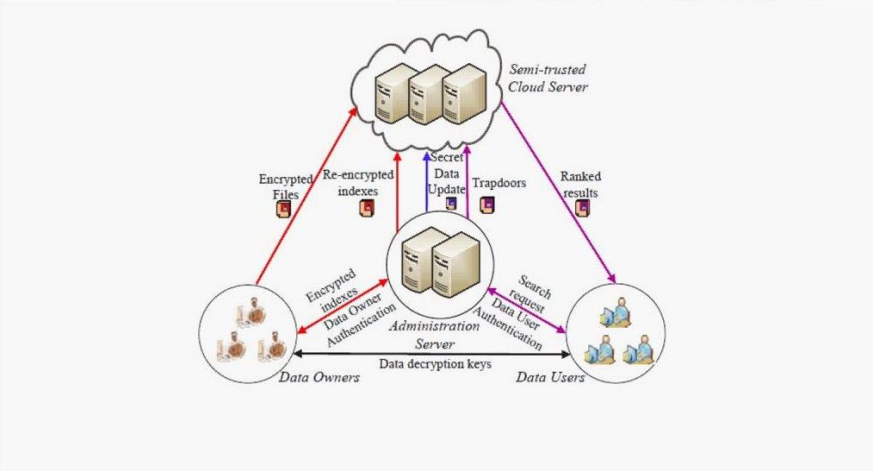


Figure1. System Architecture

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. IMPLEMENTATION PLAN

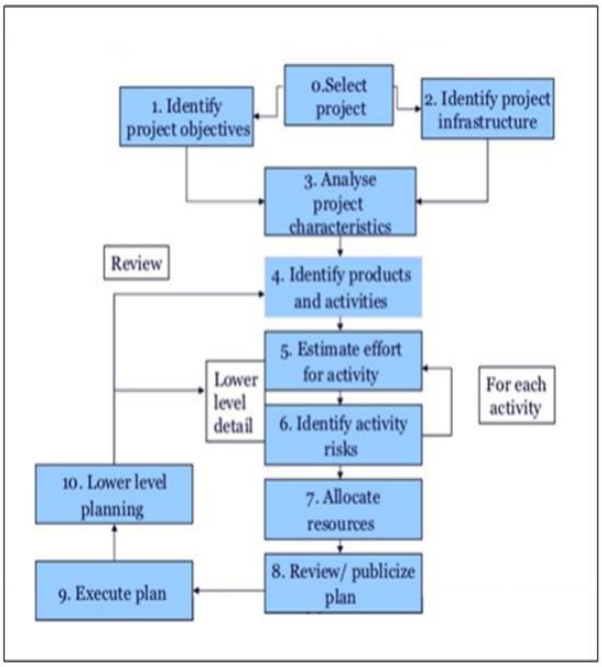


Figure 2: Software Development Planning Activity

V. DESCRIBED MODULE

A. *Data owner Login*

This is the authentication module of the system to provide access to Data owner.

B. *File upload*

Data Owner will upload file by choosing the file from the documents.

C. *Query and Feedback*

This module is used to give feedback of the result from cloud server by user. User having query he/she can directly post on it. Data Owner can see query and feedback of each user.

D. *User Login and Registration*

This is the authentication module of the system facilitating users to add themselves to the system as well as authenticate and utilize the system, thereby providing access to valid registered users in the system.

E. *Keyword ranking*

This module is developed for keywords ranking purpose. By using k-nn algorithm it ranked out the keywords from the file which is uploaded by Data owner.

F. *Verification*

Verification module used for the verify the result given by the cloud server is correct or not. This module helps to find out dishonest cloud server.

VI. MATHEMATICAL MODULES

S is the system

S= {I, O, F, K, Success, Failure}

Where,

I = Set of Input

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

I={I1, I2, I3}
Where,
I1=Login user ID
I2=Login password
I3=File
I4=Keyword to search
I5=Remark
K= Secret key
O=Set of Outputs
O= {O1, O2, O3, O4, O5}
Where,
O1=Authentication Message
O2=Encrypted File
O3= Search result
O4= Verification result
O5= Remark the cloud
F=Set of Functions
F={F1, F2, F3, F4,F5}
Where,
F1=Authentication
O1←F1(I1, I2)
F2=Encryption
O2←F2(I3,K)
F3= Search files based on keyword
O3←F3(I4)
F4= Result of verification
O4←F4(O3)
F5= Cloud behavior
O5←F5(I5)

A. Success

1) Authentication successful.
2) Application start.
3) Encrypt the data.
4) Return the result based on keywords.
5) Owner verified the data and provide data to user.

B. Failure

1) Authentication failed
2) Application not started.
3) Doesn't give the result.
4) Owner doesn't verify the data.

VII. ALGORITHM USED

A. Algorithm1. Constructing Sampled data

Input
O_i's ID i number of sampled data and w_t's file
List F I D[d]
Output

Sample data SD_i

1) Initialize sampled data SD_i to W_t //i
2) Rank W_t 'S file List F I D[d] in descending order of Relevance scores
3) Concatenate F I D[0]//$RS_{0;t}$ to SD_i
4) Uniformly and randomly generate -1 number set R Where R[r]ϵ[1;d]
5) Rank R incrementally
6) for ind=1 to -1 do
7) concatenate F I D[R[ind]]//$RS_{R[ind];t}$ to SD_i
8) end for
9) return SD_i

B. Algorithm2. Securely returning verification data

Input
Verification request set [<j;E(PK;r_j)>]jϵ[1;β]
The size of Verification data buffer γ
Output
Verification data buffer VB

1) The cloud initialize VB with γ entries each Entry with initial value 1
2) For jϵ[1;β] do
3) Locates O_j'S verification data V_j
4) Computer vd=E(PK;r_j)^{v2}
5) For i in range (0_K) do
6) V B [h_i(j)= V B [h_i(j).v d
7) end for
8) end for
9) return VB

VIII. S/W REQUIREMENT SPECIFICATION

A. Minimum Hardware Requirements

Hardware	Minimum Requirement
Processor	Pentium Dual Core 2.80 GHz or above
Primary Memory	1GB RAM or more
Secondary Memory	20 GB (minimum)

B. Minimum Software Requirements

Software	Minimum Requirement
Front End (Prog. Lang.)	J2SDK1.5 Java and J2EE
Backend (DB)	My SQL
Development Tool (IDE)	Net Beans 6.0 or later

IX. EXPECTED RESULT

Figure3 shows dataset keyword vs file. This dataset is used by owner to upload files
It shows that the file which contains more number of keywords then the possibility for it to get selected when the user type a particular keyword is more. So here search factor is the measure of a file to get selected while searching.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

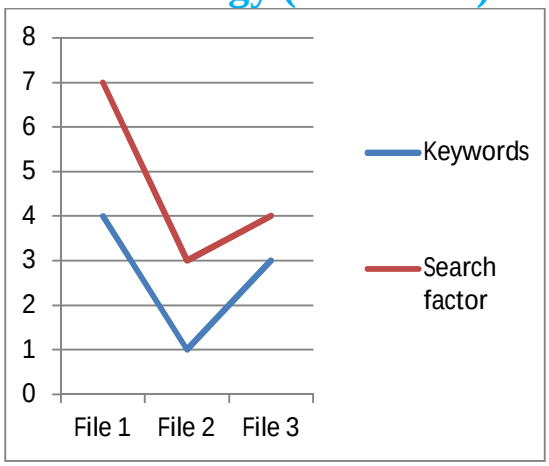


Figure3. Data table Description

The following table shows the performance result of proposed system. Tables consist of time required to retrieve data from cloud with respect to number of files present on cloud server.

Sr. No	Time(Sec)	No. of Files
1	100	7
2	160	8
3	200	11
4	310	12
5	400	13

Table1. Result Table

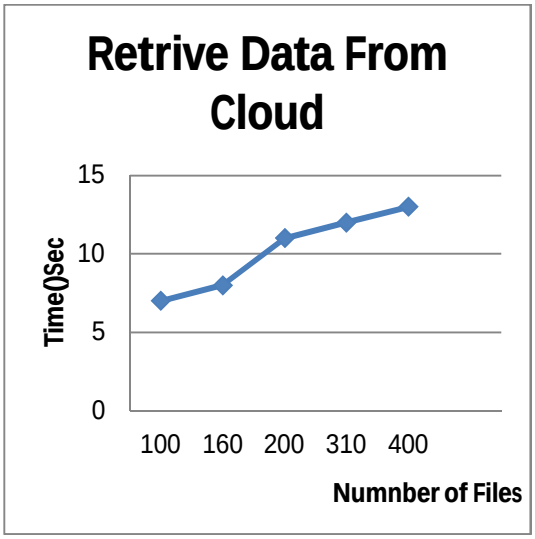


Figure4. Result Analysis

Graph shows performance and proposed system algorithm time cost. Fig.4 Shows possible result As the number of files increases the time cost also increases to retrieve information from the cloud.

X. CONCLUSION

The cloud server may be not reasonable from claiming which information owners, alternately know what number of information holders return family information utilized for verification, he also doesn't realize which information owners' information would inserted in the confirmation information support or know what number of information owners' confirmation information are really utilized for confirmation. Every last one of cloud server knows will be that, When he behaves dishonestly, he might be ran across for An helter skelter probability, and rebuffed genuinely When uncovered.. Finally, with careful Investigation Furthermore broad experiments, we affirm those viability and effectiveness for our recommended schemes.

We are allowing multiword files upload. Multiple owners can upload file to a cloud. If in case cloud misbehaves then we are sending this info to the owner of the file. We are mailing the owner the details of the user who requested his file. – This detail contains the mail id of user. So by this info owner can directly send the key to the user via mail and user can decrypt the file through that key.

XI. FUTURE WORK

In future work, Precisely, when the user's query is a sentence, we can extract the attributes of a sentence, and then express the relationship between attributes and search though the attributes.

XII. ACKNOWLEDGMENT

I am really grateful to the principal for encouragement to carry out this work and I also heartily thank Prof.S. V. BODAKE for giving me an opportunity to complete this research. I would like to thank you for encouraging my research. Your advice on research has been priceless.

REFERENCES

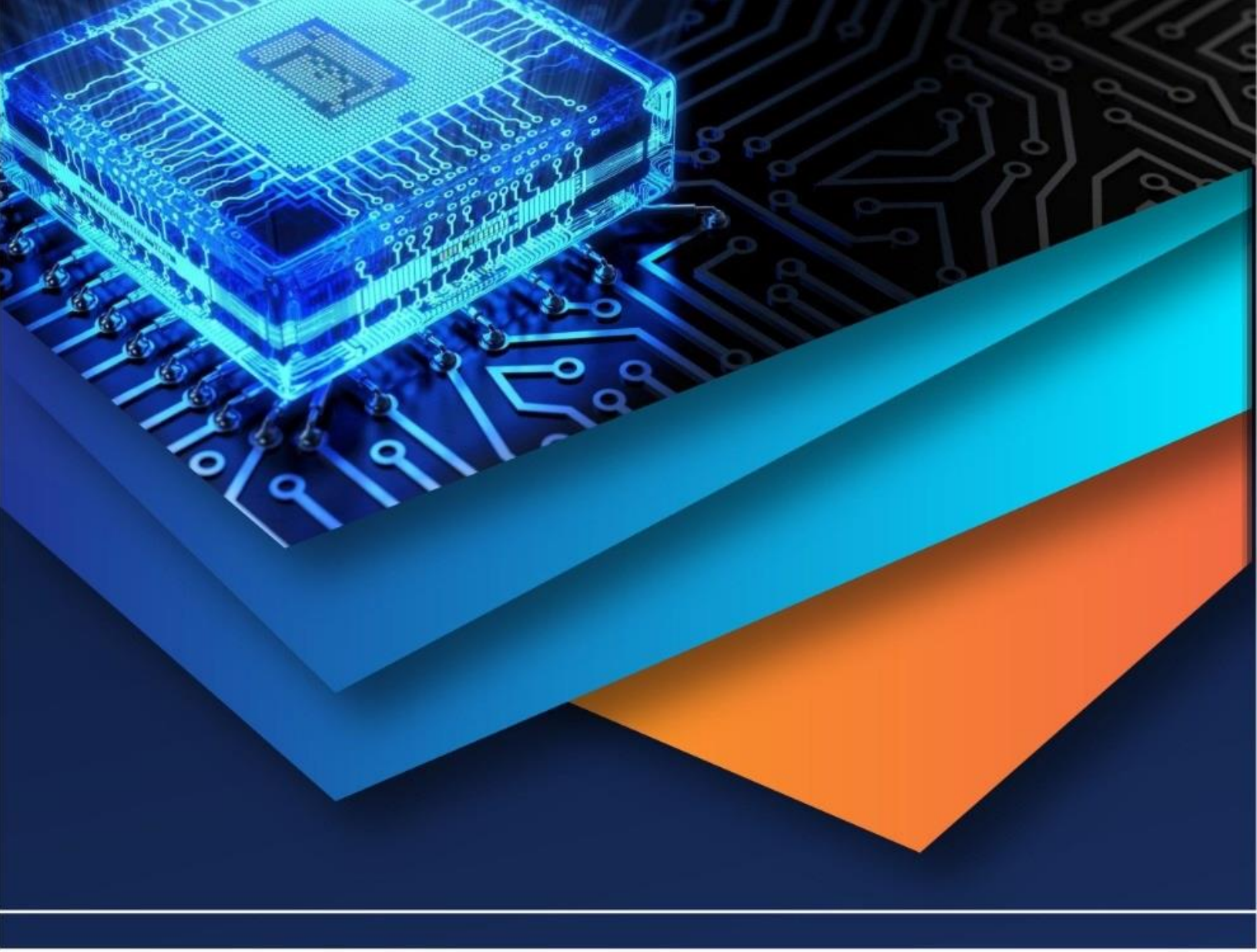
[1] Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data, " in Proc. IEEE Distributed Computing Systems (ICDCS'10), Genoa, Italy, Jun. 2010, pp. 253– 262

[2] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: Verifiable attributebased keyword search over outsourced encrypted data, " in Proc. IEEE INFOCOM'14, Toronto, Canada, May 2014, pp. 522–530

[3] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, "Efficient multi-keyword ranked query on encrypted data in the cloud, " in Proc. IEEE Parallel and Distributed Systems (ICPADS'12), Singapore, Dec. 2012, pp. 244–251

[4] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing, " in Proc. IEEE INFOCOM'10, San Diego, CA, Mar. 2010, pp. 1–5

[5] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi keyword fuzzy search over encrypted data in the cloud, " in IEEE INFOCOM, Toronto, Canada, May 2014, pp. 2112–2120.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY