Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.490 – 496

RESEARCH ARTICLE

Study of Security Risk and Vulnerabilities of Cloud Computing

Dr.P.K.Rai[1], R.K.Bunkar[2]

[1]Computer Centre, APS University, Rewa, M.P., India

[2]Computer Science, IGN Tribal University, Amarkantak, Anuppur, M.P., India

[1] pkrapsu@gmail.com; [2] bunkar.rajesh@gmail.com

Abstract— Cloud computing has been developed to decrease IT expenses and to provide alert IT services to human being users as well as organizations. Cloud computing is dynamic in nature; that is elastic, scalable and multi-shared with high capability that gives an innovative shape of carrying out business. The estimation of cloud computing security impact is difficult for two main reasons. Primary, as is true for many discussions about basic vocabulary such as "risk," "threat," and "vulnerability" are often used as if they were exchangeable, without observe to their particular definition. Secondary, not every concern that's raise is really particular to cloud computing. The important factor concerns are vulnerabilities. Cloud computing make assured well-understood vulnerabilities more significant and adds new vulnerabilities. Therefore we need to define cloud-specific vulnerabilities, cloud feature vulnerabilities and propose a reference vulnerabilities architecture of cloud computing. In this paper we have presented taxonomy of cloud computing vulnerabilities.

Keywords— architectural component; cloud computing; security cloud; security risk; Vulnerability

I. INTRODUCTION

Cloud computing defined in Buyya et al. [1] "A Cloud is a type of analogous and scattered system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service level agreements established through negotiation between the tune-up supplier". The clients use the elevated excellence networks, application, servers and services from a public pool of configurable computing capital [3]. Many corporations including Amazon, Google, SUN, IBM, Oracle, Intel, HP, and Windows Azure have invested in cloud computing and offers cloud-based solutions. There are dissimilar stories about what cloud computing "is", there is one exact path that virtualization is headed that could bring along with it. Some other harm for the security industry. One matter to focal point is cantered on vulnerability managing and how it is implemented in a cloud environment. Customer's are faced with the requirement to scan their cloud, but unable to do so. Virtualization providers have been

almost their customers and hosting providers to adopt new infrastructure to automate the distribution of CPU processing time for their applications. Across multiple reduced hardware devices. Vulnerability is an important issue of risk. ISO 27005 defines risk as the possible threat that a given threat will utilize vulnerabilities of a quality or group of assets and thereby origin harm to the grouping determine it in supplies of as one the chance of an occurrence and its result. The Open Group's risk taxonomy [10] for cloud computing and particularly about vulnerabilities is presented in the forth coming paragraphs.

Definitions of cloud computing

Cloud computing is internet-based computing and latest trend in information technology (IT) world. The internet is frequently represented as a cloud and the term "cloud computing" arises from that analogy. In brief, cloud computing is the dynamic provisioning of IT capabilities (hardware, software, or services) from third parties over a network.

Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services) [5].These property can be energetically reconfigured to adjust to a variable load (scale) allowing also for best possible resource utilization. This group of resources is typically demoralized by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized service level agreements.

CLOUD SECURITY AND PRIVACY

Security: Concerns the confidentiality, ease of use and reliability of data or information. Security may also include validation and non-repudiation.

Privacy*:* Concerns the expression of or devotion to various legal and non- legal norms regarding the right to private life. It would be there highly complex to map cloud issues onto the full panoply of privacy and personal data protection authoritarian architectures, the internationally received privacy principles give a useful frame: consent, purpose restriction, legitimacy, simplicity, data security and data subject participation.

Vulnerability: According to the Open Group's risk taxonomy [10]"Vulnerability is the possibility that a quality will be unable to resist the actions of a threat agent. Vulnerability exists when there is a differentiation between the energy being applied by the threat agent, and an object's capability to oppose that strength so, vulnerability should all the time be described in terms of conflict to a certain type of attack".

II. CLOUD CHARACTERISTIC VULNERABILITIES

Unauthorized access to management interface*:* The cloud feature on-demand self-service requires a management interface that's nearby to cloud service users. Unconstitutional access to the management interface is therefore a particularly relevant vulnerability for cloud systems [4]. The probability that unauthorized access could come about is much higher than for time-honoured systems where the management functionality is reachable only to a few administrator.

Internet protocol vulnerabilities*:* The cloud characteristic ever-present network access means that cloud services are accessed via network using standard protocols. In most cases, this system is the internet. Internet procedure vulnerabilities such as man-in-the-middle attacks are relevant for cloud computing.

Data recovery vulnerability*:* The cloud individuality of pooling and flexibility involve that resources allocated to one user will be reallocated to a different user at a later time. Memory or storage property might be possible to recover data written by a previous user.

Metering and billing evasion*:* The cloud feature to precise services means that any cloud service has a capability at a generalization level appropriate to the service type (such as storage, processing, and active user accounts). Metering data used to optimize examine

delivery with bill. Applicable vulnerabilities contain metering and billing data treatment and billing elusion.

III. Cloud Vulnerabilities

Securely transferring data*:* Our data can be vulnerable to prying eyes as we hand on it and from the cloud. Therefore we should not shift important or confidential data in an open wireless network, in a random public Wi-Fi network. It is better to use our home network, and to make sure encrypting our data. We must make sure that our wireless router is password-protected. We should ensure that the Web addresses of sites we are visiting are HTTPS rather than simply HTTP. HTTPS sites are encrypted to transfer information safely.

Accessing data*:* There is nothing worse than trying to recover our information and judgment is not presented. Customer wants to know that their data is available when they need.

Before delegate a cloud provider with our records, we have to assess what sort of undertaking they have about uptime when our data is available and consider their track record. Generally superior off sticking with honest, big-name providers.

Data backup*:* Our data isn't floating around in the clouds; it's stored on a physical server somewhere. So what happens when there is a hurricane or a flood or a power failure? Take the time to evaluate our cloud provider's disaster recovery plan when we use the cloud to store critical data then have our own backup too. In the privacy globe, they talk concerning organizations life form custodian of data and that's a good way to glance at it. We must be careful as we are handing significant information over to an important person else. Ensure that our data exist elsewhere whether on an exterior hard drive, on our laptop's hard drive or on a USB drive will give us peace of mind.

Password use*:* Multiple instance of hacks and data breach has exposed the passwords of users of well-known websites and companies. These attacks also lean-to light on what a miserable job most of us do in using strong, unique passwords. We should try not to use the identical password for all our activities in the cloud. If we use the similar password for a gaming site as we do for our bank account, we place our assets at danger, if that making a bet password is cooperation. It is fine carry out to use a password administrator such as Last Pass.

Privacy*:* Privacy is important consideration about the information we distribute. For example, why provide a phone number to sign up for an email news letter? Take the time to irregularly review which mobile applications and third party services have access to key accounts such as Facebook and Twitter. Reviewing the admission grants will remind us to sever that connection, eliminate any option of utilization or mistreatment.

Effective cloud securities are:

(a) BYOD
(b) Data control
(c) Potential data loss
(d) Enforcing security policies
(e) Visibility across all infrastructure resources,
(f) Traditional and cloud
(g) Real-time analysis of log data
(h) Compliance reporting

IV. Vulnerabilities and threats architecture of Cloud computing

In cloud computing users are no longer required to purchase hardware, software or to manage storages. Due to the development of this technology users are required to pay for cloud services on expenditure center. Fresh cloud based models are discussed, and implemented as solutions in form of on-demand services that allows businesses to enhance their efficiency and scalability. The benefits of cloud computing to various organizations are moving towards IT solutions that are based on cloud. Before opening the trip to cloud, organization must consider the possible threats and vulnerabilities that may convert their dreams of enhancing scalability and saving management cost into a terrible of data loss and misuse. Based on Cloud Security Alliance (CSA) and research, NIST [8] have identified top seven threats and vulnerabilities that are the causes behind the creation of a Cloud.

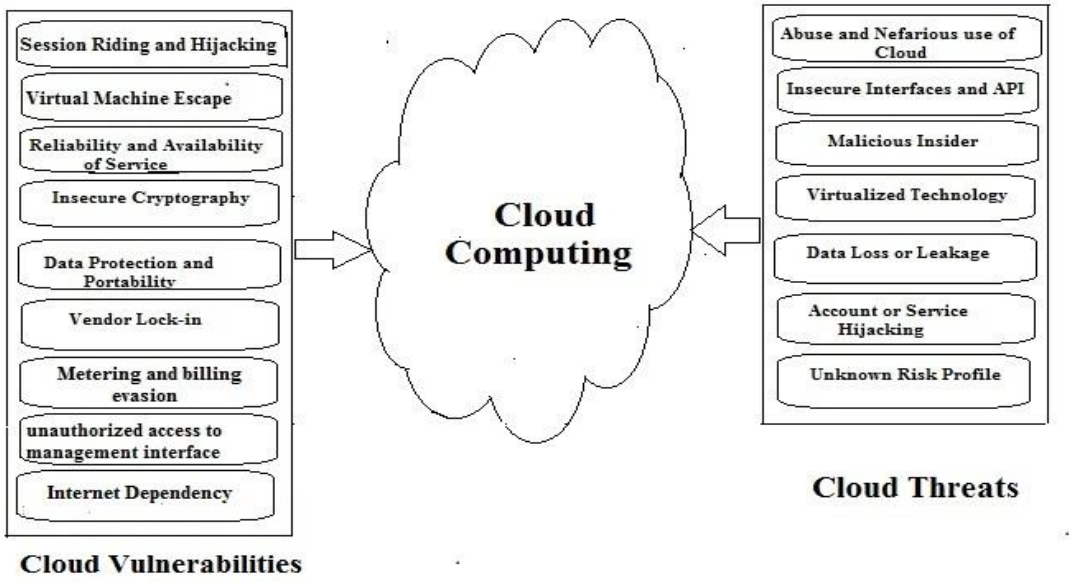

Fig1.Cloud Vulnerabilities and Threats architecture

Session riding and Hijacking: Session hijacking refers to utilize a valid session key to gain unauthorized access for the information or services residing on a workstation structure. It refers to stealing of a cookie used to authenticate a user to a remote server and it is relevant to web application technology. Weakness in the web appliance arrangement at their disposal that gives the chance to hackers in order to accomplish a wide variety of malicious activities. Session riding delete client data, execute online transactions like bid or orders, sends spam to an intranet scheme via internet and changes system as well as network configurations or even opens the firewall [6].

Virtual Machine Escape: Cloud computing servers use the matching OS, venture and web applications as contained VMs and physical servers. The capacity for an attacker or malware to slightly exploit vulnerabilities in these systems and applications is a significant threat to virtualized cloud computing environments [6].

Reliability and Availability of Service [5]: In terms of dependability and accessibility, cloud computing is not a wonderful technology. With more services organism built on top of cloud computing infrastructures, an outage or breakdown can create a domino effect by taking down large amounts of internet based services and applications which raise several questions such as in cases of failure, what forms of completion exist for stakeholders? What the liability of cloud provider? What will be suitable events to conquer these issues?

Insecure Cryptography: Attackers' can work out any cryptographic system or algorithm as main methods to hack them. It's general to find essential flaws in cryptographic algorithm which can twist strong encryption into feeble encryption or sometimes no encryption at all.

Data Protection and Portability: The cloud services are accessible based on a contract among client and a provider but what will happen when the contract is completed and client doesn't wants to continue anymore. Data security and portability remains as one of main weaknesses of cloud computing.

Vendor Lock-in: This vulnerability occurs due to immature providers and new business models which raise the risk of failure and going out of the trade. Lock in, makes a client dependent on a provider for products and services so they will be unable to deal with another provider without substantial switching costs.

Internet Dependency: Cloud computing is an internet dependent technology where users are accessing the services via web browser. What if internet is not accessible? What will happen to user systems and operations, which are very critical and need to run 24 hours such as Healthcare and Banking systems?

Illegal access to management interface: The cloud feature on-demand, self-service requires a management boundary that's accessible to cloud service users.

Unauthorized access to the management interface is therefore a particularly relevant vulnerability for cloud systems. Probability that unauthorized access could occur is much higher than for traditional systems where the management functionality is accessible only to a few administrators.

Cloud Threats [1]

(a) Abuse and Nefarious make use of of Cloud Computing
(b) Insecure appliance Programming Interfaces
(c) Malicious Insiders
(d) Shared Technology Vulnerabilities
(e) Data Loss/Leakage
(f) Account, Service & Traffic Hijacking
(g) Unknown Risk Profile

Abuse and Nefarious Use of Cloud Computing: Spammers, hackers and other criminals take advantage of the convenient listing, simple measures and reasonably unsigned access to cloud services to launch different attack. example of such attack consist of: password and key cracking; malicious data hosting; launching dynamic attack points; building rainbow tables;botnet command/control; and it basically targets: Infrastructure as a Service and Platform as a Service.

Insecure Application Programming Interfaces: Customers manage and interact with cloud services through interfaces or APIs. Provider must guarantee that security is included into their overhaul model, although user necessity is conscious of protection risk in the use, implementation, management, and monitoring of such services. Examples of such risks include: APIs dependencies; limited monitoring / logging capabilities; inflexible access controls; anonymous access; reusable tokens/passwords; clear-text authentication and/or transmission of content; and improper authorizations. Targets: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Malicious Insiders: Malicious insiders cause a larger threat in a cloud computing environment since clients do not have a clear view of supplier policies and actions. For example, employee access, worker monitor, strategy observance and hire values/practice are generally not transparent to customers. Malicious insiders can achieve unauthorized access

into organizations and their resources. Some threats contain product injure, economic force and defeat of production. Targets: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service).

Shared Technology Vulnerabilities: IaaS is based on shared infrastructure (e.g. disk partitions, CPU caches etc.), which is habitually not intended to accommodate a multi-tenant architecture. Without being seen flaws have allowed guest operating systems to gain unauthorized levels of control and/or influence on the platform. Targets: IaaS (Infrastructure as a Service).

Data Loss/Leakage: Compromised data may include: deleted or altered data without first making a backup; unlinking a record from a larger context; loss of an encoding key; and unauthorized access of sensitive data. The option of data compromise significantly increases in cloud computing caused by the structural design and operation. For instances of data loss/leakage issues include: insufficient authentication, authorization and audit (AAA) controls; inconsistent encryption; inconsistent software keys; operational failures; disposal challenges; risk of association; jurisdiction/political issues; persistence and eminence challenges; data center reliability; and disaster recovery. Targets: PaaS (Platform as a Service), SaaS (Software as a Service), IaaS (Infrastructure as a Service).

Account, Service & Traffic Hijacking: Account or service hijacking is usually carried out with stolen identification. Attacks include phishing, scheme and development of software vulnerabilities. Using stolen ID, attackers can access critical areas of cloud computing services and compromise confidently, integrity, and availability (CIA) of such services. Example of such attacks includes eavesdropping on transactions/sensitive activities, manipulation of data, returning flimsy information, redirection to dishonest sites.

Unknown Risk Profile: Cloud services mean that organizations are less involved with hardware and software ownership and maintenance. These offer important advantages, organizations should be aware that issues such as internal safety events, security acquiescence, and configuration harden; patching, auditing and logging may not be overlooked.

V. CONCLUSIONS

In this research paper we have discussed the cloud computing security and privacy which contains threats and vulnerabilities. Cloud computing has an energetic nature that is elastic, scalable and multi-shared with high capacity that gives an innovative shape of carrying out business. As the development of cloud computing, issue of security has become a top priority. This paper discusses the cloud computing vulnerabilities and data security.

ACKNOWLEDGMENT

The glory of accomplishing this research paper goes to our friends for their moral support. We have great thankful to our supervisor for encouraging us to write this paper.

REFERENCES

[1]. *Buyya R, Yeo CS, Venugopal S, Bromberg J,*

[2]. *Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering IT services As the 5th utility. Future Generation of Computer Systems 2009; 25: 599–616.*

[3]. *Cong Wang, Qian Wang, Kui Ren, Wenjing Lou "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE INFOCOM, March 2010, pp. 1-9.*

[4]. *CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" Cloud Security Alliance, 2009, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf,*

[5]. *J.Grimes, P., Jaeger, J., Lin, "Weathering the Storm: The Policy Implications of Cloud Computing" http://ischools.org/images/iConferences/CloudAbstract13109FINAL.pdf*
[6]. *S., Subashini, V. Kavitha. "A survey on security issues in service Delivery models of cloud computing". Journal of Network and Computer Applications, vol.34, pp.1-11, 2011.*
[7]. *T. Schreiber, "Session Riding a Widespread Vulnerability in Today's Web Applications" [Online], Available: http://www.securenet.de/papers/Session_Riding.pdf, white paper, 2004. [Accessed: 20-Jul-2011].*
[8]. *US National Institute for Standards and Technology (NIST) in 2009*
[9]. *Vaquero, L.M. et al. 'A Break in the Couds: Toward a Cloud Definition', ACM SIGCOMM Computer Communication Review, 2009/39(1):50–55.*
[10]. *www.opengroup.org/onlinepubs/9699919899/toc.pdf*

