iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 7 **Issue:** III **Month of publication:** March 2019

**DOI:** http://doi.org/10.22214/ijraset.2019.3017

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 7 Issue III, Mar 2019- Available at www.ijraset.com*

# Role of IT Audits in Enterprises Cloud Computing

Avneet Kaur Bagga[1], Ankita Dev[2]
[1, 2]*Symbiosis Institute of Computer Science and Research*

***Abstract: In the past few years, we have seen cloud computing evolving to change the traditional way of doing IT business across the globe. Many companies left their in-house data centre work culture and adapted cloud services which resulted them in terms of cost benefit. However, deploying cloud computing in an enterprise infrastructure also brought concerns related to security of their data.***
***The auditing procedure should maintain 1) Confidentiality, 2) Dynamic Auditing, 3) Batch Auditing.***
***In this research we tried to understand what auditing is and how much is it required for enterprise cloud computing.***
***Keywords: cloud computing, auditing, IT, AWS, cloud service***

*Objectives*
*1)* To know how IT audit plays role in enterprise cloud computing
*2)* To understand auditing
*3)* To explore what is to be done while auditing
*4)* To identify how industry is adapting cloud computing

## I. INTRODUCTION

Cloud computing is a medium to deliver IT services where the resources being utilized are retrieved from the internet. Few years back, cloud computing was a huge shift towards modern technology, where instead of maintaining a proprietary hard drive or local storage device, cloud-based storage made it possible to save them in a remote database. Cloud computing facilities like storage, computation and application by pay as per usage through Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) cloud
service models are in demand which is being provided by big IT giants like Google, Amazon, Salesforce etc. [1]

For, why companies prefer cloud -
*1)* cloud computing saves enterprise's time and money at a large scale
*2)* cloud providers are able to recognize the trend and constantly develop solutions accordingly
*3)* cloud provider's virtual servers are combined with SAN that allows for improved protection against disasters
*4)* Dedicated hardware increases security along with flexibility

Thus, this market is being forecasted to reach $411bn by 2020 according to the new research from global communications provider CenturyLink and Statista. [3].

## II. OUR FINDINGS

For our research, primarily we surveyed for responses from industrial experts to know the percentage of companies using cloud services, and which of the 5 types- public, hybrid, private in-house, private offshore, community cloud and how important is auditing for their cloud services. The below data in Fig-1 refers the companies who are using cloud services.

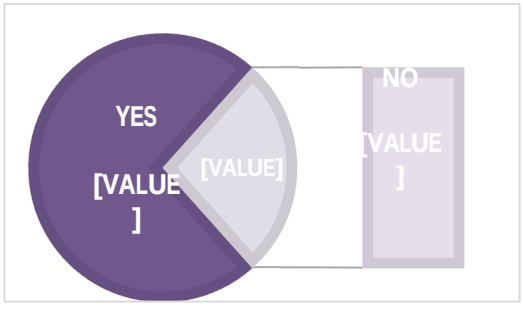



Fig 1

As per our analysis, 73.2% of companies prefer to use private cloud services where the crucial data is deployed in 'private in-house' cloud as charted in Fig 2, in order to meet the quality standard of maintaining security of their data (elaborated in Fig 3)

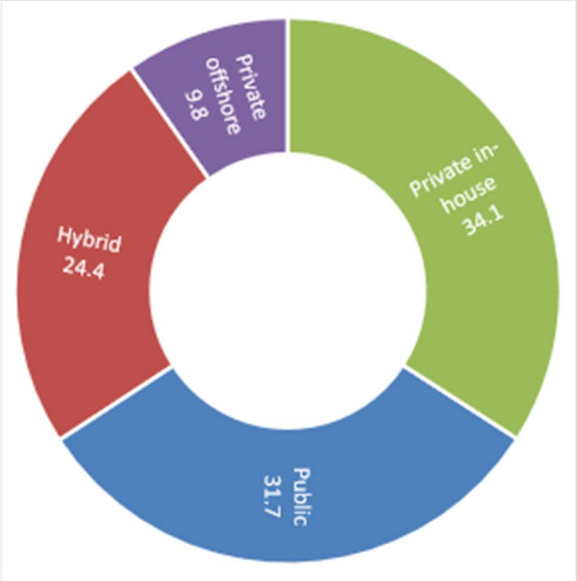



Fig 2

## III. LITERATURE REVIEW

While trying to analyse how enterprise cloud computing are being adapted in the industry, we found the maximum service being availed is of SaaS (in Fig 3) as compared to the rest and most of the organizations.

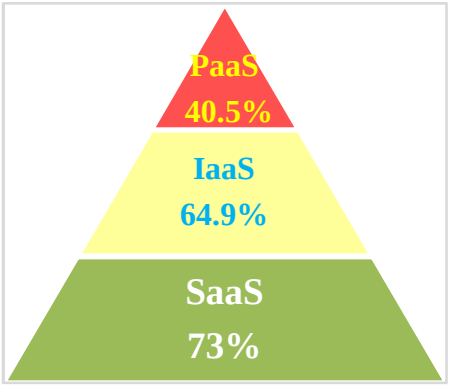



Fig 3

Along with this, we also figured out that Amazon's Cloud service leads the market with 17% of preferability over Azure and 25% preferability than GCP.

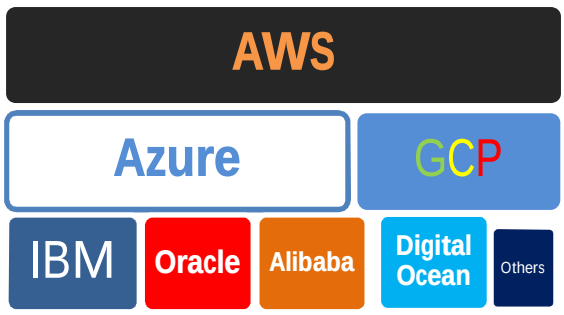



Fig 4 Most leading choice to least

However, during deep research as to why companies choose Amazon over Azure or any other, industrialists responded towards 1) Security 2) Scalability & Flexibility as their major reason.

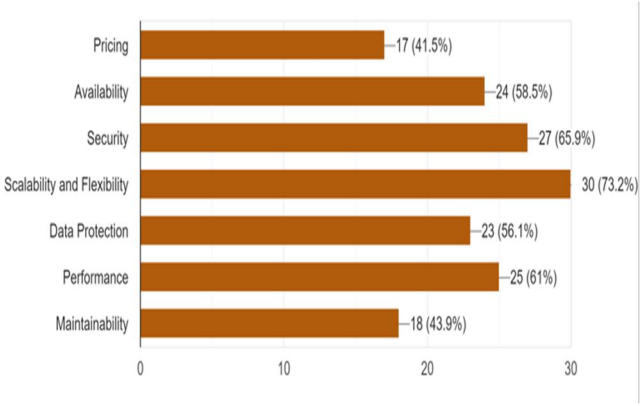



Fig 5

*A. Security*

Whether IT industry or not, security has always been a concern to every business since ages.

With the cloud computing services like the data being outsourced for a hassle-free storage management, it also brought the Security concerns like authorization and authentication, data confidentiality, integrity, privacy etc. With increasing popularity of enterprise cloud computing and its pubic connectivity via internet it is the next frontier for viruses, hackers and cyber – criminals to Start breaching and attacking. It was earlier predicted that cloud computing adoption rate will fly high in time and cloud computing vulnerability to viruses, hackers and cyber-attacks will increase because organized hackers, and hostile nations would see this as a new frontier to try to steal private information, disrupt services and cause harm to the enterprise cloud computing network.

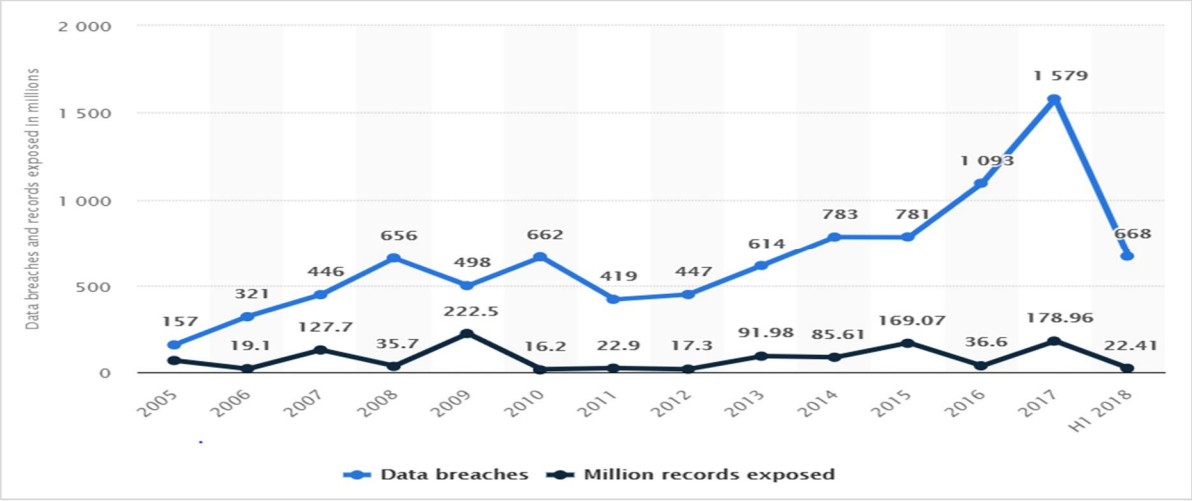



Fig 6 Statistics of security breeching

Cloud computing security risk incident has happened when Google a major cloud computing and Software as a Service (SaaS) provider had its systems attacked and hacked; the cyber-forensics has been traced to the attacks coming from China (Markoff, Barboza, 2010). [4]

*B. Auditing*

Understanding the security threats that's

can harm any business since their customer data or applications are placed on remote servers, the cloud service provider's need to adhere to some measures in order to alleviate the security threats. Audit can be considered as the process of collecting and assessing evidence to determine whether a computer system guards the asset, maintains the data integrity, allows organizational goals to be achieved effectively and uses resources efficiently. [5]

Therefore, auditing of Information Technology was coined to measure the adherence of mitigation against security.
In order to understand the role of IT audit, at first, we identified the objectives of IT audits from multiple Audit manuals. (Fig 7)

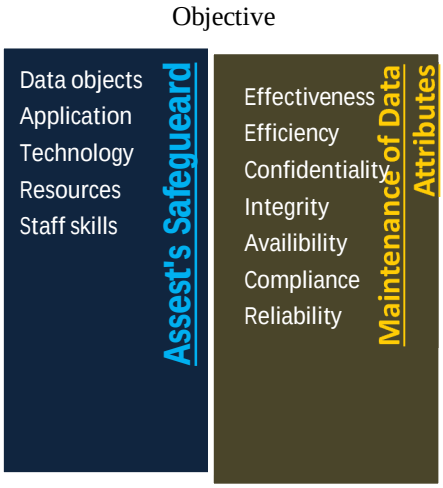



Fig 7

1) *What phases does Audit include?:* Since it is an activity which is to be performed for IT industry or not, in-order to measure the adherence towards regulations, security, integrity etc, this process also needs to obey the stages which are –


Fig 8

*a)* *Planning*: Although planning is an iterative process as the result of initial assessments provide the source for determining the extent and type of subsequent testing, it is done at the very beginning.
*b)* *Definition Of Audit's Objective And Scope*: Audit's objective could cover one or more area among the below listed points-
*i)* Review of the controls of the IT systems to gain assurance about their adequacy and effectiveness.
*ii)* Evaluation of the performance of a system or a specific programme.
*iii)* Review of the security of the IT systems.
*iv)* Examine the system development process and the procedures followed at various stages involved therein.
*v)* *Scope*: Scope defines the boundaries of the audit
*c)* *Collection And Evaluation Of Evidences*: When planning the IT audit activity, the auditor should take into consideration the 1) type of the evidence to be gathered, 2) it uses as audit evidence to meet audit objectives and its varying levels of reliability.
*d)* *Documentation and Reporting*: At last the auditors responsibility is to also document the audit evidences. [5]

2) *Types of Auditing:* There are of 2 types of auditing that has been adapted by the industry – Internal Auditing and External Auditing.

a) *Internal Auditing:* In this type of audit the company (customer to the cloud vendor) themselves conduct a series of checks by a close examination of conformance to the internal services. E.g.: Quality Management Group.

b) *External Audits:* These are audits which are conducted by external parties on the services being provided by the vendors. They can be of 2 sub categories – Cloud Security Alliance (CSA) Cloud control Matrix (CCM) has been designed to provide security principles to assess the overall security risk of any cloud provider which are listed below –

c) *Service Provider Audit:* In this case the company as a customer appoints a representative from its organization to audit the supplier for conformance.

d) *3rd Party Audit:* In this case the company appoints a 3rd party who is authorized to audit the service provider for conformance.

Also, we found few standards and options for auditing listed by AICPA in figure 10

3) *What should the role of audit be in your organization?*

a) Proactive trusted advisor/partner.

b) Proactively identify risks to be mitigated in order to optimize the benefits of the outsourcing relationship.

c) Internal Audit does not get involved with the move until it is time to audit

d) Advise on the costs savings that would be realized by a reduction of audits overall security risk of any cloud provider which are listed below

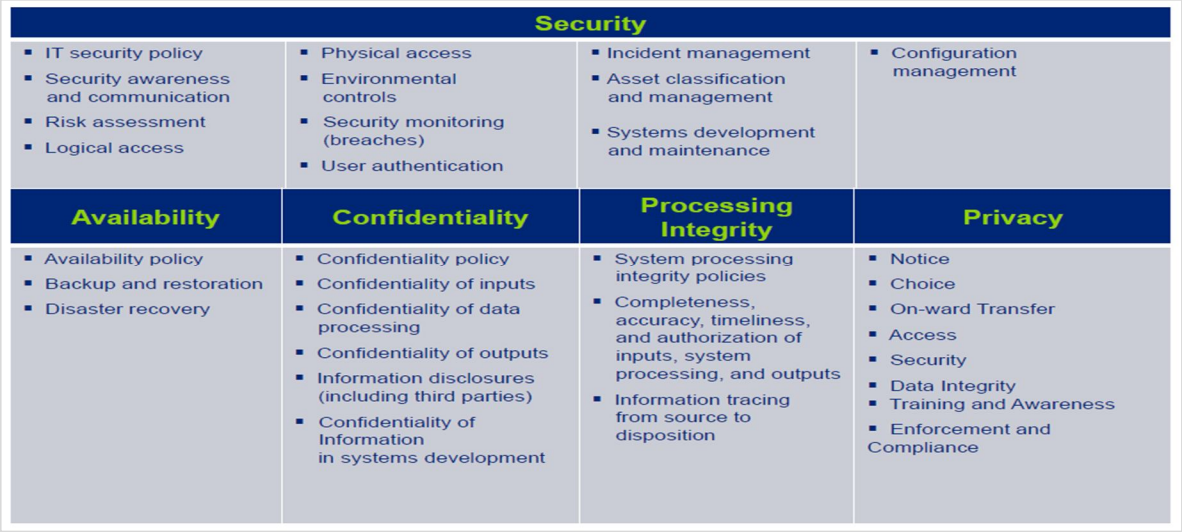



Fig 9

e) Application & Interface Security

i) Audit Assurance & Compliance

ii) Business Continuity Management & Operational Resilience

iii) Change Control & Configuration Management

iv) Data Security & Information Lifecycle Management

v) Data center Security

vi) Encryption & Key Management

vii) Governance and Risk Management

viii) Human Resources

ix) Identity & Access Management

x) Infrastructure & Virtualization Security

xi) Interoperability & Portability

xii) Mobile Security

xiii) Security Incident Management, E-Discovery & Cloud Forensics

xiv) Supply Chain Management, Transparency and Accountability

xv) Threat and Vulnerability Management [7]

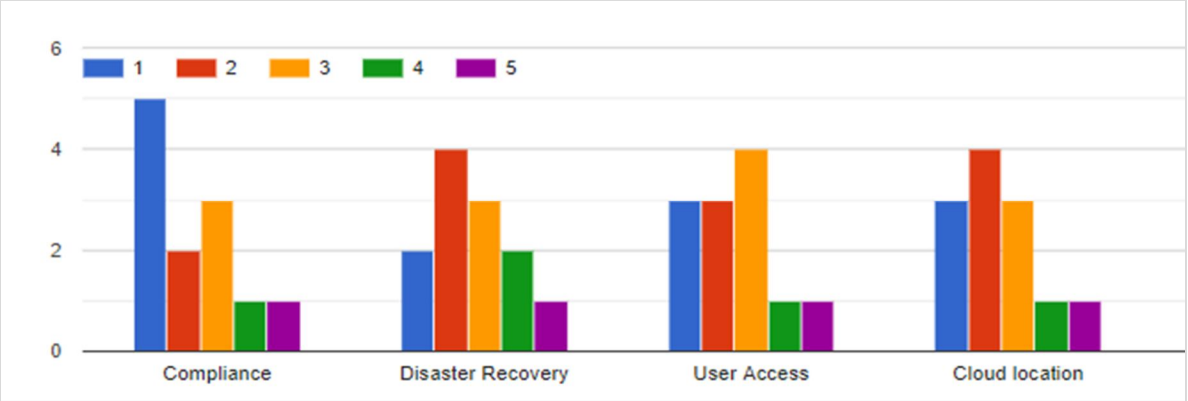



Fig 10 On scale of 1-5 what companies prefer

*4) What auditing Includes?* As auditing is the process of conducting an official inspection, auditors need to inspect against few parameters or best said as standards. There are a set of certain and many checkpoints an auditor has to evaluate cloud computing in order to adhere to the nitty-gritty of assurance against frauds. In [10] Ministry of Electronics & Information Technology, has defined list of parameters for auditing the cloud service providers.

In [5], Zhixiong Chen and John Yoon also have listed few of the headers (mentioned below) for auditors to refer while auditing for SaaS and IaaS service model as they are the most availed services for Public, Private, Community cloud.

Proposed Checklists by Chen and Yoon

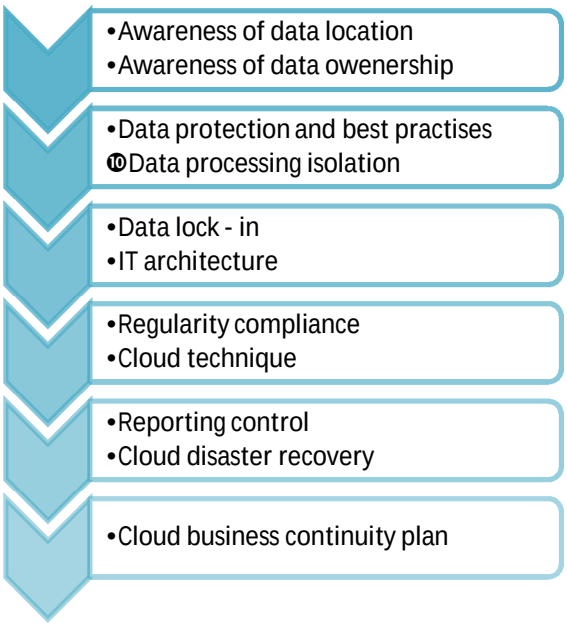



Fig 11

It also includes other checkpoints with respect to the aspects of auditing where the service providers are inspected on

*a)* Standards: This part of audit is to understand the conformance to the applied standard itself.E.g.: Is ISO 9001 being followed by the service provider!

*b)* System: The audit checks for application of the theoretical concepts of quality standards in the organization. E.g.: Is document control under place! Are the right tools being used!

*c)* Process: This area of audit should check for the final execution of the steps in the project itself. E.g.: Are the steps identified in ISO 9001 documentation being executed!

*d)* Product or service: In the final part of audit the check has to be made if the product or service is as per expected measurements of quality. E.g.: Does the product match to all feature requirements!

Some of the standards, frameworks and guidelines that is being used while auditing security include:

*i)* ISO 27001/27002 standards
*ii)* Control Objectives for Information and Technology (COBIT) framework
*iii)* ISACA's IT Assurance Framework (ITAF)
*iv)* IT Audit and Assurance Guidelines
***v)*** SysTrust and WebTrust frameworks [8]

## IV. IT AUDIT IN CLOUD COMPUTING WITH INDUSTRIAL CASE

Pinal County's risk existence in IT Disaster recovery

What was identified: It was found that a defined and repeatable Disaster Recovery Program is not in place for Pinal County by the Pinal County's IT department

How it was identified: As a part of the Pinal County FY2016 Audit Plan, Internal Audit performed a Disaster Recovery audit.

**A.** A formal DR program has not been formally defined and aligned with a leading Business Continuity or DR framework. Specifically, Pinal County does not have a repeatable process and / or controls to better manage DR efforts:

- A DR policy, based on a leading framework, has not been developed to outline the DR lifecycle, objectives, roles and responsibilities.
- A process to align strategic Pinal County objectives with IT DR objectives.
- A repeatable IT risk assessment that investigates factors such as environmental, regulatory, and compliance risks associated with DR, and geographic scope of disruptions.
- Application and system Recovery Time Objectives were not created in collaboration with the IT customer.
- Application and system Recovery Point Objective requirements have not been formally defined; however, the IT department has set an RPO of 24 hours.
- The IT department's Contingency of Operations Plan (COOP) has not been updated since 2010.
- Notification procedures and formal DR communication methodologies do not exist.
- Comprehensive DR testing does not occur on a consistent and repeatable basis.
- DR roles and responsibilities are inherently understood but not defined.
- Formal DR training has not been defined or provided to stakeholders.
- A process for on-going DR plan and program maintenance does not exist.

Fig 12 Improvement opportunities that were identified during Auditing [11]

## V. CONCLUSIONS

Auditing cloud computing is like auditing new IT—understand the IT, identify the risks, evaluate mitigating controls and audit the risky objects.

The understanding and risk assessment can be improved with a good outline to think about the IT and risks and, thus, assist the IT auditor in conducting an effectual risk assessment.

Also, as an IT auditor, it is likewise their responsibility to be updated of the trending technology and to maintain updated checkpoints for inspecting, be it for the cloud provider or any organization.

## VI. RECOMMENDATION

ISACA (Information Systems Audit and Control Association) has listed the area to focus on cloud computing Audits.

*A. Planning*

*1)* Define the audit/assurance objectives
*2)* 1.2 Define the boundaries of review
*3)* 1.3 Identify and document risks
*4)* 1.4 Define the change process
*5)* 1.5 Define assignment success
*6)* 1.6 Define the audit/assurance resources required
*7)* 1.7 Define deliverables
*8)* 1.8 Communications

*B. Governing the cloud*

*1)* 2.1 Governance and Enterprise Risk Management (ERM)
*2)* 2.2 Legal and Electronic Discovery
*3)* 2.3 Portability and Interoperability

*C. Operating in the cloud*

*1)* 3.1 Incident Response, Notification and Remediation
*2)* 3.2 Application Security
*3)* 3.3 Data Security and Integrity
*4)* 3.4 Identity and Access Management
*5)* 3.5 Virtualization

Below the *Use and Benefits* of using ISACA is listed as stated by Deloitte

*1)* Tools along with templates to be used as a roadmap for Cloud audits
*2)* Provide stakeholders with an assessment of the effectiveness of the cloud computing service provider's internal controls and security
*3)* Identify internal control deficiencies within the customer organization and its interface with the service provider
*4)* Provide audit stakeholders with an assessment of the quality of and their ability to rely upon the service provider's attestations regarding internal controls. [7]

## VII. ACKNOWLEDGEMENT

This work has been supported under the guidance by Mr. Supratik Ghatak, Professor in Symbiosis Institute of Computer Science and Research.

## REFERENCES

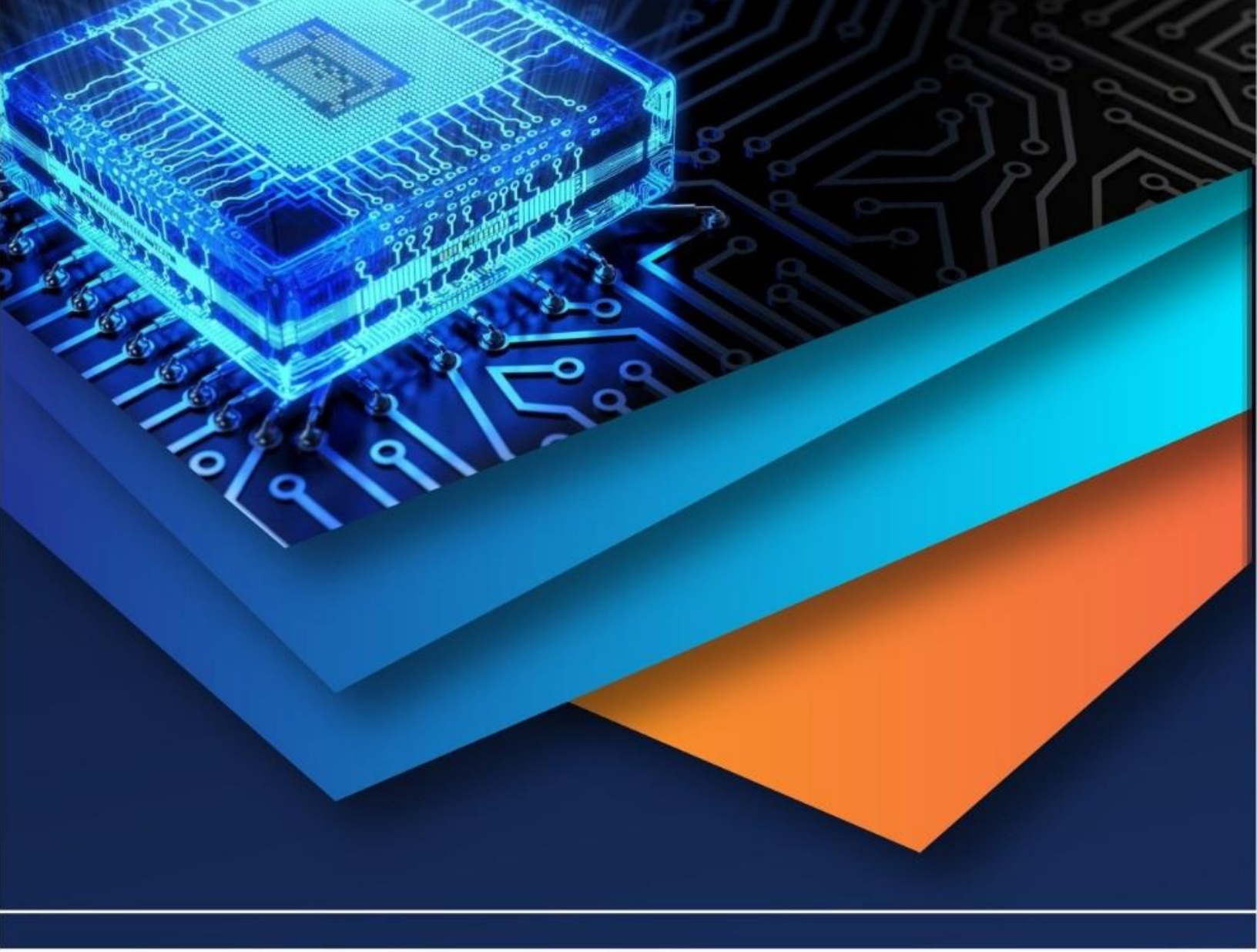
[1] Cloud Computing Security Auditing, Irfan Gul, M Hasan Islam, January 2011 [1]
[2] Gleeson, E. 2009. Computing industry set for a shocking change. Retrieved January 10, 2010 from http://www.moneyweek.com/investment-advice/computing-industry-set-for-a-shocking-change-43226.aspx
[3] Anthony Spadafora , Cloud computing market worth $411 billion by 2020 Retrieved August 21, 2018 https://www.itproportal.com/news/cloud-computing-market-worth-dollar411-billion-by-2020/ [3]
[4] An overview of the security concerns in enterprise cloud computing, Anthony Bisong1 and Syed (Shawon) M. Rahman, Vol.3, No.1, January 2011 [4]
[5] IT Audit Manual, http://www.al.undp.org/content/dam/albania/docs/STAR/IT%20AUDIT%20MANUAL.pdf [5]
[6] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of breaches-and-records-exposed/
[7] Cloud Computing –What Auditors need to know, Deloitte
[8] https://www.oreilly.com/library/view/auditing-cloud-computing/9781118116043/a01.html
[9] https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118269091.app1
[10] https://meity.gov.in/writereaddata/files/CSP-01-07%20-%20Audit%20Report.pdf Pinal County IT Disaster Recovery Internal Audit Report – may 5, 2016
[11] http://www.pinalcountyaz.gov/InternalAudit/FYReports/Pinal%20County%20IT%20Disaster%20Recovery%20Internal%20Audit%20Report%20-%20May%202016.pdf

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 7 Issue III, Mar 2019- Available at www.ijraset.com*

**AUTHORS**

Ankita Dev, has worked with Cognizant for 2 years and is now pursuing MBA-IT from Symbiosis Institute of Computer Science and Research
She has completed her bachelor's from Jawaharlal Nehru Architecture and Fine arts university.
LinkedIn- - https://www.linkedin.com/in/ankita-dev-02a873114/

Avneet Kaur Bagga, has completed her bachelor's from Maeer's Arts commerce science college pune.
Pursuing MBA-IT from Symbiosis Institute of Computer Science and Research,
LinkedIn – https://www.linkedin.com/in/avneetkaur-bagga-a371ba178



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY