iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

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 XII December 2017- Available at www.ijraset.com

A Comprehensive review on Cloud Computing and Security Issues

Suvendu Kumar Nayak[1], P Annan Naidu[2]
[1, 2]*Centurion University, India.*

Abstract: Cloud computing means on demand delivery of IT resources via the Internet. It provides a solution of IT infrastructure in low cost. Cloud computing is a flexible infrastructure, Internet centric approach and ease of access. There are many organizations accepted cloud computing services in terms of storage, computation and IT services. In order to provide privacy preventing services to the individuals as well as organizations, cloud computing process should concerned about security issues. This paper presents brief idea about cloud computing and latest survey on security issues .
Keywords: Cloud Computing, Barriers to cloud adoption, Virtualization, Cloud Security, Multi-tenancy.

I. INTRODUCTION

Generally, IT companies follows traditional methods and supported requirements to provide IT infrastructure. Now a days IT companies preferred Cloud computing services to overcome the following requirements like server room, mail server, networking, firewalls, routers, modems, switches, high speed internet, configurable system, maintenance engineers and to reduce the IT infrastructure cost, Cloud Computing comes into existence.

According to the National Institute of Standards and Technology (NIST) definition, "The cloud computing is a model for enabling convenient, resource pooling, ubiquitous, on-demand access which can be easily delivered with different types of service provider interaction"[1]. The cloud computing follows simple "pay as you go" (PAYG) model, where you pay for the services you've used[2].

Cloud Computing characteristics includes High availability and reliability, Multi-Sharing, Device and Location Independence, On demand services, scalability, Services in pay-per-use mode. Cloud computing offers three models: Public cloud, Private cloud and hybrid cloud. Cloud computing also consists of the following actors such as cloud consumer, cloud provider, cloud auditor, cloud broker and clod carrier.

Cloud Computing implements virtualization technique or virtualized resources to provide effective services to end user. For example web services, virtualization and multi- tenancy. Cloud services are delivered to end users or customers through internet, web services(or applications) are used to manage cloud resource services that makes web service is one of the major component of cloud computing. The customers' processes are executed in virtualized environment that in turn utilize the physical resources. Multiple virtual processes of various users are allocated to same physical machines that are segregated logically [3].

A. Cloud Computing Infrastructure

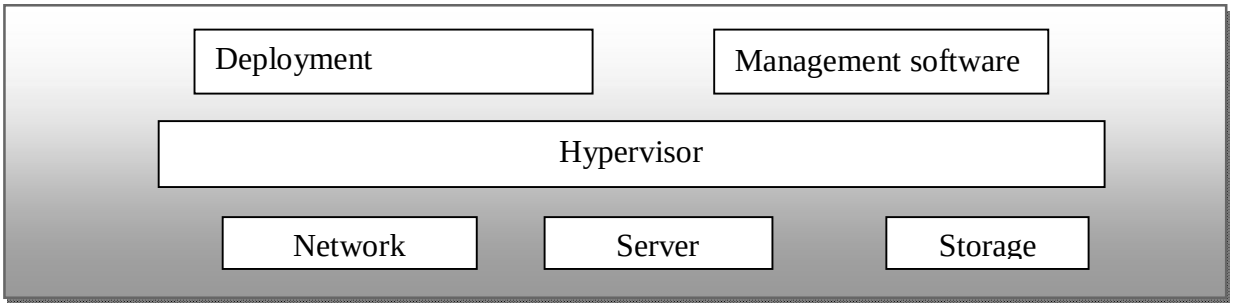


Fig-1

Hypervisor- It is a low-level program, It allows to share a single physical storage case between different occupants.
Deployment software- It is used for executes or deploys and integrate the application on cloud.
Management Software-It is used to maintain and configure the cloud infrastructure.

Network-It allows connecting the cloud services via the internet.
Server-helps to compute the resource sharing.
Storage- helps to storing files, distributed files, sharing, and accessing files.

Table-1: Evolution of Cloud Computing

Evolution of Computing	Year				
	1970-80	1990	2000	2010	2020
Centralized	Mainframe Technologies				
Distributed		Client-server distributed			
Internet			WWW		
Mobile				Transported Technologies	
Cloud/&Ubicomp					Ubiquitous computing/ Cloud computing

B. Statistics On Cloud Data Storage

Email remains the most common corporate information stored in the cloud (44%), followed by customer data (39%) and employee data (35%). Fewer organizations store intellectual property information (22%), financial corporate data (22%) or development data (22%) in the cloud.[15].

Fig-2 represents the above statistics .

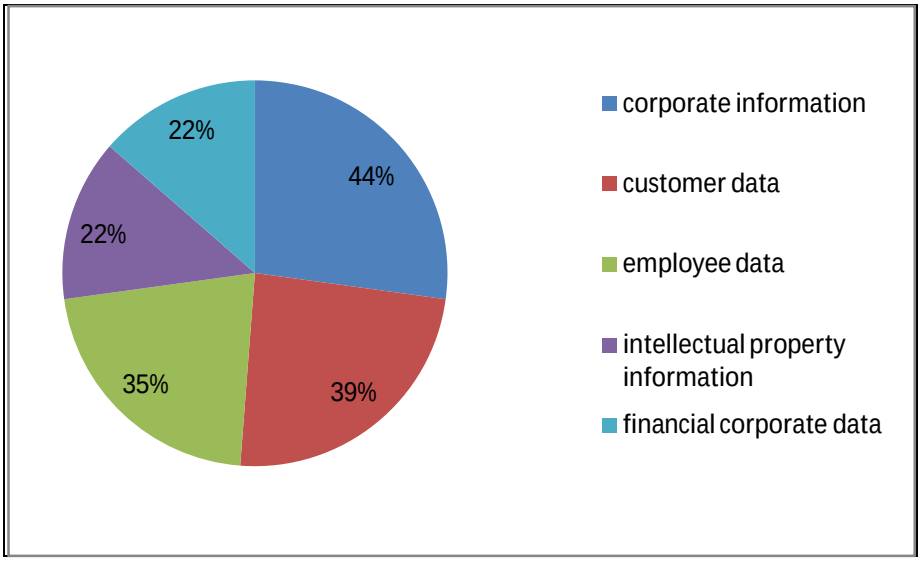


Fig-2

II. SURVEY ON SECURITY ISSUES

A. Key Survey Findings On Cloud Security

While cloud computing has become a mainstream delivery choice for applications, services and infrastructure, concerns about cloud security remain high. The top three cloud security concerns respondents need to address include protecting against data loss (57%), threats to data privacy (49%), and breaches of confidentiality (47%).[15]

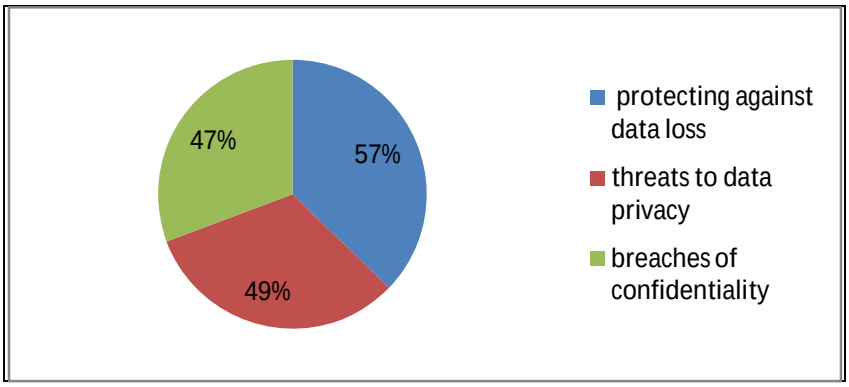


Fig-3

Moving to the cloud brings new security challenges that require new types of skills. To address these evolving security needs, 53% of organizations want to train and certify their current IT staff - by far the most popular approach. This is followed by partnering with a managed service provider (MSP) (30%), leveraging software solutions (27%) or hiring dedicated staff (26%).[15]

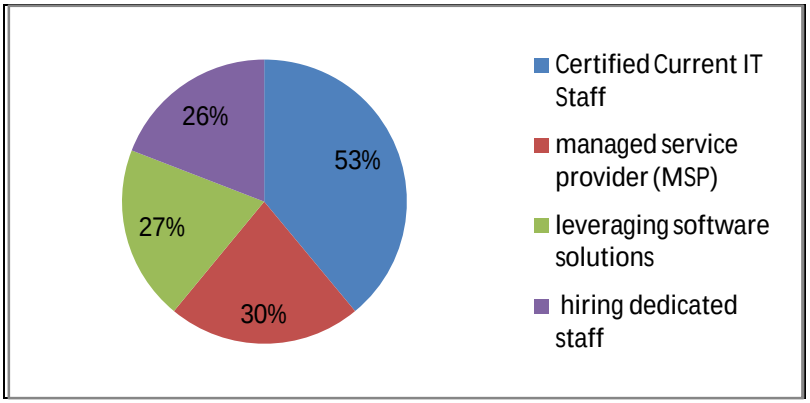


Fig-4

B. BarriersT Cloud Adoption

Cloud security risks still top the list of barriers to cloud adoption (33%). The most dramatic shift compared to the previous survey is the rise in the lack of staff and expertise to manage cloud security (28%) - moving from #5 to #2 and trading places with legal and regulatory concerns (24%) as key barriers to cloud adoption.[15]

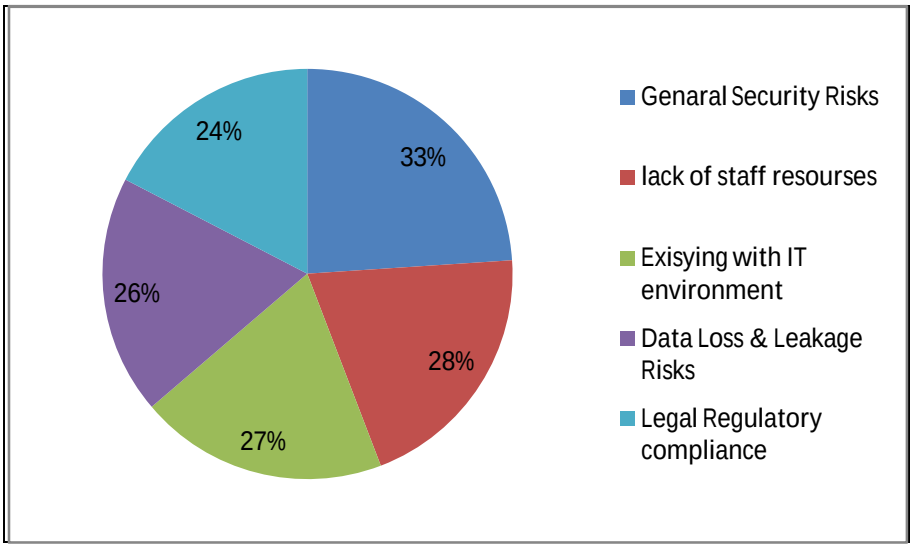


Fig-5

C. Various Security Issues

In spite of many benefits of the cloud , the security and privacy apprehension has been one of the critical issue which is preventing the popularity of this technology. Some CSPs private policy implies that the data which are in cloud can be randomly handled . As a result the owners data may be compromised with the privacy. Though the CSPs are taking utmost care to secure data hosted in the cloud by using firewalls and virtualization mechanism, but this measures does not guarantee full proof security due to poor deployment strategy and low degree of transparency.[4]

The Table-2 describes different categories of latest security issue .

Table-2

Risk due to nature of the cloud environment [4]	Risk of attacks due to cloud component[5]	Risk from Cloud storage[4]	Risk from cloud providers[16]
Outsourcing	Network based attacks	Due to chain of service provider	Malicious insider
Extensibility and Shared Responsibility	VM based attacks	Data scavenging	
Virtualization	eDDOS(economic Distributed Denial of Service)	Data deduplication	
Multi-tenancy		Improper media refinement	
Service Level Agreement			
Heterogeneity			

1) *Outsourcing :* Due to this nature the owner of the data lose control over it.
2) *Extensibility and Shared Responsibility:* The cloud service delivery model will create several security model with responsibility shared between customer and provider which leads to new security management challenge. There is a trade-offs to each model consumer extensibility and security.
3) *Virtualization:* The traditional security does not address security risk unique to virtualization like communication blind spots, inter VM attacks and mixed trust levels of VMs.
4) *Multi-tenancy:* This feature of cloud environment makes it less secure because the isolation of user data and setting cannot be assured.
5) *Service Level Agreement:* It is a binding contract between the cloud provider and customer. It outlines responsibilities of both side. A close monitoring is required to see whether SLA meets the requirement or not.
6) *Heterogeneity:* To maximize the performance and efficiency the heterogeneous cloud are created which gives integration challenges .
7) *Network based attacks:* Cloud platforms are now attractive targets for attackers. Some network based attacks are spam , port scanning , SQL injection and spoofing attacks. This kind of attacks degradeQoS of the provider.
8) *VM based attacks:* When a number of virtual machines are hosted on a system leads to several security threat.Some VM based attacks are cross VM side channel attack , VM creation attack ,VM migration attack and VM scheduler attack. .
9) *Eddos(economic Distributed Denial of Service) :*The DoS attack is a kind of attack where the attacker sends overwhelming of requests to server machine , as a result the machine is disabled to provide the requested service. But it in cloud computing environment the unlimited requests scales up the server automatically. Such type of requests are appear as legitimate to the user but actually these are fake requests . The cost will increase as the sever scales up automatically by fake requests . At some point of time your billing amount cross your ability to pay which leads to economic Distributed Denial of Service.
10) *Cloud storage security :*Very often one CSP takes the resource (storage) of another CSP with some agreement . In this case the outsourced file are more open to attacks. When the service provider break the relationship with its partner CSP then there may be chance that the users data is still lying in passive hard drives of even after the user account get deleted. An attacker can recover the data even if it is deleted from cloud storage. The file system do not delete the data entirely . The attackers are taking advantages of this weakness of the cloud platform.

Data deduplication provides low cost storage and better bandwidth utilization . In the other hand this method causes information leakage . The attacker can easily know about the existence of the file and its content.

Improper medi are finement brings greater risk to data . Cloud providers do not have many options for data sanitization for their customers.

11)Malicious insider: The damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers.

III. LITERATURE REVIEW ON CURRENT SECURITY ISSUES OF

Work	Focused Area	Proposed Scheme/Basic Theory	Major Components	Security Issues and Attacks	Recommended solutions
[5]	Security Issues, Security Threats	Automated Cloud Protection using intrusion detection and prevention systems	Cloud security Issues, comparative analysis of attacks	Yes	Yes
[6]	Security Issues, Security Threats and solutions	A Three-tier Security Achitcture: Application level, cloud service middleware level,Infrastructure level	Classification of Cloud computing security issues,Public cloud and private cloud Security issues,	Yes	Yes
[7]	Security issues in service delivery models	survey of different Security Risks	Security issues in SaaS, IaaS, PaaS	Yes	Yes
[8]	Data Security and solutions in cloud computing	Survey of different Security challenges	Models of Cloud Computing,Data Security challenges	NO	Yes
[9]	seurity and privacy for cloud storage and computaion	Proposed a secure protocol i.eSecCloud	Model the security problems in cloud computing,SecCloudprotoclos, performance and analysis	Yes	Yes
[10]	Security in cloud computing	challenges at communication level and its solutions	Cloud Computing architectural frame work,cloud security challenges	Yes	Yes
[11]	security challenges and solutions	Case study on Amazon Web services	cloud computing model, security in cloud	Yes	NO
[12]	cloud computing security	Approaches to achieve confidentiality from cloud provider	Core problems of Cloud computing security	Yes	Yes

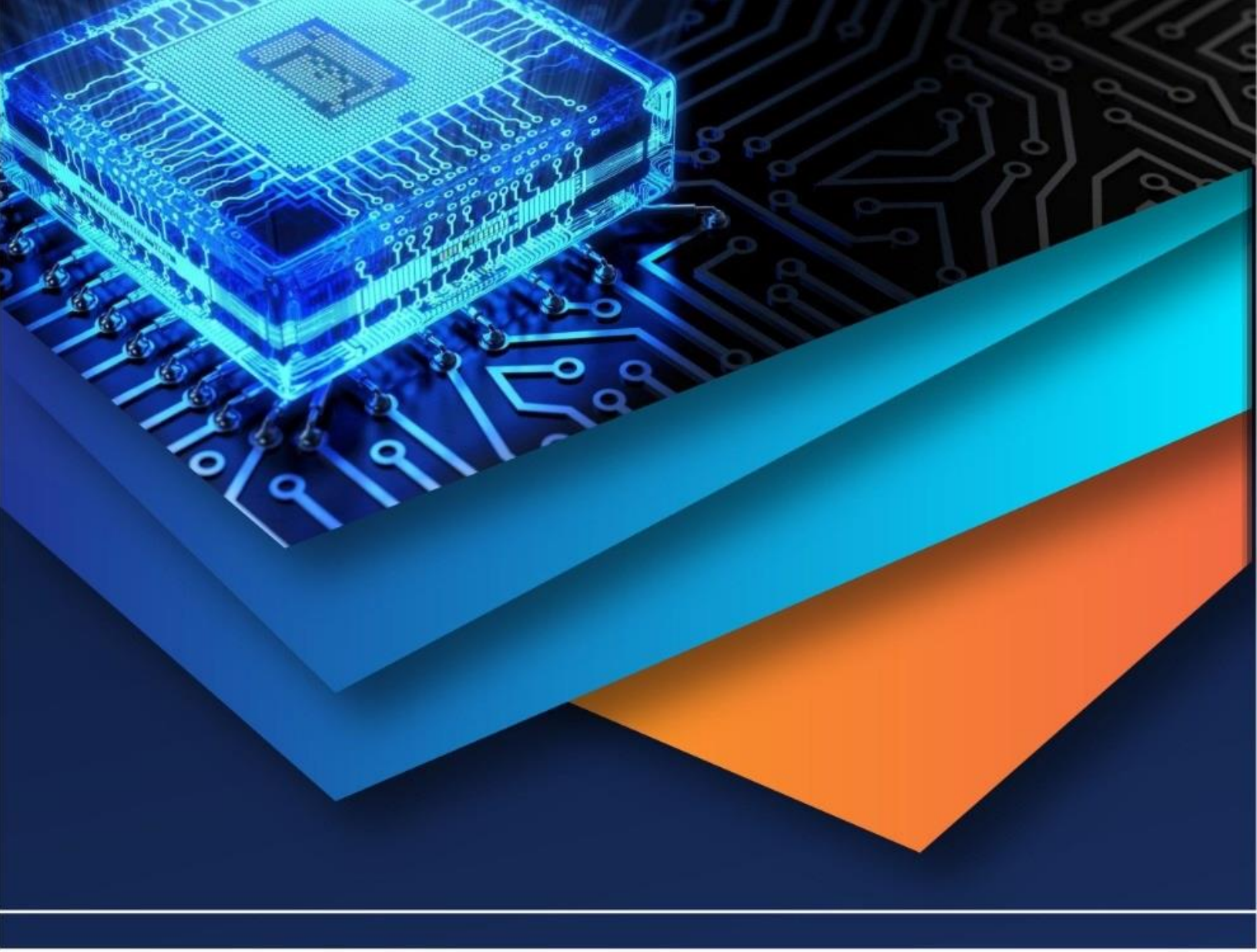
[13]	Security models and strategies of cloud computing	Common security issues of cloud computing	Security models and security strategies of cloud computing	Yes	Yes
[14]	security challenges in cloud computing	service level agreements(SLA) for cloud security	cloud computing classification, a framework for security method for cloud SLAs	Yes	NO

IV. CONCLUSION

In this paper we have described about the advantageous of cloud platform , statistics on different sources of cloud data and the barrier to popularity of cloud adoption. This paper also includes various latest issues in cloud computing. The stated issues are nicely categories depending upon the nature of the cloud environment , cloud components , cloud storage and CSP. An extensive literature review conducted on current security issues . The readers are encouraged to do categorical analysis of the stated security issue and may come up with preventive measures.

REFERENCES

[1] Zissis, Dimitrios, Lekkas, Dimitrios, 2012. Addressing cloud computing security is-sues. Future Gener. Comput. Syst. 28 (3), 583–592.
[2] S. Subashinin , V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications 34 (2011) 1–11.
[3] Mazhar Ali, Samee U. Khan, Security in cloud computing: Opportunities and challenges,Information Sciences 305 (2015) 357–383,journal home page: www.elsevier.com/locate/ins.
[4] The 6th International Symposium on Applications of Ad hoc and Sensor Networks(AASNET'14)State-of-the-art Survey on Cloud Computing Security Challenges,Approaches and SolutionsFarrukhShahzadaaKing Fahd University of Petroleum and Minerals, Dhahran, KSA.
[5] Minhaj Ahmad Khan,A survey of security issues for cloudcomputing,Journal of Network and Computer Applications 71 (2016) 11-29.
[6] Saurabh Singh, A survey on cloud computing security: Issues, threats, and solutions, Journal of Network and Computer Applications 75 (2016) 200–222.
[7] S. Subashini , V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications 34 (2011) 1–11.
[8] R. VelumadhavaRao, K. Selvamanib, Data Security Challenges and Its Solutions in Cloud Computing, Procedia Computer Science 48 (2015) 204 – 209 ,ICCC-2015.
[9] Lifei Wei, Haojin Zhu, Security and privacy for storage and computation in cloud computing, Information Sciences 258 (2014) 371–386.
[10]Mazhar Ali, Samee U. Khan, Security in cloud computing: Opportunities and challenges, Information Sciences 305 (2015) 357–383.
[11]FarrukhShahzad, State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions, Procedia Computer Science 37 (2014) 357 – 362.
[12]Mark D. Ryan, Cloud computing security: The scientific challenge, and a survey of solutions, The Journal of Systems and Software 86 (2013) 2263–2268.
[13]JianhuaChea, YaminDuan, Study on the security models and strategies of cloud computing, 2011 International Conference on Power Electronics and Engineering Application, Procedia Engineering 23 (2011) 586 – 593.
[14]ChunmingRong , Son T. Nguyen, Beyond lightning: A survey on security challenges in cloud computing, Computers and Electrical Engineering 39 (2013) 47–54.
[15]https://www.cloudvisory.com/assets/Cloud_Security_Report_Cloudvisory.pd
[16] http://www.enisa.europa.eu



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY