Cloud Computing and Data Storage

S.V.Subramanyam[1]
Professor
Department of AI & ML,
School of Engineering
Malla Reddy University,
svsubramanyam@mallareddyuniversity.com

G.Appa Rao[2]
Assistant. Professor
Department of AI & ML,
School of Engineering
Malla Reddy University,
apparao.g@mallareddyuniversity.ac.in

Abstract
Cloud computing has grabbed the spotlight in the year 2013 Cloud computing trend is increasing rapidly so to make cloud computing more popular the very first step for the organization is to identify exact area where the cloud related threats lieOn-demand cloud computing and data storage can save companies money, but many businesses—particularly in finance and health care—are wary of handing data to third parties, fearing hacking, accidental data loss, or theft by rogue employees of cloud providers. Cloud computing is a set of Information Technology services offered to users over the web on a rented base Generally, cloud services are provided by a third-party supplier who possesses the arrangement. Cloud computing has many advantages such as flexibility, efficiency, scalability, integration, and capital reduction.

Keywords: virtual machines, security of data, private cloud computing, security services

I.Introduction

On-demand cloud computing and data storage can save companies money, but many businesses—particularly in finance and health care—are wary of handing data to third parties, fearing hacking, accidental data loss, or theft by rogue employees of cloud providers. New security solutions are appearing: One verifies cloud providers' claims that data is safely lodged on its own server. Another protects your cloud-based data by using a math function to divide it into 16 segments, any 10 of which can be used to re-create the entire original set.

The first of these solutions responds to recent demonstrations that hacking within clouds—using one set of rented computers or "virtual machines" to attack another—is theoretically possible. In 2009, computer scientists at the University of California, San Diego and MIT showed how an attacker using Amazon's Elastic Compute Cloud could land on the same physical server as his intended victim. (In one method, they forced a hypothetical victim to hire more virtual machines by bombarding his website with traffic and then created attacking virtual machines at the same time. This put the two sets of machines on the same cloud server 40 percent of the time.)The researchers also pointed out that attackers who sat on the same servers as victims could do things like monitor usage of shared physical resources, such as the server's central processing unit (CPU), to infer information such as what kinds of programs the victim was running and how much Web traffic the victim was handling. These actions are known as "side-channel" attacks.

Amazon, in a move similar to ones made by other cloud providers, now offers a virtual private cloud service in which a customer is promised his own isolated server. Because customers are likely to want to confirm that they're getting what they paid for, a group of researchers at RSA Laboratories, in Cambridge, Massachusetts, and the University of North Carolina at Chapel Hill has developed a verification method that involves monitoring a piece of shared server hardware called the CPU cache, which allows quick access to frequently tapped memory resources. The prototype technology lets a client monitor whether the CPU cache on its cloud server is doing anything beyond what would be expected by the client's own computation. Such a discovery would suggest that someone else is sharing the server. "This allows you to check on your situation in the cloud,", "It's a way of doing detection on when you actually have a physical server to yourself."

II. Cloud Service Models

Cloud Software-as-a-Service : Software –as-a-Service is a software distribution scheme which gives right to access the software and its functions remotely as a web-based service. Software-as-a-Service eliminates the all possibilities for organizations to handle the installation, set-up The end user takes on these offered services based on their requirements and pay for what they have used. The end user is capable of deploy and run any software, which comprise Operation Systems, applications. The end user does not supervise or monitor the core cloud infrastructure, but has hold over the operation systems and deployed application. Flexibility and scaling are the liabilities of the end user, not the supplier. Moreover IaaS is small task

performing -it-yourself information hub so as you would require to form the means (server, storage) and make the task completed. Waiting right away, small end users did not have the investment to make a purchase of immense computing resources and to make sure that they had the space they wanted to manage unpredicted spikes during load. Amazon Elastic Compute Cloud (Amazon EC2) is an infrastructure–as-a-Service model that facilitates scalable compute volume, on demand, in the cloud. It actually allows end users to leverage Amazon"s huge infrastructure with no up-front investments. Amazon EC2 decreases the clock needed to get hold of and boot latest server instances and permit users to immediately scale space – equally up and down as their computing needs vary

III. Cloud Deployment Models
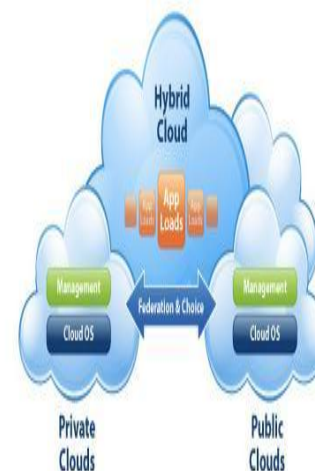
- **Public Cloud**-A cloud is to be entitled as public cloud when the services (like applications, storage) are being provided over network that are available publically, anyone can access it. Public cloud"s benefits may be taken as on a pay per usage mode or other purchasing schemes.

- **Private Cloud** –A private cloud is an infrastructure that provides the services to a single organization, whether managed by internally or by a third party. Cloud which is hosted externally is termed as "externally hosted" private cloud and other hosted by third party are termed as "on premise" private cloud

Community Cloud-It comprises sharing of computing infrastructure between organizations of identical community.

Hybrid Cloud-A hybrid cloud is a collection of private as well as public c loud options.)

That are mains unique entities but is bound together by standardized or proprietary technology

IV. Cloud Computing Technologies

UCSB
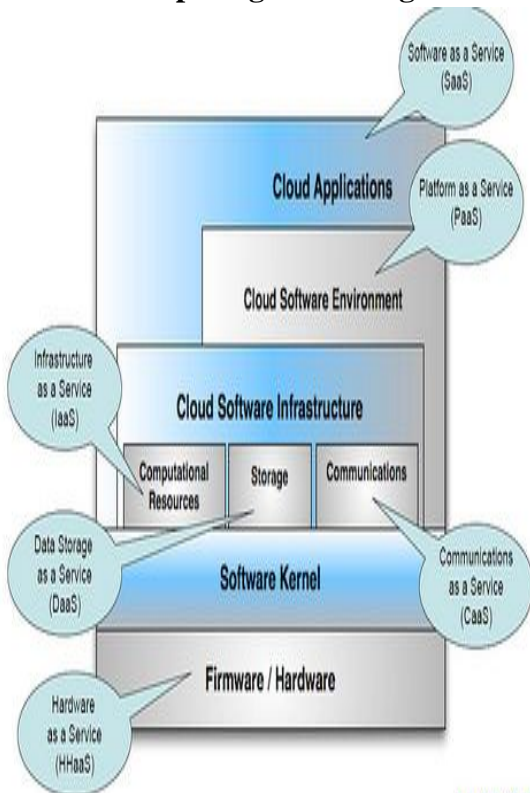
1.Microsoft Cloud Technologies
Microsoft is a fore most provider of cloud technologies and applications with results that matches with all type of business needs. It provides all type of services whether it is PaaS, IaaS or SaaS.

2.Oracle Cloud Technologies
Oracle also provides the complete enterprise read public cloud solution including IaaS, PaaS and SaaS. Oracle offers the following services Database, it is available Database-as-a-Service a long with accessing the Database in the Cloud directly through standard network connections, or as a Platform as a Service, with a complete development and deployment environment. Develop J2EE standards JSP, JSF, Serv let, EJB, JPA,JAX –RS and JAX-WS applicat ions .

3.Google Cloud Technologies
Google cloud also provides the services such as Software-as-a-Service, Platform-as-a-Service and Infrastructure-as-a-Service. Google cloud enables developers to build, test and deploy applications on Google"s highly scalable and secure infrastructure. As we know that Google has already provided infrastructure that allows Google to return billions of search results in milliseconds, Google has the ability to build, organize and operate a huge network of servers and fiber-optic cables .All this in aggregate makes Google the King of all cloud. Google Apps Engine-with Apps Engine you can run your applications on a fully managed Platform-as-a-Serv ice using built-In services.

V. Cloud Com puting Security Threats
Cloud computing faces as much security threats as that are existing in the networks, intranets .these threats come in various forms.

Cloud computing alliance did research in 2013 on cloud computing security threats and identified these threats

- ➢ Traffic Hijac king
- ➢ Insecure Interface and APIs.
- ➢ Denial of Serv ice.
- ➢ Malic ious Insiders.
- ➢ Abuse of Cloud Se rvices.
- ➢ Insufficient Due Diligence.
- ➢ Shared Technology Vulnerab ilit ies
- ➢ Data Breaches
- ➢ Unknown Risk Profile
- ➢ Perimeter Security Model Broken

VI Cloud Security Issues

While cost and ease of use are the two main strong benefits of the cloud computing, there are some major a larming issues that need to be referenced when allowing moving critical application and sensitive data to public and shared cloud environment. The main aspect describing the achievement of any new computing technology is the height of security it provides whether the data located in the cloud is protected at that level that it can avoid any sort of security issue. Here are some security issues, presented in this paper.

- ✓ Data confidentiality issue
- ✓ Data availability issue
- ✓ Data integrity issue
- ✓ Trust issue
- ✓ Data locality issue

• Data confidentiality issue:
Confidentiality is a set of rules or an agreement that bounds access or location restriction on certain types of information so in cloud data reside publically so Confidentiality refers to, customer‟s data and computation task are to be kept confidential from both cloud provider and other customers who is using the service.

• Data availability issue:
When keeping data at remote location which is owned by others, data owner may face the problem of system failure of the service provider. And if cloud stops working, data will not be available as the data depends on single service provider. Cloud computing is to provide on-demand service of different levels. If a certain service is no longer available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose faith in the cloud system

• Data integrity issue:
As the word itself explains the "completeness" and "wholeness" of the data which is the basic and central needs of the information technology, The data integrity proofs the validity, consistency and regularity of the data. It is the perfect method of writing of the data in a secure way the persistent data storage which can be reclaim or retrieved in the same layout as it was stored later. Therefore cloud storage is becoming popular for the outsourcing of day-to-day management of data .So integrity monitoring of the data in the cloud is also very important to escape all possibilities of data corruption and data crash. The cloud provider should provide surety to the user that integrity of their data is maintained in the cloud.

• Trust issue:
Trust in the both conventional IT business and cloud computing need to be earned. Trust is also a major issue in cloud computing. cloud is becoming popular, many people are using cloud but still people have some doubt in their confidential mind that their data might not be

safe in the cloud like they don"t put their account no, passport copy and other confidential information they might think that their information may be stolen or misused. Therefore cloud provider must have to come forward to tackle with the trust issue and build trust with the users so that more and more people will be able to take advantage of cloud computing without having any doubt

• Data locality issue:
In the data storage model of cloud computing environment the user the applications provided by the service provider and process their data but in this scenario the user does not have any knowledge about where their data is being stored, in many situations this can be a legal issue

VII. Conclusion
Cloud computing is the cost, time and performance effective technology. the usage of cloud computing will surely will increase more in next few years. Some security issues are the key concern in the cloud computing. Especially privacy and integrity of data are the key concern security issues. In the cloud as data is stored publically and really don"t know where the data is being stored, don"t know the exact location of the data, due to this data stored in the cloud has a higher risk of being accessed by un-autheorized person during storage as well as transmission

ACKNOWLEDGEMENT

References
1.Gaddam Shwetha & V.Sridhar Reddy, "Secure Data Sharing In Cloud Computing Using Revocable-Storage IdentityBased Encryption", International Journal of Research in Advanced Computer Science Engineering, Volume 4 Issue 1, 2018, Page 14-19.

2. Mr G. Anthes, "Security in cloud," Communications of ACM, vol. 53, no. 11, pp. 16–18, 2010.

3. M. Armbrust et al., "A view of cloud computing," Commun. ACM, vol. 40, no. 4, pp. 50–58, 2010.

4. K Usha Rani & S Pratima Reddy "System to Monitor Human Health using Mobile and Cloud Computing", International Journal of Research in Advanced Computer Science Engineering, Volume 4 Issue 12, 2019, Page 7-16.

5. Routhu Sreelekha, "Cloud Computing and Security Challenges",International Journal & Magazine of Engineering, Technology, Management and Research (IJMETMR), ISSN 2348-4845, Volume 2 Issue 8, August 2015, Page 775-779.

6. N.JYOTHIRMAI & B.MANJUSHA, "Cloud Computing", Yuva Engineers, ISSN No: 2320-3706 (Print), April 2010, http://www.yuvaengineers.com/cloud-computing-n-jyothirmai-b-manjusha/

7. J. Beckham, "Top 5 Security Risks of Cloud Computing," cisco.com, May 3, 2011.

8. J. Che, Y. Duan, T. Zhang, J. Fan," Study on the security models and strategies of cloud computing", Procedia Engineering, Vol. 23, pp586-593, 2011.

About the Authors:

S.V.Subramanyam he is working in Dept of Artificial intelligence and Machine Learning at Malla Reddy University . He did B.Tech In computer science and information technology from J.B.I.E.T ,and M.Tech in Computer Science and Engineering from Indur Institute of Engineering and Technology , He Published papers in many national and international conferences and journals . his area of interest is Data Base,Data mining and Data Warehouse and computer networking

Mr.G.AppaRao, well known author and excellent teacher received B.Tech from Sarada Institute of Tech&Management, Srikakulam, Affliated by JNTUH and M.E (NIE) from Karunya University, Coimbatore. He worked for 3 years inSt.Theressa Institute of Engineering &Technology, Garividi, Vizayanagaram Dist. He worked for 7 years as Asst. Professor in Dept. of CSE in S.R.K Institute of Technology, Vijayawada, Krishna Dist. He worked for 2 years as Asst.Professor in Dept. ofCSE in DIET, Anakapalle, Visakhapatnam Dist, AP. Presently he is working in AI & ML Dept of Malla Reddy University, Hyderabad. His areas of Interest include Data Warehouse and Data Mining, Networking information security, and Machine Learning.