RESEARCHERID
THOMSON REUTERS

ISSN: 2277-9655
[Neware * *et al.*, 6(11): November, 2017] Impact Factor: 4.116
IC™ Value: 3.00 CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

RECENT THREATS TO CLOUD COMPUTING DATA AND ITS PREVENTION MEASURES

Rahul Neware*

*Department of Computer Science & Engineering, G. H. Raisoni College of Engineering, Nagpur, India

DOI: 10.5281/zenodo.1049430

ABSTRACT

As the cloud computing is expanding day by day due to its benefits like Cost, Speed Global Scale, Productivity, Performance, Reliability etc. Everyone, like Business vendors, governments etc are using the cloud computing to grow fast. Although Cloud Computing has above mentioned and other benefits but security of cloud is problems and due to this security problem adoption of cloud computing is not growing. This paper gives information about recent threats to the cloud computing data and its prevention measures so that to increase its wide-spread adoption.

KEYWORDS: Cloud Computing, Cloud Security , Cloud Services ,Data Privacy.

I. INTRODUCTION

Cloud computing is on demand computing gives access to shared resources like Network, Storage, Devices etc. when user demands that service. The National Institute of Standard and Technology (NIST) gives a definition of cloud computing: "Cloud Computing is a model for enabling convenient, On-demand network access to shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort for service provider interaction"[1]. Cloud Computing uses abstraction in which end user of cloud does not know about where from resource coming or where data stored and from where user getting data because of the distributed computing. User import all the services from cloud this will reduces the cost of establishment and maintenance[11].

Main thing in cloud computing is that it uses Virtualization technique. "Virtualization is the creation of virtual version of computer"[12]. Virtualization assigns a logical name for a physical resource and then provides a pointer to that physical resource when a request is made. Virtual machine Introspection(VMI) used in detecting stealth attack and User and Kernel level processes of virtual machine.[2]

Cloud Computing consist of three main basic layers(services) ,

- **IaaS(Infrastructure as a Service):**
  It provides Virtual machines, Storages, infrastructure and other hardware. IaaS service provider manages all the infrastructure. In IaaS client is responsible for all other aspects of the deployment, include Operating System, Application and user interaction with system.
- **PaaS(Platform as a Service):**
  It provides Virtual machines, Operating system, Applications, service, development framework, transaction and control structures. In PaaS client can display its application or use application and tools supported by PaaS service provider. Client is responsible for installing for installing and managing the application that it is deploying.
- **SaaS(Software as a Service):**
  It is a complete operating environment with application management user interface. In SaaS application is provide to the user through browser and Client is responsible for everything. Everything from the application down to the infrastructure is the vendor's responsibility

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

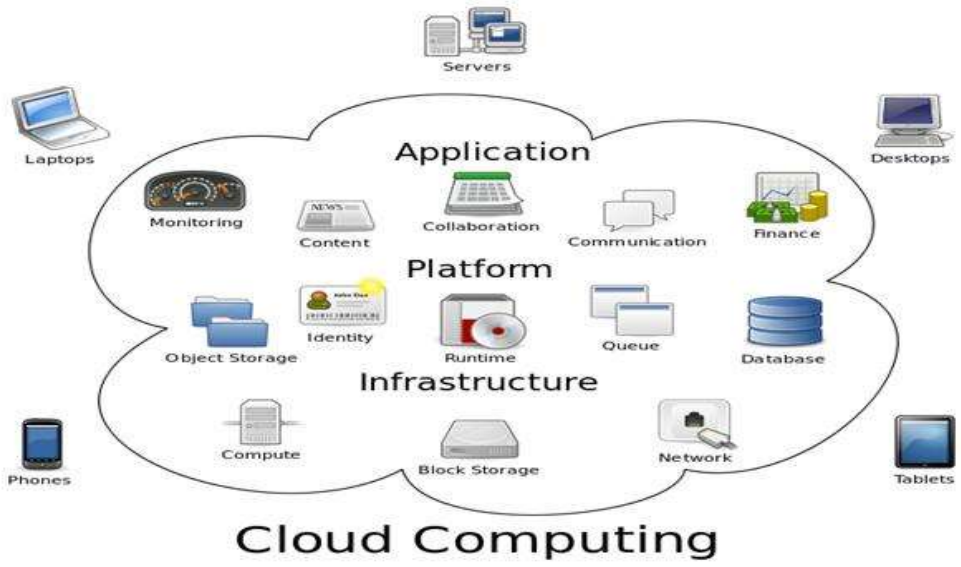

Fig. 1.1 Cloud Computing with its 3 service and their components

Characteristics of Cloud Computing [3],

Following are the characteristics of Cloud Computing

a. On Demand self service: A client can provision computer resources without the need for interaction with cloud service provider personnel.
b. Broad network access: Access to resources in the cloud is available over the network using standard methods that provide platform independent access to clients of all types.
c. Resource Pooling: A cloud service provider creates resources that are pooled together in a system that supports multitenant usage.
d. Rapid Elasticity: System can add resources by scaling up systems and can be elastically provisioned. Scaling can be automatic or manual.
e. Measured service: The use of cloud system resources is measured, audited, and reported to the customer based on a metered system.

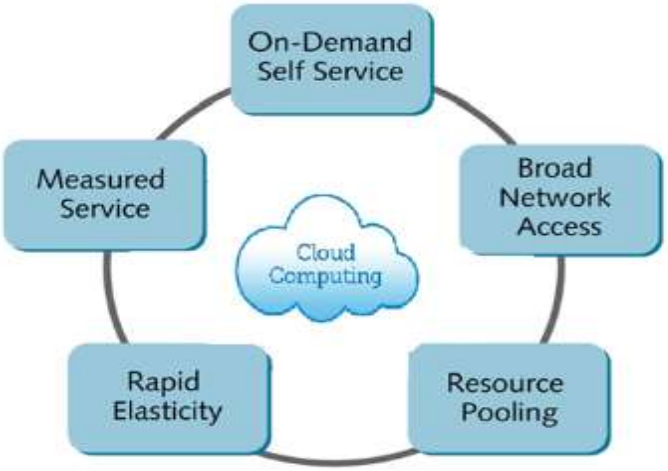

Fig. 1.2 Characteristics of Cloud Computing

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

II. INTRSIONS IN CLOUD ENVIRONMENT

1. Insider Attack

It is like internal intrusion in which attacker try to gain access to cloud as a potential user and do some unwanted task [7]. Insider attacks are very difficult to detect because attacker used same login details as potential user used. Example of this is EC2 (Elastic Compute Cloud) internal DoS attack [4].

2. Denial of Service attack(DoS & DDoS)

In this types of attack attacker send as many as possible requests or packets to the victims virtual machine and create flood sinario by using various zombie machines. Attacker used this attack to stop service of intended servers called as Direct DoS and if the hardware of server machine is not able to process the flood then it is called Indirect DoS[5].

3. Backdoor attack

Backtracking means creating a way to penetrate into system without giving user identity test and disclose user information. By using backdoor attacker gain access to the user system and use it as zombie to carried out DDoS attack.

4. User to root attack

In user to root attack attacker get access to the system of hypervisor by using getting the potential users login details by using any of attacks. When attacker get access to any network system access then by using vulnerability get access to root system[6]. Example of root attacks are buffer overflow, Pal, xtream etc.

5. Attacks on Hypervisor

In this by using attacks like DKSM[8], SubVir[9], BLUEPILL[7] gets access to hypervisor and then control the virtual machine. When attacker gets access to hypervisors then it is pretty easy to control the Virtual machine and damage any server utilities using applications[].

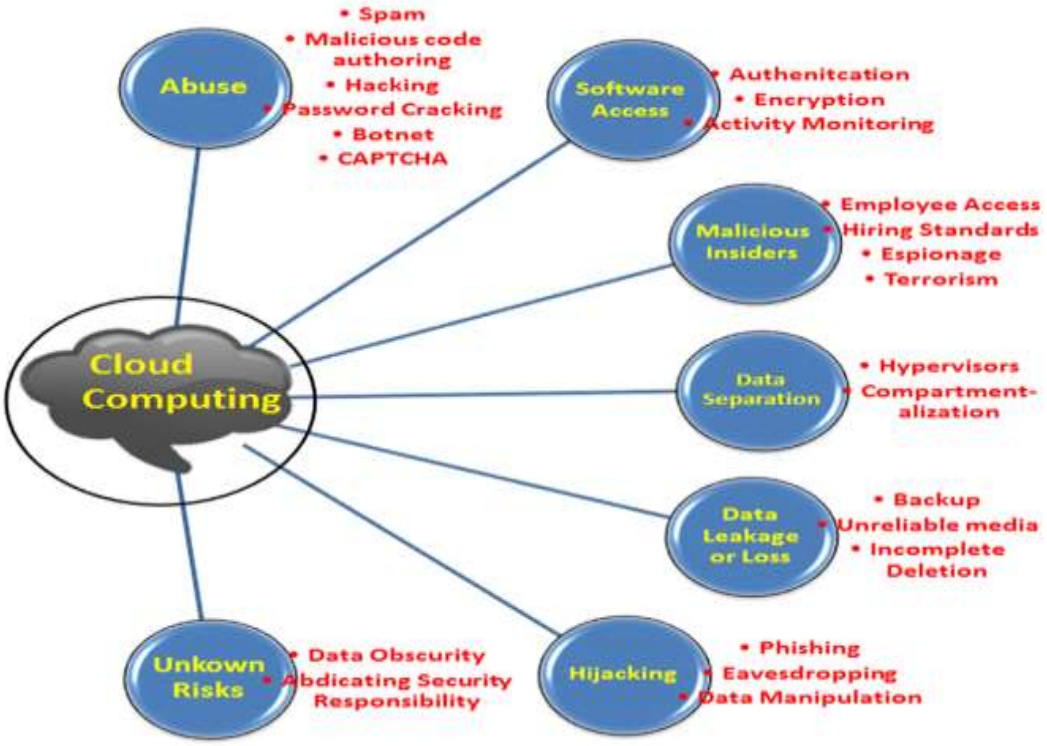

Fig 2.1. Threats to Cloud Computing

III. RECENT THREATS TO CLOUD COMPUTING DATA

I. Data Breaches

In cloud data breach all the personal data of user or data of any organization data is stolen or used by the attacker for any bad intension. Data breach's main reason are human errors, vulnerabilities in application, weak security mechanism etc. In data breaches any type of data is misused like identification data, Login details, medical data, secret data of any government body. Data breaches has many business impacts. In last 5 years many data breaches seen and that is the main reason of decreasing adoption of cloud.

In 30 December 2016 ESEA (E- Sport Entertainment Association) issued a warning of data breach. I this data breach 1,503,707 ESEA record leaked which include private information of users like registration details, Last Login, user details, email address, website URL. Again in 21 March 2017 data breach data on America's Job Link is observed and 4.8 million job seeker information is stolen which include full name, birth date and social security number.

II. Insecure Interface and API's

User of cloud interact with cloud services by using user interface and API's (Application programming interfaces) management, provision, administration and checking altogether performed with these interfaces. The security accessibility of general cloud administration is subject to the security of these fundamental API's. From confirmation and access control to encryption and action checking, these interfaces must be intended to ensure against both unplanned and malicious attempt to policy. Organization and third party expand this interfaces to offer value added service to their clients. This present many sided quality of new layer of API. Which increase risk, since organization might required to surrender their accreditation to outsiders to empower their organization. Interfaces and API's are most uncovered piece of system. May be the main resource with an IP address accessible outside the Organization limit. This is the target of attack.

Arby's on 19 January 2017 announced data stolen by the installation of malicious software on company point-to-point scale system. Stolen information contains the credit card and debit card details. In 2015 Internal Revenue Service(IRS) USA announced that 300000 records are stolen through vulnerable API.

III. System Vulnerability

Vulnerability are bugs in program used to taking data and control system or disturbing admin operations. Vulnerability in operating system at the level of kernel, libraries, and application programs given arises to security risk. Vulnerability bug are very old security problem to the computer system. With the multi tenancy in cloud system from different association are keep each other close to access shared memory and shared resources which create security risks. Damage from vulnerabilities are considerable like assaults can be moderated with essential IT process. Standard defenselessness checking for vulnerability will carried out and finding vulnerability and update the system which will decrease this type of attacks. Secure plan and design can reduce the attacks on taking control of system by limiting access control to the system.

IV. Account Hijacking

Account and server hijacking is a top threat for data theft. Account hijacking can be performed by using any old attack type like phishing, vulnerability. When attacker gain access to login details of cloud user then it will monitor all the activities of user like transactions, data handling and any other operations. When attacker hijack cloud account of user then it will also access the services area of cloud which affects standards of those services. User and organization be aware of this attack and user should implement the protection strategy for this type of attack to save litigation which causes data breach. Organization should stop sharing login details to users and implement strong 2 factor authentication mechanism. All record and record exercises from in to out should be monitored by organization. In June 2014 Amazon AWS code space account is hijacked and all company is destroyed in this attack.

V. Malicious Insider

A malicious insider threat which is former potential user of cloud service who has access to all the data of organizational cloud and misuse this data to compromise the cloud security. Insiders like admin can access all the data also have access to all services of cloud i.e. IaaS, PaaS and SaaS by which it will get all the data. The system which depends on cloud service provider(CSP) are on the very high risk. If for security of cloud encryption applied then also this all are vulnerable because cloud service provider monitor all the activities with cloud network. Examples of malicious insider are admin, Tech-savvy insider, poor internal enforcement.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

VI. Advanced Persistent Threat

It is a parasitical type of cyber attack that invades system to set up on dependable balance in figuring foundation of target organization from which they carry information and protected innovations. Advance persistent threats seek after their objectives stealthily over extended period of time, often adapting to the security measure against protecting them. Spearphishing, coordinate hacking system, conveying assault code through USB gadgets, infiltration through accomplice systems and utilization of unsecured or outsider systems are regular purposes of passage for Advanced persistent system. Once set up, APTs can move along the side through information focus systems and mix in with typical system movement to accomplish their goals. It requires security control, management and training to avoid this attack. Awareness program is best defense of Advanced persistent system attack because it requires user action to start.

VII. CONCLUSION

Cloud computing is a recent trend in computing .It has many benefits according to its use but mostly used in business and organizations. Need to study threats to cloud computing is because of its vulnerability and risk while used as outsourcing and trusting to cloud. In this paper, all recent threats to cloud computing data with its prevention measures are present because data is most important for organization so its security measures are also important. Data breaches occur due to vulnerabilities and insecure APIs and UI. To prevent this breaches organization should train their user, mostly insider user of data are responsible for data breaches

VIII. REFERENCES

[1] The NIST Definition of Cloud Computing, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[2] S. Roschke and F. Cheng, "Intrusion Detection in the Cloud," Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp.227-234.
[3] A. Bakshi and B. Yogesh, "Securing cloud from DDOS attacks using intrusion detection system in virtual machine," Second International Conference on Communication Software and Networks, 2010, pp.260–264.
[4] "Black Hat presentation demo vids: Amazon", [Online]. Available: https://www.sensepost.com/blog/2009/ blackhat-presentation-demovids- amazon/
[5] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan, "A Survey of Intrusion Detection Techniques in Cloud," Journal of Network and Computer Applications (JNCA), Elseiver, vol. 36, 2012, pp.42– 57.
[6] S.G. Kene and D.P. Theng, "A review on intrusion detection techniques for cloud computing and security challenges," IEEE 2nd International Conference on Electronics and Communication Systems (ICECS 2015), 2015, pp.227-323.
[7] S. A. Aljawarneh, R. A. Moftah, and A. M. Maatuk, "Investigations of automatic methods for detecting the polymorphic worms signatures," Futur. Gener. Comput. Syst., vol. 60, pp. 67–77, 2016.
[8] S. Bahram, X. Jiang, Z. Wang, M. Grace et al., "DKSM: subverting virtual machine introspection for fun and profit," 2010 29th IEEE Symposium on Reliable Distributed Systems (SRDS),New Delhi, Punjab India, 2010, pp.82-91.
[9] J.S. King, P.M. Chen, Y-M. Wang et al., "SubVirt: Implementing malware with virtual machines," 2006 IEEE symposium on security and privacy, 2006, pp.314–27.
[10] J. Rutkowska, "Subverting VistaTM Kernel for Fun and Profit," Black Hat Conference, 2006.
[11] Nicolas Carr, The Big Swtich Our New Destiney ; W. W. Norton & Co., 2008
[12] https://en.wikipedia.org/wiki/Cloud_computing

CITE AN ARTICLE

Neware, R. (n.d.). RECENT THREATS TO CLOUD COMPUTING DATA AND ITS PREVENTION MEASURES. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *6*(11), 234-238.