RESEARCH ON CLOUD COMPUTING ISSUES AND STRATEGY

R.Arjunarao
Associate Professor, Dept. of Computer Science
Aurora Degree & PG College, Chikkadapally Hyderabad
Ananth Madhu Priya
Asst-professor, Dept. of Computer Science
Aurora Degree & PG College, Chikkadapally Hyderabad

Received: Oct. 2019 Accepted: Nov. 2019 Published: Dec. 2019

Abstract: Cloud computing, in now days it is been playing a key role in terms of data storing and reducing the overall cost to organization. The worldwide computing infrastructure is rapidly covering towards cloud based architecture. But most of them worried about security; mostly they used to keep the data in multi cloud. Data centers located around the world provide the cloud services. As this field of technology seen a rapid growth in recent times, security has been the major concern. Security is the major issue for every technology either it was from past or recently innovated. For example, open systems like Android (Google Apps) still facing many day-to-day security threats or attacks. In this case if the data is hacked or lost in the sense entire data will be loose. To avoid these kinds of vulnerabilities and to achieve good security we are proposing of multicolor where the data will be stored in different databases clouds. This paper surveys recent research related to single cloud and multi-cloud security and addresses possible solutions this work aims to encourage the use of cloud computing due to its ability to decrease security risks. In cloud data automatically changing dynamically from client side in this case hacker may have a chance to hack the full data through the network or attacking on the database.

Keywords: Security; Storing Data in Cloud multi-clouds; Distributing Data; Single-Cloud; Data Integrity; Data Intrusion; service availability;

Introduction: Cloud computing is the delivery of various hardware and software services over the internet, through a network of remote servers. These remote servers are busy storing, managing, and processing data that enables users to expand or upgrade their existing infrastructure [1]. The capabilities and breadth of the cloud are enormous. The IT industry broke it into three categories to help better define use cases. The significance of the cloud is increasing exponentially. Gartner forecasts that the cloud services market will grow 17.3% in 2019 ($206.2 billion) and by 2022, 90% of organizations will be using cloud services.

Table 1. Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

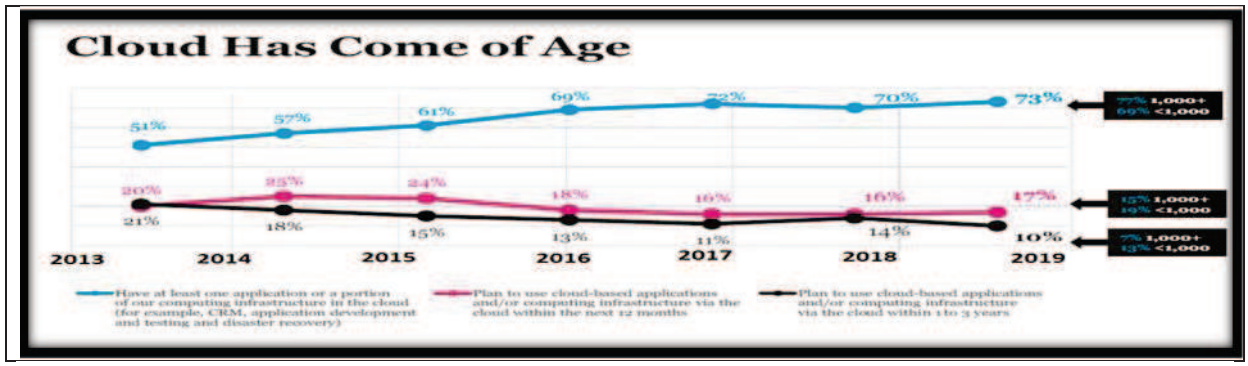
	2017	2018	2019	2020	2021
Cloud Business Process Services (BPaaS)	42.2	46.6	50.3	54.1	58.1
Cloud Application Infrastructure Services (PaaS)	11.9	15.2	18.8	23.0	27.7
Cloud Application Services (SaaS)	58.8	72.2	85.1	98.9	113.1
Cloud Management and Security Services	8.7	10.7	12.5	14.4	16.3
Cloud System Infrastructure Services (IaaS)	23.6	31.0	39.5	49.9	63.0
Total Market	**145.3**	**175.8**	**206.2**	**240.3**	**278.3**

a) Software as a Service (SaaS) – software is owned, delivered and managed remotely by one or more providers. To start, Software-as-a-Service, or SaaS, is a popular way of accessing and paying for software. Instead of installing software on your own servers, SaaS companies enable you to rent software that's hosted, this is typically the case for a monthly or yearly subscription fee. More and more CRM, marketing, and finance related tools use SaaS business intelligence and technology, and even Adobe's Creative Suite has adopted the model[1].

b) Infrastructure as a Service (IaaS) – compute resources, complemented by storage and networking capabilities are owned and hosted by providers and available to customers on-demand.

c) Platform as a Service (PaaS) – the broad collection of application infrastructure (middleware) services. These services include application platform, integration, business process management and database services.

All of this is a deviation from traditional on-premise computing which is done via a local server or personal computer. These traditional methods are increasingly being left behind. In fact, the IDG's recently published Enterprise Cloud Computing Survey (2019) found that 73% of organizations have at least one application, or a portion of their computing infrastructure already in the cloud – 17% plan to do so within the next 12 months.



What Are The Challenges Of Cloud Computing?

In January 2019, Right Scale conducted its annual State of the Cloud Survey on the latest cloud trends. They questioned 1200 technical professionals across a broad cross-section of organizations about their adoption of cloud infrastructure. Their findings were insightful, especially in regards to current cloud computing challenges. To answer the main question of what are the challenges for cloud computing, below we have expanded upon some of their findings and provided additional cloud computing problems that businesses may need to address.

Cloud computing is used for enabling global access to mutual pools of resources such as services, apps, data, servers, and computer networks. It is done on either a third-party server located in a data canter or a privately owned cloud. This makes data-accessing contrivances more reliable and efficient, with nominal administration effort. Because cloud technology depends on the allocation of resources to attain consistency and economy of scale, similar to a utility, it is also fairly cost-effective, making it the choice for many small businesses and firms.

But there are also many challenges involved in cloud computing, and if you're not prepared to deal with them, you won't realize the benefits. Here are six common challenges you must consider before implementing cloud computing technology.

1. Cost: Cloud computing itself is affordable, but tuning the platform according to the company's needs can be expensive. Furthermore, the expense of transferring the data to public clouds can prove to be a

problem for short-lived and small-scale projects. Companies can save some money on system maintenance, management, and acquisitions.

2. Service Provider Reliability: The capacity and capability of a technical service provider are as important as price. The service provider must be available when you need them. The main concern should be the service provider's sustainability and reputation. Make sure you comprehend the techniques via which a provider observes its services and defends dependability claims.

3. Downtime: Downtime is a significant shortcoming of cloud technology. No seller can promise a platform that is free of possible downtime. Cloud technology makes small companies reliant on their connectivity, so companies with an untrustworthy internet connection probably want to think twice before adopting cloud computing.

4. Password Security: Industrious password supervision plays a vital role in cloud security. However, the more people you have accessing your cloud account, the less secure it is. Anybody aware of your passwords will be able to access the information you store there. Businesses should employ multi-factor authentication and make sure that passwords are protected and altered regularly, particularly when staff members leave.

5. Data privacy: Sensitive and personal information that is kept in the cloud should be defined as being for internal use only, not to be shared with third parties. Businesses must have a plan to securely and efficiently manage the data they gather.

6. Vendor lock-in: Entering a cloud computing agreement is easier than leaving it. "Vendor lock-in" happens when altering providers is either excessively expensive or just not possible. It could be that the service is nonstandard or that there is no viable vendor substitute. It comes down to buyer carefulness. Guarantee the services you involve are typical and transportable to other providers, and above all, understand the requirements.

Cloud Deployment Models

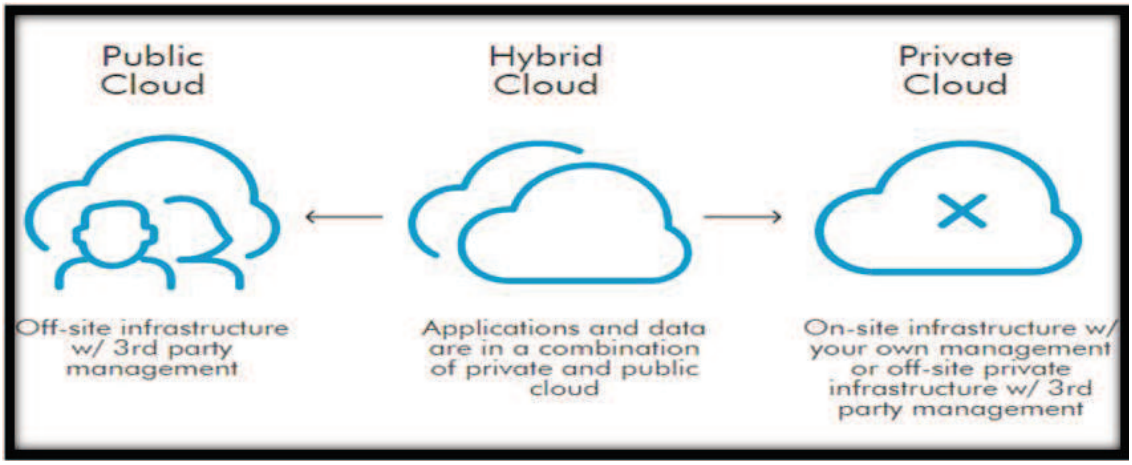
There are three Cloud Deployment Models and are described below:

- Public cloud Model
- Private cloud Model
- Hybrid cloud Model

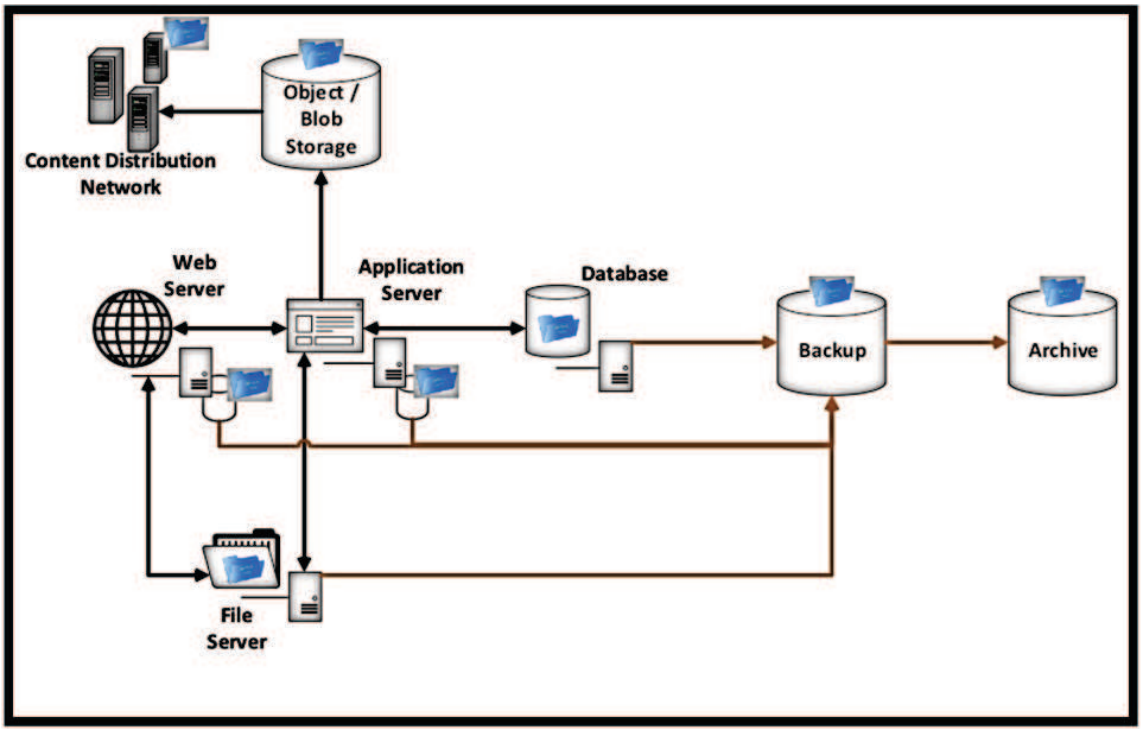
Public Model: This infrastructure is available to the general public. As the name suggests, public cloud is a model in which resources are generally available to everyone or anywhere.

Private Model: This model is developed for the private organizations like one house and an organization and they can use it for their own purpose. This kind of a service is not accessed by everyone.

Hybrid Model: Hybrid Clouds are combination of public and private cloud in a same network. This can be done if private cloud need some important services from the public cloud like Private cloud can store some information on their private cloud and we can use that information on public cloud. In cloud computing, there are many issues but protect is the major issue.



Protect Cloud Data: Beyond access control, data protection involves three separate challenges: protecting data from unauthorized access, ensuring continued access to critical data in the event of errors and failures, and preventing the accidental disclosure of data that was supposedly deleted.



Protect Data from Unauthorized Access: Encrypt data at rest to protect it from disclosure due to unauthorized access. Cloud service providers typically provide encryption capabilities for the storage services they offer. Properly manage the associated encryption keys to ensure effective encryption. Cloud service providers offer consumers a choice of Cloud service providers -managed or consumer-managed keys. Cloud service providers -managed keys are convenient, but provide the consumer no control over where or how the keys are stored. Consumer-managed keys place the burden of key management on the consumer but provide better control. Cloud service providers offer hardware security modules in the cloud to assist in securely managing keys.

Ensure Availability of Critical Data: Cloud service provider significant guarantees against loss of persistent data. No system is perfect, however, and major cloud providers have accidently lost customer data. In addition to Cloud service provider errors, cloud consumer staff may also make mistakes that can result in data loss. You must ensure that Cloud service provider data backup and recovery processes meet your organization's needs. Your organization may need to augment Cloud service provider's processes with additional back-up and recovery actions. Cloud service providers may provide services that consumers can configure to perform additional backup and recovery operations. Prevent Disclosure of Deleted Data.

Security Issues in Cloud Computing: Based on the study, we found that there are many issues in cloud computing but security is the major issue which is associated with cloud computing. Top seven security issues in cloud computing environment as discovered by "Cloud Security Alliance" CSA are [1]:
Misuse and reprehensible Use of Cloud Computing: Hackers, spammers and other criminals take advantage of the suitable registration, simple procedures and comparatively unspecified access to cloud services to launch various attacks like key cracking [4].

Insecure Application Programming Interfaces (API): Customers handle and interact with cloud services through interfaces or API's. Providers must ensure that security is integrated into their service models, while users must be aware of security risks [4].

Wicked Insiders: Malicious insiders create a larger threat in cloud computing environment, since consumers do not have a clear sight of provider policies and procedures. Malicious insiders can gain unauthorized access into organization and their assets [4].

Shared Technology issues/multi-tenancy nature: This is based on shared infrastructure, which is not designed to accommodate a multi-tenant architecture [4].

Data Crash: Comprised data may include; deleted or altered data without making a backup; unlinking a record from a larger environment; loss of an encoding key; and illegal access of sensitive data [4].

Account, Service & Traffic hijacking: Account or service hijacking is usually carried out with stolen credentials. Such attacks include phishing, fraud and exploitation of software vulnerabilities. Attackers can access critical areas of cloud computing services like confidentiality, integrity and availability of services [4].

References:

1. "Security Guidance for Critical Areas of Focus in Cloud computing", April 2009, presented by Cloud Security Alliance (CSA).
2. Arijit Ukil, Debasish Jana and Ajanta De Sarkar" A SECURITY FRAMEWORK IN CLOUD COMPUTING INFRASTRUCTURE "International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013 DOI: 10.5121/ijnsa.2013.5502 11.
3. Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy ," Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.
4. Kashif Munir and Prof Dr. Sellapan Palaniappan," FRAMEWORK FOR SECURE CLOUD COMPUTING ", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.2, April 2013.
5. Ayesha Malik, Muhammad Mohsin Nazir "Security Framework for Cloud Computing Environment: A Review", Journal of Emerging Trends in Computing and Information Sciences ©2009-2012 CIS Journal. All rights reserved, VOL. 3, NO. 3, March 2012 ISSN 2079-8407
6. Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, VasanthBala and PengNing, "Managing security of virtual machine images in a cloud environment", November 2009, Proceedings of the 2009 ACM workshop on Cloud computing security pages 91-96.
7. Miranda Mow bray and Siani Pearson, "A Client- Based Privacy Manager for Cloud computing", June 2009, Proceedings of the Fourth International ICST Conference on communication system software and Middleware.
8. Flavio Lombardi and Roberto Di Pietro, "Transparent Security for Cloud", March 2010, Proceedings of the 2010 ACM.

***