iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IX **Month of publication:** September 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)

Security Information and Assurance in a Cloud Computing Environment

Swathi.K[1], Vijayanathan R[2]

[1]Associate Professor& Head, [2]Senior Librarian & Head,
[1]Department of Computer Science and Engineering, [2]Departments of Library and Information Science,
[1,2]Cauvery College of Engineering & Technology, Trichy, 639 103 (TN)

Abstract- Cloud computing is the use of computing resources that are delivered as a service over a network. Today, cloud computing generates a lot of excitement. It is both promising and daunting. Businesses world see its potential but also have many issues for discussion. Cloud computing offers attractive financial and technological advantages but some of them has not been fully evaluated with respect to security. Security is considered one of the most critical aspects in cloud computing due to the sensitivity and importance of data stored in the cloud. Cloud Computing has several major issues such as data security, trust, expectations, regulations, and performance. This paper discusses the privacy and security issue of cloud computing and some existing security solutions about Distributed Denial-of- Service (DDoS) attacks, Intrusion Detection Systems (IDSs), Antivirus (AV), and Email Security, suggested by some researchers.

I. INTRODUCTION

"CLOUD computing" implies access to isolated computing services suggested by third parties via a TCP/IP connection to the public internet. It is internet based development and use of computer technology. It is a method of computing in which resources are supplied "as a service" over the Internet to users who need not have information of, technology in, or control over the technology infrastructure that supports them.

Cloud computing is the next stage of an evolution of the internet. It provides everything from computing power to computing infrastructure, applications, business processes to personal collaboration. The cloud is a set of hardware, networks, storage, services and interfaces that enable the delivery of computing as a service. Economically, the main appeal of cloud computing is that the customer only use what they need, and only pay for what they actually use. Cloud computing utilizes servers housed in highly secure data centers for data storage and management, so organizations no longer need to purchase and look after their IT solutions in-house. In the world of cloud computing, the Vendors provide applications and enabling technology, infrastructure, hardware, and integration. The Partners to these vendors that are creating cloud services offerings and provide support services to customers and the business leaders, who are either use or evaluate various types of cloud computing offerings.

Public cloud, Private cloud and Hybrid cloud, which combine both public and private clouds are types of cloud computing.

- Public cloud: Public cloud provides scalable, dynamically provisioned, virtualized recourses available over the internet from an off-site third-party provider. Think Grid is a company that provides a multi-tenant architecture for supplying services such as Hosted Desktops. Other popular cloud vendors include Salesforce.com, Amazon EC2 and Flexi Scale.
- Private cloud: It is providing hosted services on the private networks. This type of cloud is used by large companies and allows their corporate network and data center administrators to effectively become in-house service providers.
- Hybrid cloud: It combines resources from both internal and external providers and so it becomes the most popular choice for enterprises. It is comprise of two or more than two clouds.

There are three service models in cloud computing as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).

- **Software-as-a-Service (SaaS):** This provides the customer with ready to use application running on the infrastructure of service provider. Salesforce,

IJRASET: ISSN: 2321-9653 Volume II, Issue IX, September 2014

ISSN: 2321-9653

DocLanding, Zozo, Workday are instances of SaaS are used for different purposes such as email, billing, human resource management etc.

- **Platform-as-a Service (PaaS):** It provides platform oriented service, controlling the installed applications and available hosting environment configuration. Google App Engine, LaodStorm are the instances of PaaS for running web applications and testing their performance.
- **Infrastructure–as-a-Service (IaaS):** It provides infrastructure services such as memory, CPU and storage. The customer can deploy and run software. Amazon S3 and Flexiscale are examples of IaaS for storage and maintaining virtual servers.

On-demand service, broad network access, resource pooling, rapid elasticity are good characteristic of cloud computing. Though the cloud computing is more promising and beneficial technology and also it is attracting the enterprises and organizations to move, it is facing various security issues as sensitive data access, privacy of data, authentication data segregation, identity management, policy integration, recovery, accountability, visibility under virtualization, malicious insiders, account control and multi-tenancy issues.

II. CLOUD SECURITY ISSUES

Cloud computing provides tremendous advantages to organizations of all sizes. For small businesses, cloud computing permits time-constrained IT groups to work additional with efficiency. For big enterprises, the cloud provides the flexibility to proportion or right down to respond quickly to dynamical market conditions. Businesses of all sizes will leverage the cloud to extend innovation and collaboration. Nonetheless several organizations are hesitant to totally leverage the advantages of the cloud, citing issues relating to data loss and unauthorized access, and are reluctant to rely on cloud suppliers to resolve these challenges.

A survey conducted by International Data Corporation (IDC) gives the strength of cloud computing to be implemented in IT industry and also gives the inspiration to cloud service providers. Figure 2.1 is the graphical representation of the survey which represents security as the most ranked according to IT executives. This survey was the contribution of the opinion of about 263 IT professionals regarding their views about cloud and it was observed that many of the executives are worried about security perspective of cloud.

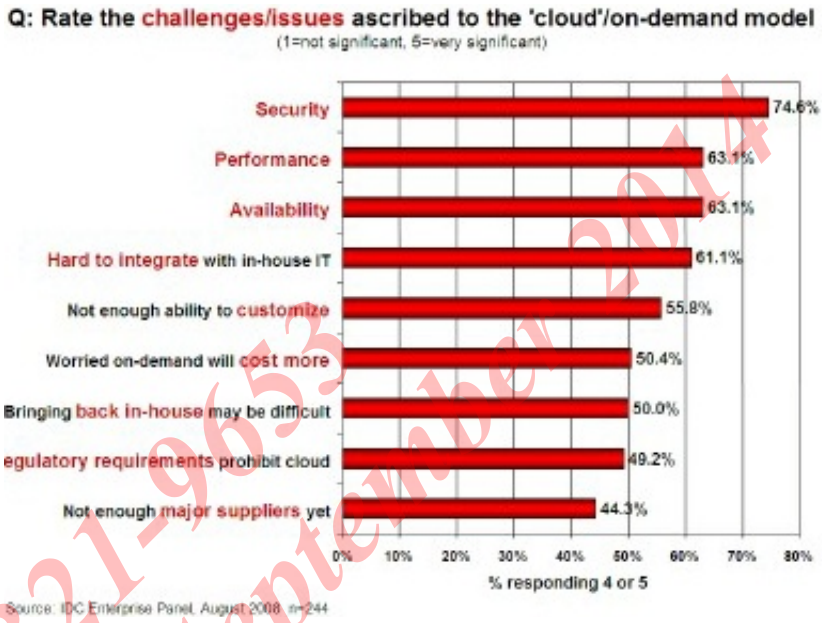


Fig. 2.1: Cloud Challenges/Issues survey [2].

Following are some major issues of cloud computing while its implementation.

a) Privacy

It related to storing and securing data, and monitoring the use of the cloud by the service providers. In the context privacy occur according to the cloud deployment model [3]. Privacy in Cloud computing include following issues:

Unauthorized Secondary Usage

- Lack of User Control
- Data Proliferation and Tran border Data Flow
- Dynamic Provisioning

b) Security

Cloud vendors are being facing issues in confidentiality, integrity and availability in data security. Cloud is expected to offer the capabilities like encryption strategies to ensure safe data storage environment, strict access control, secure and stable backup of user data. Some security issues in cloud computing is as follows:

1. Access
2. Availability and backup
3. Control over data life cycle
4. Multi-tenancy
5. Audit

IJRASET: ISSN: 2321-9653 Volume II, Issue IX, September 2014

c) Trust

Trust revolves around 'assurance' and confidence that people, data, entities, information or processes will function or behave in expected ways. At a deeper level, trust might be regarded as a consequence of progress towards security or privacy objectives [5]. Trust between the Service provider. and the customer is one of the main issues in cloud computing. There is no way for the customer to be sure whether the management of the Service is trustworthy, and whether there is any risk of insider attacks. This is a major issue and has received strong attention by companies [9]. The only legal document between the customer and service provider is the Service Level Agreement (SLA). This document contains all the agreements between the customer and the service provider; it contains what the service provider is doing and is willing to do [10]

III. TAXONOMY OF SECURITY ASPECTS WITHIN CLOUD COMPUTING SYSTEMS.

The taxonomy given in the figure 3.1 contains four classes as infrastructure, application and platform, administration, and compliance. It attracts on array of initial studies of cloud security problems prepared by Gartner [20] and therefore the Cloud Security Alliance [21].

The taxonomy shown in Figure 3.1 consist of four categories as infrastructure, application and platform, administration, and compliance and draws on a number of initial studies of cloud security issues prepared by Gartner[6] and the Cloud Security Alliance[7

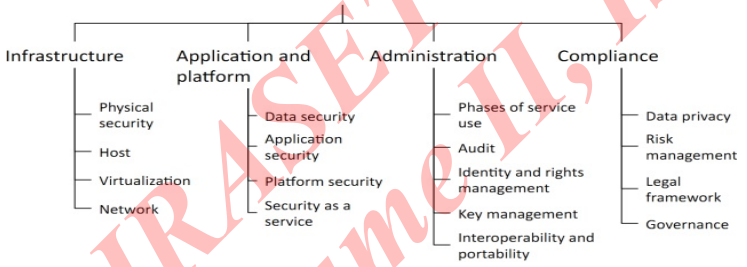


Fig. 3.1: Taxonomy of security aspects within cloud computing systems

This taxonomy specify a more detailed taxonomy of critical security areas in cloud computing. In a sense, taxonomy of cloud computing risks maps out the security critical aspects involved in procuring cloud services and may be regarded as the starting point for a deeper consideration of security issues [8].

- **Infrastructure**

The infrastructure area of the taxonomy concerns the threats to the security of services on the infrastructure layer. The infrastructure layer is divided into the four areas of physical security, host, virtualization and network which constitute the core components of the cloud infrastructure. Although users of a cloud infrastructure service do not usually have any influence on these core components, they should nonetheless be aware of the potential threats to security which exist at this level. The complexity of cloud infrastructures also makes it very difficult for users to evaluate their security and leaves them with little choice but to trust the cloud resource provider [22].

- **Application and platform**

The key risks affecting the application and platform part of the cloud taxonomy are those which can arise during the development and use of cloud services and which may have their origins both in the infrastructure and in the application provided as a service as well as the associated platform. Security aspects originating from service oriented architectures and web applications play an important role in securing data, applications and processes in cloud computing systems [22].

- **Administration**

The administration of cloud services presents one of the main challenges from a security perspective. This is still given too little support by cloud providers, let alone tools available to cloud users. These are still under development and aim at enabling cloud service users to manage their rented cloud services in an integrated and efficient way. The whole of this domain is still the subject of ongoing research and it is likely to take some time before the administration of cloud services is comparable to the level of quality achieved for other existing programs and tools in corporate networks [22].

- **Compliance**

The domain compliance brings together all the regulatory issues which may impact the protection goals. The legal framework of data protection laws and legal requirements of companies regarding data storage and processing in cloud computing systems are briefly discussed in the following. A risk management process is also discussed which can be used by cloud consumers to contain the risks involved in using cloud services. Important security guidelines, certificates and standards which a cloud vendor ought to have are also discussed in the context of governance. In general it is the case that compliance monitoring procedures for Internet based services such as cloud services must be extended if they are about to cover applications, users and activities in cloud computing systems effectively [22].

The infrastructure area of the taxonomy concerns the threats to the security of services on the infrastructure layer. The complexity of cloud infrastructures makes it very difficult for users to evaluate their security and leaves them with little choice but to trust the cloud resource provider. The key risks affecting the application and platform part of the cloud taxonomy are those

IJRASET: ISSN: 2321-9653 Volume II, Issue IX, September 2014

which can arise during the development and use of cloud services and which may have their origins both in the infrastructure and in the application provided as a service as well as the associated platform.

The administration of cloud services presents one of the main challenges from a security perspective. The domain compliance brings together all the regulatory issues which may impact the protection goals

3.1 Security Concerns

To provide effective security for a cloud environment, both the cloud provider and consumer must partner to provide solutions to the following security concerns:

- **Governance and Enterprise Risk Management:** The ability of an organization to govern and measure enterprise risk that is introduced by cloud computing. This concern includes items such as legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault.
- **Compliance and Audit:** Maintaining and proving compliance when using cloud computing. Issues involve evaluating how cloud computing affects compliance with internal security policies, and also various compliance requirements.
- **Application Security:** Securing application software that is running on or being developed in the cloud. This concern includes items such as whether it is appropriate to migrate or design an application to run in the cloud.
- **Encryption and Key Management:** Identifying proper encryption usage and scalable key management. This concern addresses access controls of both accesses to resources and for protecting data.
- **Identity and Access Management:** Managing identities and leveraging directory services to provide access control. The focus is on issues that are encountered when extending an organization's identity into the cloud.

IV. EXISTING CLOUD SOLUTIONS

Due to a general lack of interoperability standards, and the lack of sufficient market pressure for these standards, transitioning between cloud providers may be a painful manual process.

4.1 Recommended Solutions

Following are some recommended solution for all clouds and services.

- **All Cloud Solutions:**

i. Substituting cloud providers is in virtually all cases a negative business transaction for at least one party, which can cause an unexpected negative reaction from the legacy cloud provider.

ii. Understand the size of data sets hosted at a cloud provider. The sheer size of data may cause an interruption of service during a transition, or a longer transition period than anticipated. Many customers have found that using a courier to ship hard drives is faster than electronic transmission for large data sets.

iii. Document the security architecture and configuration of individual component security controls so they can be used to support internal audits, as well as to facilitate migration to new providers.

- **For IaaS Cloud Solutions:**

i. Understand how virtual machine images can be captured and ported to new cloud providers, who may use different virtualization technologies.

ii. Identify and eliminate (or at least document) any provider-specific extensions to the virtual machine environment.

iii. Understand what practices are in place to make sure appropriate deprivation of VM images occurs after an application is ported from the cloud provider.

iv. Understand the practices used for decommissioning of disks and storage devices.

v. Understand hardware/platform based dependencies that need to be identified before migration of the application/data.

vi. Ask for access to system logs, traces, and access and billing records from the legacy cloud provider.

vii. Identify options to resume or extend service with the legacy cloud provider in part or in whole if new service proves to be inferior.

viii. Determine if there are any management-level functions, interfaces, or APIs being used that are incompatible with or unimplemented by the new provider.

- **For PaaS Cloud Solutions:**

i. When possible, use platform components with a standard syntax, open APIs, and open standards.

ii. Understand what tools are available for secure data transfer, backup, and restore.

iii. Understand and document application components and modules specific to the PaaS provider, and develop

IJRASET: ISSN: 2321-9653 Volume II, Issue IX, September 2014

application architecture with layers of abstraction to minimize direct access to proprietary modules.

iv. Understand how base services like monitoring, logging, and auditing would transfer over to a new vendor.

v. Understand control functions provided by the legacy cloud provider and how they would translate to the new provider.

vi. When migrating to a new platform, understand the impacts on performance and availability of the application, and how these impacts will be measured.

• **For SaaS Solutions:**

vii. Perform regular data extractions and backups to a format that is usable without the SaaS provider.

viii. Understand whether metadata can be preserved and migrated.

ix. Understand that any custom tools being implemented will have to be redeveloped, or the new vendor must provide those tools.

x. Assure consistency of control effectiveness across old and new providers.

xi. Assure the possibility of migration of backups and other copies of logs, access records, and any

other pertinent information which may be required for legal and compliance reasons.

xii. Understand management, monitoring, and reporting interfaces and their integration between environments.

xiii. To find whether there is a provision for the new vendor to test and evaluate the applications before migration.

Also, some researchers have suggested cloud based security solutions related to distributed denial-of-service (DDoS) attacks, intrusion detection systems (IDSs), antivirus (AV), and email security.

4.1 Cloud Computing Security Overlay Network

Khaled Salah., et.al.,(2013) suggested cloud computing security overlay network. Such overlay networks were first used in the deployment of the Internet over telephone networks. They are virtual networks built on top of physical networks. They proposed and analyzed a cloud-based security overlay network that offers an integrated set of security service. Security systems designed to protect any virtual or physical machine using an overlay network. The collaboration among all these security systems can provide a robust computing.

4.2 Distributed Denial of Service Attack (DDoS)

This attack is the form of attack that an attacker aims to prevent legitimate users from accessing information or services. The common type of this attack occurs when an attacker floods a network with excessive requests to the target server until the server is unable to provide services to normal users [13][14].

Ping Du and Akijiro Nakao proposed the Cloud-Based Attack Defense (CLAD) architecture for preventing DDoS attacks against webservers. It is basically a distributed system that runs over a cloud infrastructure as a security overlay network to protect web servers using a set of smart collaborative and transparent Web proxies. CLAD is not yet available as a commercial product. Imperva Cloud DDos Protection Service(www.imperva.com/products/wsc_cloud-ddos-protection-service.html) is an analogous commercial cloud-based service that protects Web applications from DDoS attacks using an overlay

4.3 Intrusion Detection System (IDS)

Kleber Vieira and colleagues [14] proposed intrusion detection architecture suitable for grid and cloud computing environments in which audit data is collected from the cloud and two intrusion detection techniques are applied. Also, Sebastian Roschke and colleagues [15] proposed an extensible and distributed IDS architecture for cloud computing. This architecture involves several IDS sensors distributed across the cloud and a central management unit. Each protected endpoint is monitored by a separate sensor. Each sensor reports alerts to the central management unit, which gathers all sensor alerts and processes them. The design can detect attacks using the correlated alerts from different IDS sensors [11].

4.4 Antivirus

Wei Yan and Erik Wu [16] and Xufei Zheng and Yonghui Fang [17] proposed an automatic malware discovery system for providing AV software support using the cloud. They described a hybrid approach in which the client has a lightweight version of the malware signatures, and the central cloud-hosted AV service hosts the large database of signatures. A hybrid processing model is established between the desktop and the cloud AV services. Jon Oberheide and colleagues proposed CloudAV, an in-cloud architecture in which each host runs a process to detect executables entering a system, which are sent into the network for analysis, and then either executed or quarantined on the basis of the network service's threat report [13].

4.5 Email Security

McAfee Cloud Security helps organizations safely and confidently leverages secure cloud computing services and solutions. Rather than adopting the unique and sometimes unknown security practices and policies of each cloud vendor, McAfee Cloud Security allows businesses to extend and apply

IJRASET: ISSN: 2321-9653 Volume II, Issue IX, September 2014

their own access and security policies into the cloud by securing all the data traffic moving between the enterprise and the cloud, as well as data being stored in the cloud. McAfee SaaS Endpoint Protection is a commercial product providing a cloud-based AV service in which all the malware and viruses are intercepted in the cloud before they reach customers' mail servers. [18].

Nick Feamster [19] proposed a shift from home-based spam filtering to a cloud-based operation by third parties that have both operations expertise and a broader view of network activity. The Zscaler system [13] provides antispam services, among others, in the cloud. It uses a proxy to filter the network traffic into the cloud. McAfee SaaS Email Protection also provides a cloud-based email antispam solution [13].

V. CONCLUSION

In this paper we have discussed security issues of cloud computing and some existing cloud security solutions by some researchers. There are many more challenges about security aspect of cloud computing like virtualization. Though there are various solutions available for the challenges in cloud computing, stakes holders, vendors, enterprises and organizations have to think seriously about security aspect of cloud computing before adopting the cloud system.

REFERENCES

[1] Grobaur, B., Walloschek T., Stoker E., (2011). Understanding Cloud Computing Vulnerabilities. Security and Privacy. IEEE, Vol.9, pp 50.
[2] R. Kalaichelvi Chandrahasan,, S. Shanmuga Priya and Dr. L. Arokiam., "Research Challenges and Security Issues in Cloud Computing", International Journal of Computational Intelligence and Information Security, March 2012, Vol. 3, No. 3
[3] Kresimir P., Zeljko H. (2010). Cloud Computing Security and Challenges. MIPRO 2010, May 24-28, 2010
[4] Heiser, Jay and Mark Nicolett: Assessing the security risks of cloud computing. Technical Report G00157782, Gartner Research, June 2008.
[5] www.cloud-standards.org
[6] Cloud Computing Security Issues and Solutions, Published by JoshuaKissoon on Sat, 03/23/2013 - 02:22, Retrieved from http://cleverlogic.net/articles/cloud-computing-security-issues-and-solutions
[7] Vibha Sahu, Brajesh Dubey, Dr.S.M. Ghosh " Clouding Computing Threats", International Journal for Research in Applied Science and Engineering Technology (IJRASET), Volume 2 Issue 8, August 2014, Page No: 207-213
[8] Weis, J., & Alves-Foss, J., " Securing Database as a Service", IEEE Security

Author Biography:



Dr.K.Swathi obtained her under-graduation in B.E., (Computer Science & Engineering) from Bharathidasan University, Trichy in 1999. She obtained her M.E. degree in Computer and Communication Engineering from Anna University, Chennai in 2004.She obtained Ph.D degree in Faculty of Information & Communication Engineering from Anna University, Chennai in 2014. Presently, she is working as Associate Professor in Computer Science & Engineering, Cauvery College of Engineering and Technology, Trichy in 2008. She has 14 years teaching experience and also she had attended many workshops, seminars and conferences on Research issues in Image processing. She has published papers in international journals and presented papers in various Conferences. She is the life member of Indian Society for Technical Education (ISTE). Her areas of interest include Image processing, Data mining, network security and Software engineering.

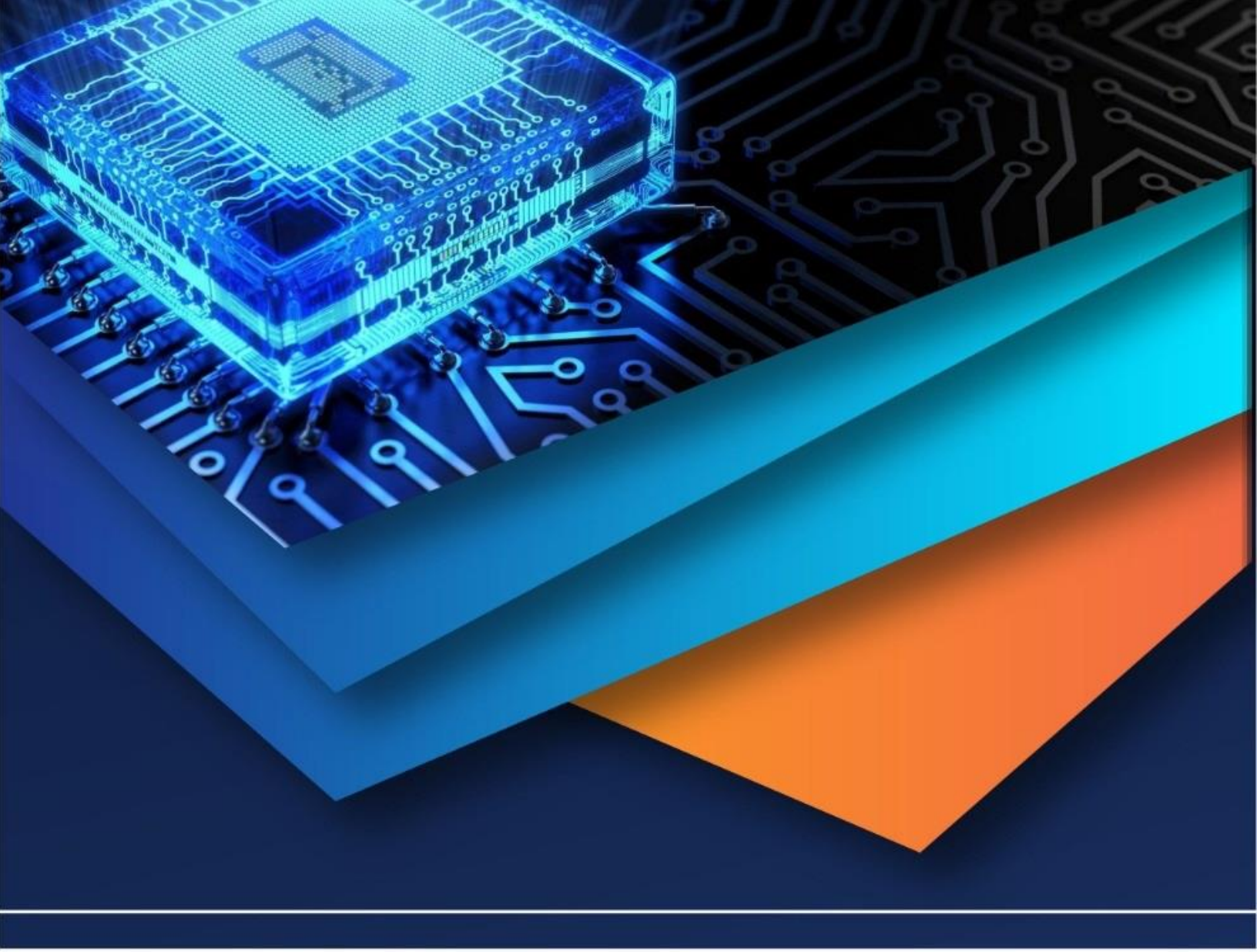
Corresponding Author



Vijayanathan.R. received his Master of philosophy Library and Information Science from Annamalai University in 1999 Also he obtained his post-graduate degree in Master of Economics in Bharathidasan University in 1996.He is working as a Sr. Librarian, Department of library and Information Science in Cauvery College of Engineering and technology, Trichy from 2009.

He has published 11 research papers in National and International journals. His areas of interested are networking; Cloud computing, IC Technologies, Environmental study, Library Automation, Webometric study, Scientometric study, Bibliometric analysis, and citation study.

IJRASET: ISSN: 2321-9653 Volume II, Issue IX, September 2014



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)