iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VIII **Month of publication:** August 2014

DOI:

www.ijraset.com

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

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Cloud Computing Threats

Vibha Sahu[1], Brajesh Dubey[2], Dr.S.M.Ghosh[3]

[1]*Dr.C.V.RAMAN UNIVERSITY,BILASPUR,INDIA*

PHD SCHOLAR

[2]*DR.C.V.RAMAN UNIVERSITY, BILASPUR,INDIA*

MPHIL SCHOLAR

[3]*RUNGTA COLLEGE OF ENGINEERING & TECHNOLOGY BHILAI, C.G..INDIA*

ASSOCIATE PROFESSOR

Abstract:The progress of cloud computing services is accelerating the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloudremains attractive trend from a financial perspective.Development of the cloud service model delivers business-supporting technology more efficiently than ever before. The shift from server to service-based thinking is transforming the way technology departments think about, design, and deliver computing technology and applications. Security is a key requirement for cloud computing combine as a robust and feasible versatile solution. Central component of managing risks in cloud computing is to understand the nature of security threats. Recognizing both the promise of cloud computing, and the risks associated with ithere we identify critical areas in cloud computing andunderstand cloud security threats in order to make educated risk-management decisions regarding cloud adoption strategies. This report focuses on threats specifically related to the shared, on-demand nature of cloud computing.

Keywords:cloud computing, problems, threats, security.

1. INTRODUCTION

Among the most significant security risks associated with cloud computing is the tendency to bypass information technology (IT) departments and information officers. Although shifting to cloud technologies exclusively is affordable and fast, doing so undermines important business-level security policies, processes, and best practices. In the absence of these standards, businesses are vulnerable to security breaches that can quickly erase any gains made by the switch to SaaS. Cloud computing need to appeal to the feelings of the clients and address the potential security risks in a manner that clients will feel safe and secure. By addressing security is this way clients will feel safer and secure and hence trust cloud service providers. The central component of managing risks in cloud computing is to understand the nature of security threats Security is a key requirement for cloud computing combine as a robust and feasible versatile solution. Many similarities in these viewpoints indicate a grave concern on crucial security and legal obstacles for cloud computing, including service availability, data confidentiality, provider lock-in and status fate sharing. These concerns have their origin not only on existing problems, directly inherited from the adopted technologies, But also related to new issues derived from the work of essential cloud computing features. The top threats report reflects the current consensus among experts about the most significant threats to cloud security. While there are many vulnerabilities to cloud security, this report focuses on threats specifically related to the shared, on-demand nature of cloud computing. To identify the top threats, we searched on web, read many journals and publication and conduct some survey.We identified the following threats to cloud security (ranked in order of severity):

1. Data Breaches

2. Data Loss

3. Account Hijacking

4. Insecure APIs

5. Denial of Service

6. Nasty Insiders

7. Misuse of Cloud Services

8. Lacking Due Diligence

9. Shared Technology Issues

These documents will offer valuable guidance during the formation of comprehensive, appropriate cloud security strategies

2. CLOUD COMPUTING SECURITY THREATS

2.1 Data Breaches:It's every CIO's worst nightmare: the organization's sensitive internal data falls into the hands of their competitors. If a cloud service database is not properly designed, a flaw in one client's application could allow an attacker access not only to that client's data, but every other client's data as well. While this scenario has kept executives awake at night long before the advent of computing, cloud computing introduces significant new avenues of attack. In November 2012, researchers from the University of North Carolina, the University of Wisconsin and RSA Corporation released a paper describing how a virtual machine could use side channel timing information to extract private cryptographic keys being used in other virtual machines on the same physical server. However, in many cases an attacker wouldn't even need to go to such lengths.

2.1.1 Implications:-Unfortunately, while data loss and data leakage are both serious threats to cloud computing. You may be able to encrypt your data to reduce the impact of a data breach, but if you lose your encryption key, you'll lose your data as well. Conversely, you may decide to keep offline backups of your data to reduce the impact of a catastrophic data loss, but this increases your exposure to data breaches.

2.1.2 controls:

Retention Policy

Secure Disposal

Non-Production Data

Information Leakage

Risk Assessments

Encryption Key Management

User ID Credentials

Data Security/Integrity

Production/Non-Production Environments

Remote User Multi-Factor Authentication

2.2.Data Loss:For both consumers and businesses, the prospect of permanently losing one's data is terrifying. Just ask Mat Honan, writer for wired magazine: in the summer of 2012, attackers broke into Mat's Apple, Gmail and Twitter accounts. They then used that access to erase all of his personal data in those accounts, including all of the baby pictures Mat had taken of his 18-month-old daughter.

Of course, data stored in the cloud can be lost due to reasons other than malicious attackers. Any accidental deletion by the cloud service provider, or worse, a physical catastrophe such as a fire or earthquake, could lead to the permanent loss of customers' data unless the provider takes adequate measures to backup data. Furthermore, the burden of avoiding data loss does not fall solely on the provider's shoulders. If a customer encrypts his or her data before uploading it to the cloud, but loses the encryption key, the data will be lost as well.

2.2.1 Implications:- Under the new EU data protection rules, data destruction and corruption of personal data are considered forms of data breaches and would require appropriate notifications.

ISSN: 2321-9653

Additionally, many compliance policies require organizations to retain audit records or other documentation. If an organization stores this data in the cloud, loss of that data could jeopardize the organization's compliance status.

2.2.2 Controls

Retention Policy

Risk Assessments

Environmental Risks

Equipment Location

2.3.Account or Service Traffic Hijacking:

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

In April 2010, Amazon experienced a Cross-Site Scripting (XSS) bug that allowed attackers to hijack credentials from the site. In 2009, numerous Amazon systems were hijacked to run Zeus botnet nodes.

2.3.1 Implications :- Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach. Organizations should look to prohibit the sharing of account credentials between users and services, and leverage strong two-factor authentication techniques where possible.

2.3.2 Controls

User Access Policy

User Access Restriction/Authorization

User Access Revocation

User Access Reviews

Incident Management

User ID Credentials

Remote User Multi-Factor Authentication

Audit Logging / Intrusion Detection

2.4. Insecure Interfaces and APIs :- Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third-parties in order to enable their agency.

2.4.1 Implications :- While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

2.4.2 Controls :- User Access Restriction/Authorization

Data Security/Integrity

ISSN: 2321-9653

Application Security

2.5.Denial of Service :- Simply put, denial-of-service attacks are attacks meant to prevent users of a cloud service from being able to access their data or their applications. By forcing the victim cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker (or attackers, as is the case in distributed denial-of-service (DDoS) attacks) causes an intolerable system slowdown and leaves all of the legitimate service users confused and angry as to why the service isn't responding.

While DDoS attacks tend to generate a lot of fear and media attention (especially when the perpetrators are acting out of a sense of political "hactivism"), they are by no means the only form of DoS attack. Asymmetric application-level DoS attacks take advantage of vulnerabilities in web servers, databases, or other cloud resources, allowing a malicious individual to take out an application using a single extremely small attack payload – in some cases less than 100 bytes long.

2.5.1 Implications :- Experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock: there's no way to get to your destination, and nothing you can do about it except sit and wait. As a consumer, service outages not only frustrate you, but also force you to reconsider whether moving your critical data to the cloud to reduce infrastructure costs was really worthwhile after all. Even worse, since cloud providers often bill clients based on the compute cycles and disk space they consume, there's the possibility that an attacker may not be able to completely knock your service off of the net, but may still cause it to consume so much processing time that it becomes too expensive for you to run and you'll be forced to take it down yourself.

2.5.2 Controls :-

Baseline Requirements

Capacity/Resource Planning

Equipment Power Failures

Application security

2.6 Malicious Insiders :- The risk of malicious insiders has been debated in the security industry. While the level of threat is left to debate, the fact that the insider threat is a real adversary is not.

CERN defines an insider threat as such:

"A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."

2.6.1 Implications :- A malicious insider, such as a system administrator, in an improperly designed cloud scenario can have access to potentially sensitive information.

From IaaS to PaaS and SaaS, the malicious insider has increasing levels of access to more critical systems, and eventually to data. Systems that depend solely on the cloud service provider (CSP) for security are at great risk here. Even if encryption is implemented, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack.

2.6.2 Controls :-

Third Party Audits

Ownership / Stewardship

Handling / Labeling / Security Policy

Information Leakage

User Access

Unauthorized Persons Entry

Off-Site Authorization

Background Screening

Policy Enforcement

User Access Restriction / Authorization

User Access Reviews

Roles / Responsibilities

Segregation of Duties

Encryption

2.7 Abuse of Cloud Services :-One of cloud computing's greatest benefits is that it allows even small organizations access to vast amounts of computing power. It would be difficult for most organizations to purchase and maintain tens of thousands of servers, but renting time on tens of thousands of servers from a cloud computing provider is much more affordable. However, not everyone wants to use this power for good. It might take an attacker years to crack an encryption key using his own limited hardware, but using an array of cloud servers, he might be able to crack it in minutes. Alternately, he might use that array of cloud servers to stage a DDoS attack, serve malware or distribute pirated software.

2.7.1 Implications :- This threat is more of an issue for cloud service providers than cloud consumers, but it does raise a number of serious implications for those providers. How will you detect people abusing your service? How will you define abuse? How will you prevent them from doing it again?

2.7.2 Controls

Incident Response Legal Preparation

Acceptable Use

2.8 Insufficient Due Diligence :-Cloud computing has brought with it a gold rush of sorts, with many organizations rushing into the promise of cost reductions, operational efficiencies and improved security. While these can be realistic goals for organizations that have the resources to adopt cloud technologies properly, too many enterprises jump into the cloud without understanding the full scope of the undertaking.

Without a complete understanding of the CSP environment, applications or services being pushed to the cloud, and operational responsibilities such as incident response, encryption, and security monitoring, organizations are taking on unknown levels of risk in ways they may not even comprehend, but that are a far departure from their current risks.

2.8.1 Implications:-An organization that rushes to adopt cloud technologies subjects itself to a number of issues. Contractual issues arise over obligations on liability, response, or transparency by creating mismatched expectations between the CSP and the customer. Pushing applications that are dependent on "internal" network-level security controls to the cloud is dangerous when those controls disappear or do not match the customer's expectation. Unknown operational and architectural issues arise when designers and architects unfamiliar with cloud technologies are designing applications being pushed to the cloud.

The bottom line for enterprises and organizations moving to a cloud technology model is that they must have capable resources, and perform extensive internal and CSP due-diligence to understand the risks it assumes by adopting this new technology model.

2.8.2 Controls

Risk Assessments

Baseline Requirements

Industry Knowledge / Benchmarking

Capacity / Resource Planning

Program

Assessments

Management Program

Impact Analysis

Business Continuity Planning

Data Security / Integrity

Application Security

ISSN: 2321-9653

2.9 Shared Technology Vulnerabilities :-Cloud service providers deliver their services in a scalable way by sharing infrastructure, platforms, and applications. Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models. A defensive in-depth strategy is recommended and should include compute, storage, network, application and user security enforcement, and monitoring, whether the service model is IaaS, PaaS, or SaaS. The key is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud.

2.9.1 Implications :-A compromise of an integral piece of shared technology such as the hypervisor, a shared platform component, or an application in a SaaS environment exposes more than just the compromised customer; rather, it exposes the entire environment to a potential of compromise and breach. This vulnerability is dangerous because it potentially can affect an entire cloud at once.

2.9.2 Controls

Handling / Labeling / Security Policy

Baseline Requirements

User Access Policy

Segregation of Duties

Encryption

Vulnerability / Patch Management

User ID Credentials

Segmentation

Shared Networks

Audit Logging / Intrusion Detection

3.CONCLUSION

The top threats report reflects the current consensus among experts about the most significant threats to cloud security. While there are many vulnerabilities to cloud security, this report focuses on threats specifically related to the shared, on-demand nature of cloud computing. With descriptions and analysis of these threats, this report serves as an up-to-date threat identification guide that will help cloud users and providers make informed decisions about risk mitigation within a cloud strategy.The time to institute strong cloud security and encryption is now- before attack. Don't think that it cannot (or will not) happen to anyone because either we are too powerful or too big(or too small).It happened to Amazon. It happens to business every day. And these type of catastrophes have the ability to exhaust the budgets, destroy reputation, and in some cases eradicate business.

4.FUTURE SCOPE

Security is a crucial aspect for providing a reliable environment and then enables the use of applications in thecloud and for moving data and business processes tovirtualized infrastructures. However, the impact ofsuch issues is intensified in cloud computing due tocharacteristics such as multi-tenancy and resource sharing,since actions from a single customer can affect allother users that inevitably share the same resources andinterfaces.

A deeperstudy on current security solutions to manage cloud computingvirtual machines inside the cloud providers shouldbe a focus of future work in the area.Researches relatedto identity and credentials management in the cloud environment should address basic needs for bettersecurity mechanisms in virtualized and distributed architectures,guiding other future researches in the securityarea.

REFERENCES

1. IDC (2009) Cloud Computing 2010 –Update. slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update

2. CSA (2009) Security Guidance for Critical Areas of Focus in Cloud Computing.

3. Hubbard D, Jr LJH, Sutton M (2010) Top Threats to Cloud Computing. Tech. rep., Cloud Security Alliance. cloudsecurityalliance.org/research/projects/top-threats-to-cloud-computing

4. Tompkins D (2009) Security for Cloud-based Enterprise Applications.http://blog.dt.org/index.php/2009/02/security-for-cloud basedenterprise-applications/

5. Brodkin J (2008) Gartner: Seven cloud computing security risks.http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853.

6. Cross-VM Side Channels and Their Use to Extract Private Keys http://www.cs.unc.edu/~yinqian/papers/crossvm.pdf

7.Multi-TenantDataArchitecture
http://msdn.microsoft.com/en-us/library/Aa479086

8. Cross-VM Side Channels and Their Use to Extract Private Keys http://www.cs.unc.edu/~yinqian/papers/crossvm.pdf

9. Pirate Bay Ditches Servers and Switches to the Cloud http://news.cnet.com/8301-1023_3-57534707-93/pirate-bay-ditches-servers-and-switches-to-the-cloud/

10. Insider threats to cloud computing http://www.cloudtweaks.com/2012/10/insider-threats-to-cloud-computing/

11. Cloud's privileged identity gap intensifies insider threats http://www.darkreading.com/insider-threat/167801100/security/news/240146276/cloud-s-privileged-identity-gap-intensifies-insider-threats.html

12. Computerworld: DDoS is Cloud's security Achilles heel (September 16, 2011) http://www.computerworld.com.au/article/401127/ddos_cloud_security_achilles_heel/

13. OWASP: Application Denial of Service https://www.owasp.org/index.php/Application_Denial_of_Service

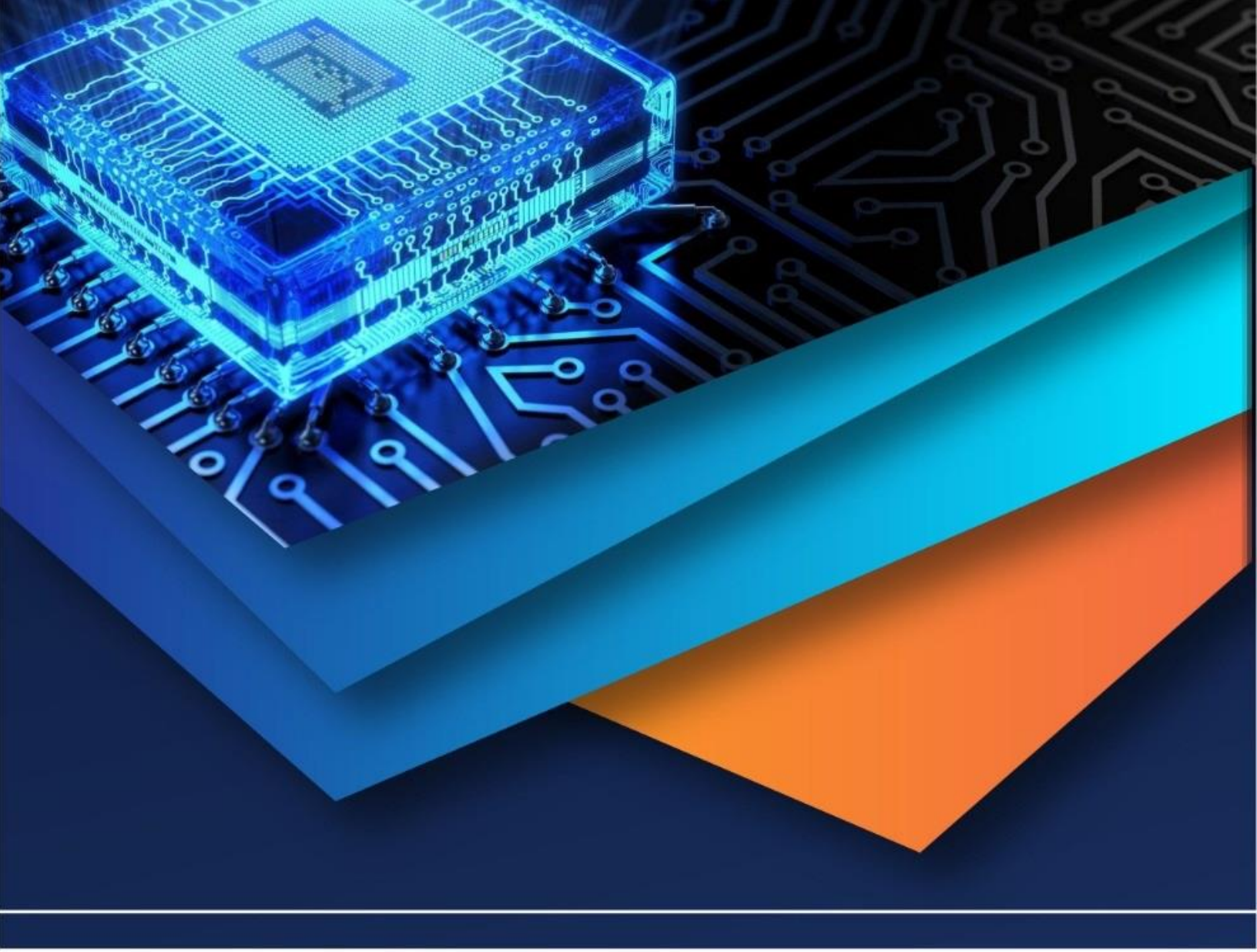
14. Insecure API Implementations Threaten Cloud http://www.darkreading.com/cloud-security/167901092/security/application-security/232900809/insecure-api-implementations-threaten-cloud.html

15. Web Services Single Sign-On Contains Big Flaws http://www.darkreading.com/authentication/167901072/security/news/232602844/web-services-single-sign-on-contain-big-flaws.html

16. Perfecting the unknown: Cloud Computing http://www.mysanantonio.com/business/article/Perfecting-the-Unknown-Cloud-Computing-4157844.php

17. New virtualization vulnerability allows escape to hypervisor attackshttp://www.informationweek.com/security/application-security/new-virtualization-vulnerability-allows/240001996

18.RadwareDDoSpedia
http://security.radware.com/knowledge-center/DDoSPedia/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY