The Risks, Threats and Vulnerabilities in Moving to the Cloud

[1]Poornachandra C M, [2]Dr. Vijayalakshmi M N

[1]Student, [2]Associate Professor,
[1]Master of Computer Applications,
[1]RV College of Engineering®, Bengaluru, India.

Abstract: Cloud computing is the availability of computer system resources on-demand, like data storage, and computing power, which does not require any direct user interaction. Cloud computing has various benefits, starting with potentially lower cost (more capabilities in the public cloud which helps in productivity and more limited capabilities in the private cloud) and faster time. To revolutionize the digital transformations companies are rapidly using the cloud. Organizations expose themselves to a myriad of commercial, financial, technical, legal, and compliance risks, that adopt cloud technologies or chooses the cloud service providers (CSP) and services or applications without becoming fully informed of the risks involved. Cloud infrastructure can be complex, and everyone knows that complexity is the enemy of security. Organizations can also make grave errors and expose critical data and systems, while most cloud security experts agree that companies can benefit from the security solutions built into the cloud. Data security is amongst the key concerns holding back enterprises from adopting cloud solutions, with the array of benefits that the cloud offers. As a supportive statement, a survey found that 93% of companies are moderate to extremely concerned about cloud computing security risks.

IndexTerms **– Cloud Computing, Cloud Service Providers, Security, Data Security.**

I. INTRODUCTION

Cloud computing technology, also popularly referred to as the cloud, has redefined the way information is stored and shared. It has helped transcend the limitations of using a physical device to share and opened a whole new dimension of the internet. However, cloud computing is not everyone's cup of tea, everyone talks about it but only a handful of people or organizations understand it.

According to research or survey, around 81% of all the enterprises already using a multi-cloud strategy, and around 67% of enterprise infrastructure is cloud-based. On average, 36 cloud-based services are being used every day by a single person. Already 90% of the companies are on the cloud, and an average business runs 38% and 41% of workloads in public and private cloud respectively. If considered the services, then around 89% of the companies use Software as a Service (SaaS) and Infrastructure as a Service (IaaS) is growing very rapidly [11].

Most of the small-scale organizations will move on to the cloud without knowing about the risks, threats, and vulnerabilities in moving to the cloud. To avoid a major problem later, all the cloud service providers should be assessed first with various criteria. This paper is providing a comprehensive research and differences between all the cloud service providers along with the services they are providing so that any small-scale organization can move on to the cloud without being exposed to a lot of risks.

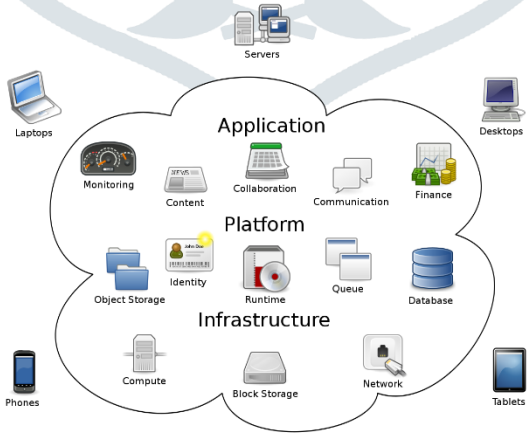

Fig 1: Cloud Computing Architecture

II. LITERATURE SURVEY

With the introduction of any new technologies, there always exists a threat, various research has been made to find out such risks, threat and vulnerabilities by many scholars.

In recent days, the major trend in technology is Cloud Computing. The data hosting technology has become very popular lately which is saving a lot of costs to companies. The new security risks start to appear since this concept is still in its first stages. The

research will set forth the major security issues in cloud computing and propose a new solution to secure data, storage in the cloud environment [1].

Cloud Computing has eliminated the burden of hardware and software infrastructure by facilitating virtual machines via the internet, it has come out as a growing trend in the industry. Even with the indispensable advantages, the security of the data is concerned since cloud computing brings critical challenges that cannot be avoided from the consumer side. In this paper, the author has analyzed the various security aspects that are vulnerable to cloud computing and which are to be resolved [2].

The author of this paper has studied issues in the cloud service delivery models and the various security issue faced in cloud computing. The recommendations are further provided, based on the detailed study that could be followed to conquer the security concerns in the cloud [3].

Cloud services became a vital part of several organizations. Cloud suppliers got to adhere to security and privacy policies to confirm that the users' information remains confidential and secure. Although there are a unit some in-progress efforts on developing cloud security standards, most cloud supplier's area unit implementing a mish-mash of security and privacy controls, that has crystal rectifier to confusion among cloud customers on what security measures they ought to expect from the cloud services, and whether or not these measures would accommodate their security and compliance necessities. A comprehensive study has been conducted to review the potential threats featured by cloud customers and have detected the compliance models and security controls that ought to be in situ to manage the chance. Supporting this study, an associate degree metaphysics have been developed, describing the cloud security controls, threats, and compliances. Associate degree application is additionally developed that classifies the protection threats featured by cloud users and mechanically determines the high-level security and compliance policy controls that got to be activated for every threat. the applying conjointly displays existing cloud suppliers that support these secure ty policies. Cloud customers will use this method to formulate their security policies and notice compliant suppliers albeit they're not aware of the underlying technology [4].

This paper focuses on security risks related to the operation and use of cloud-based information systems in various companies or organizations for different usage [5].

This paper proposes a replacement approach that addresses the existing problems of cloud by observance, acquiring, and adapting in public accessible cloud vulnerability information for effective vulnerability assessments. The vulnerability information from public vulnerability databases is related to and a Network Vulnerability Tests for specific cloud vulnerabilities is developed. The approach has been enforced, evaluated, and also the suitableness is verified [6].

The analysis under mean-field and fluid approximations suggest a shift in cloud architecture design and operation paradigm from maximizing the economic benefits to management and optimization of the inherent systemic risk/benefit tradeoffs [7].

In this paper, the author focuses on a particular side of risk assessment as applied in cloud computing: ways inside a framework which will be employed by cloud service suppliers and repair shoppers to assess risk throughout service preparation and operation. It describes the varied stages within the service lifecycle wherever risk assessment takes place and also the corresponding risk models that are designed and enforced. The impact of risk on beaux-arts parts, with special stress on holistic management support at service operation, is additionally represented. The danger tax assessor is shown to be effective through the experimental analysis of the implementation and is already integrated into a cloud computing toolkit [8].

This paper aims at transportation to light-weight a number of the threats and vulnerabilities to the cloud computing existence, with the importance of enlightening users and suppliers on what's at stake on moving their business or organization whole or half to the cloud [9].

The author of this paper has done the Risk Assessment (RA) use cases for cloud computing platforms square measure given within the context of associate degree ISO 27001 Info Security Management System (ISMS) developed for Alcohol Observance Systems (AMS) across a portfolio of product and services [10].

III. EXISTING RISKS, THREATS AND VULNERABILITIES OF MOVING TO CLOUD

3.1 RISKS OF MOVING TO CLOUD

Consumers Have Reduced Visibility and management: Once transitioning assets/operations to the cloud, organizations lose some visibility and management over those assets/operations, and after the exploitation external cloud services, the responsibility for a few of the policies and infrastructure moves to the Cloud Service Provider.

On-Demand Self Service Simplifies Unauthorized Use: CSPs build it terribly straightforward to provision new services. The on-demand self-service provisioning options of the cloud modify associate organization's personnel to provide further services from the agency's Cloud Service Provider without IT department consent. The use of software in a corporation that's not supported by the organization's IT department is often named shadow IT.

Separation Among Multiple Tenants Fails: The exploitation of system and code vulnerabilities at intervals of a CSP's infrastructure, platforms, or applications that support multi-tenancy will cause a failure to take care of separation among tenants. This failure may be utilized by the associate assailants to realize access from one organization's resource to a different user's or organization's assets or information. Multi-tenancy will increase the attack surface, resulting in the associate exaggerated likelihood of knowledge outflow if the separation controls fail.

Data Deletion is Incomplete. Threats related to information deletion exist as a result of the patron has reduced visibility into wherever their information is physically kept within the cloud and a reduced ability to verify the secure deletion of their information. Since the data is spread over a number of different storage devices within the CSP's infrastructure in a multi-tenancy environment, this risk is concerning. In addition, deletion procedures may differ from provider to provider. Additionally, deletion procedures might take issue from supplier to supplier. Organizations might not be ready to verify that their information was firmly deleted which remnants of the information aren't obtainable to attackers. This threat will increase as a place of work uses a lot of CSP services.

Increased quality Strains IT workers. Migrating to the cloud will introduce quality into IT operations. Managing, group action, and in operation within the cloud might need that the agency's existing IT workers learn a brand new model. IT workers should have the capability and talent level to manage, integrate, and maintain the migration of assets and information to the cloud additionally to their current responsibilities for on-premises IT.

3.2 THREATS OF MOVING TO CLOUD

Credentials are Stolen: If an attacker gains access to a user's cloud credentials, the attacker can have access to the CSP's services to provide additional resources (if credentials allowed access to provisioning), as well as target the organization's assets. The cloud computing resources could be leveraged by the attackers to target the organization's administrative users, other organizations using the same CSP, or the CSP's administrators. An attacker may be able to access the agency's systems and data if access to a CSP administrator's cloud credentials is gained.

Insiders Abuse Authorized Access: The organization's or CSP's networks, systems, and data are uniquely positioned to cause damage or infiltrate information if any Insiders, such as staff and administrators for both organizations and CSPs abuse their authorized access.

Stored Data is Lost: Malicious attacks are not the only reason to lose the data stored in the cloud. A permanent loss of customer data can be caused by accidental deletion of data by the cloud service provider or a physical catastrophe, such as a fire or earthquake.

CSP Supply Chain is Compromised: The third parties may not satisfy/support the requirements that the CSP is contracted to provide with an organization if the CSP outsources parts of its infrastructure, operations, or maintenance.

3.3 VULNERABILITIES OF MOVING TO CLOUD

Misconfigured Cloud Storage - Cloud storage may be a made supply of taken knowledge for cybercriminals. Despite the high stakes, organizations still create the error of misconfiguration of cloud storage that has price several corporations greatly.

Insecure genus Application Programming Interfaces(API) - Application Programming Interfaces (API) are meant to contour cloud computing processes. However, if left insecure, genus APIs will open lines of communications for attackers to use cloud resources.

Loss or Theft of Intellectual Property: One of the most valuable assets of an organization is Intellectual Property, and if the data is stored online, it is also vulnerable to security threats.

Compliance Violations and Regulatory Actions: Every enterprise has steadfast rules to determine who can access which data and what can be done with it. It is always a security risk as it can be difficult to keep track of who can access the information in the cloud since the cloud offers the benefit of ease of access. It is important for organizations to know the details about their data storage and access control, under compliance or industry regulations.

Loss of Control Over End-User Actions: The Company could lose control of its data assets and ultimately become vulnerable to breaches and insider security threats when it is not aware of how its employees are using cloud computing services.

IV. COMPARISON OF DIFFERENT CLOUD SERVICE PROVIDERS

The purpose of the cloud services comparison is to produce an Associate in Nursing illustration of the large variety of services out there and therefore the names given to them. As compared the top 3 cloud suppliers and their services, it's going to become evident that there is little characteristic of one cloud service supplier from another aside from the names given to services.

Table 1: Comparison of Cloud Compute Services

Cloud Compute Services/ Service Providers	AWS	AZURE	GOOGLE
Burstable VM Types	t4g	B	f1/g1
General Purpose VM types (latest generation)	m6g	Dv4/Dsv4	n2d-standard
High Performance Compute VM types	p3/g4/f1	HBv2/HC	clusters
Storage Optimized VM types	h1/i3/d2	Lsv2	n/a
Container services	ECS	ACI	Compute Engine
Kubernetes services	EKS	AKS	Kubernetes Engine
Serverless containers	Fargate	ACI	Cloud Run
Serverless computing	Lambda	Functions	Cloud Functions
Block storage	EBS	Azure Disks	HDD/SSD
Object storage	S3	Azure Blob	Standard
File storage	EFS	Azure Files	Filestore
Infrequent access storage 1	Standard-IA	Cool Blob	Nearline
Infrequent access storage 2	One Zone-IA	n/a	Coldline
Archive storage	Glacier	Azure Archive	Archive
Hybrid storage	Gateway	StorSimple	ClearSky
Physical bulk data transport solution	Snow Family	Import/Export	Transfer App

V. MEASURES THAT CAN BE TAKEN TO AVOID ANY RISKS, THREATS AND VULNERABILITIES

There are several preventive measures that companies can take in order to prevent cloud security vulnerabilities in the early stages. It could be simple cloud security solutions such as implementing multi-factor authentication to more complex security controls for compliance with regulatory mandates.

Controlling the creation and configuration of cloud resources: Several cloud computing problems have come back from those who wish to maneuver into the cloud while not understanding the way to secure the knowledge.

The penetration tests can be conducted which can replicate an external attack targeting the API endpoints and get a secure code review as well. In order to ensure the continuous development of secure applications and APIs, it is best to have a secure Software Development Life Cycle (SDLC).

Organizations can consider using Secure Socket Layer (SSL) / Transport Layer Security (TLS) encryption for data-in-transit: Using the schemas such as one-time passwords, digital identities, etc. to ensure strong authentication controls, multi-factor authentication can be implemented.

The most effective way to prevent loss or theft of intellectual property is by doing frequent backups. A proper schedule can be set for regular backups and a clear delineation of what data is eligible for backups and what is not. To detect and prevent unauthorized movement of sensitive data, the Data Loss Prevention (DLP) software can be made use.

Training can be given to employees to make them understand how to handle security vulnerabilities, such as phishing and malware. Employees must be educated about cloud computing and how to protect confidential information which is carried outside the organization on mobile devices or laptops. The repercussions related to malicious activities should be informed to the employees.

VI. RESULTS AND DISCUSSION

The massive adoption of the cloud isn't without a reason. The benefit of accessibility, price effectiveness and disaster recovery, are simply a number of factors facilitating in moving to the cloud. Even with all the benefits, the organizations or companies should asses the cloud service providers with their requirement and the risks, threats and vulnerabilities so that there will be a better clarity about choosing the service provider and the services by taking proper measures to safely move in to cloud. Below table 2 gives the final conclusion for this research for top 3 cloud service providers

Table 2: Comprehensive comparison between top 3 Cloud Service Providers

Criteria/Service Provider	AWS	AZURE	GOOGLE
Market Share	33%	16%	8%
Cost/Month for 1vCPU & 2GB RAM	Rs.1.89 / Hour	Rs.3.18 /Hour	Rs.3.51 /Hour
Free Trial	12 Months	12 Months	12 Months
Pros	Reliable, Quality Service, Professional Support	Infrastructure Configuration, Ideal for Big Projects	Reliable, Affordable
Cons	Expensive despite regular lowering of price	Unsatisfactory customer experiences and technical support	Limited Feature and Services

REFERENCES

[1] Mostapha Derfouf, Amina Mimouni and Mohsine Eleuldj. 2015. Vulnerabilities and storage security in cloud computing. International Conference on Cloud Technologies and Applications (CloudTech)

[2] Neha Kajal, Nikhat Ikram and Prachi. 2015. Security threats in cloud computing. International Conference on Computing, Communication & Automation

[3] Seema Rawat, Bhawna Dhruv, Praveen Kumar and Payal Mittal. 2015. Dissection and Proposal of Multitudinal Security Threats and Menace in Cloud Computing. IEEE International Conference on Computational Intelligence & Communication Technology

[4] Amit Hendre and Karuna Pande Joshi. 2015. A Semantic Approach to Cloud Security and Compliance. IEEE 8th International Conference on Cloud Computing

[5] Michaela Iorga and Anil Karmel. 2015. Managing Risk in a Cloud Ecosystem. IEEE Cloud Computing Volume: 2, Issue: 6

[6] Kennedy A. Torkura and Christoph Meinel. 2015. Towards Cloud-Aware Vulnerability Assessments. 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)

[7] Marbukh. 2016. Systemic Risks in the Cloud Computing Model: Complex Systems Perspective. IEEE 9th International Conference on Cloud Computing (CLOUD)

[8] Karim Djemame, Django Armstrong, Jordi Guitart and Mario Macias. 2016. A Risk Assessment Framework for Cloud Computing. IEEE Transactions on Cloud Computing Volume: 4, Issue: 3

[9] N. F. Efozia, E. Ariwa, D. C. Asogwa, O. Awonusi and S. O. Anigbogu. 2017. A review of threats and vulnerabilities to cloud computing existence. Seventh International Conference on Innovative Computing Technology (INTECH)

[10] Choi Myeonggil. 2019. The Security Risks of Cloud Computing. IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)

[11] Radoslav Ch. 2021. Cloud Computing Statistics for 2020. Tech Jury