© 2017 IJSRST | Volume 3 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Investigation on Security Challenges over a Cloud Computing

[1]Paladi Bhavani ,[2]Cholleti Jyothi

[1,2]Assistant Professor, Department of Computer Science and Engineering, TKR College of Engineering and Technology, Hyderabad, Telangana, India

ABSTRACT

Cloud computing is a better option for the organizations to take as their best option without any initial investment and day by day frequent and heavy use of cloud computing is increasing but despite all the benefits a cloud offers to an organization there are certain doubts and threats regarding the security issues associated with a cloud computing platform. The security issues mostly involve the external control over organizational structure and management and personal and private data of the organization can be compromised. Personal and private data in this computing environment has a very high risk of breach of confidentiality, integrity and data availability. Progression of cloud computing is mainly vulnerable due to these security concerns and challenges. This detailed study discusses about some of the challenges associated with cloud computing services and security issues related to this platform.

Keywords : Cloud Computing, Security, Integrity, Hybrid Cloud

I. INTRODUCTION

Growth of cloud computing have changed the entire scenario of computing applications in a very revolutionary way. Users in this new platform can access computing applications and network from a remote location whereas the computing infrastructure is located at some unknown and remote locations to which user has no control and direct access [7], [6], [10]. In this case user sends a request for any processing of data to a remotely located cloud infrastructure and when the remote server is done with the processing the output is again send back to the user. Data regarding the user interface with the cloud computing infrastructure may be stored on remote location either by the user itself or by the cloud computing software which makes the system vulnerable to the following cases (a) sending user's personal data to the cloud server (b) sending processed data back to user's systems from server computers (c) chance of storing user's personal data in the systems servers of cloud computing infrastructure which are not controlled and owned by the user. Due to these factors it is of high importance to have issues related to research and study of security aspects of cloud computing because only due to the above mentioned factors cloud computing becomes more susceptible to security threats. The main concept of the cloud computing is its infrastructure and the process of handling the user's requests where user take the computing resources on rent for the time of his usage and resources always remain somewhere else with ownership of someone else [4], [9], [8]. By means of unwanted breach into the systems using different methods of hacking, it is always possible to access personal data in cloud computing. Cloud computing cannot avoid this to happen due to its approach and nature of its process. Secure cloud computing cannot be considered as a single step process but it is an ongoing process which makes it compulsory to analyze security of the cloud computing as a compulsory practice [6], [10], [9], [8], [28], [11], [12]. The present study focuses on the safe implementation of the cloud based computing infrastructure and to address issues of secure usage of this new facility. Various security issues involved in cloud computing implementation have also been discussed and discussion regarding the authentication of cloud computing has also been taken care of with a view to keep integrity in security of cloud computing.

II. METHODS AND MATERIAL

1. Security issues in a Cloud

Recently the "Cloud Security Spotlight Report" showed that "90 percent of organizations are very or moderately concerned about public cloud security." These concerns run the gamut from vulnerability to hijacked accounts to malicious insiders to full-scale data breaches.

Following are the major security issues concern

Data Breaches: Cloud computing and services are relatively new, yet data breaches in all forms have existed for years. The question remains: "With sensitive data being stored online rather than on premise, is the cloud inherently less safe?"

Hijacking of Accounts: Attackers now have the ability to use your (or your employees') login information to remotely access sensitive data stored on the cloud; additionally, attackers can falsify and manipulate information through hijacked credentials. Other methods of hijacking include scripting bugs and reused passwords, which allow attackers to easily and often without detection steal credentials Insider Threat: An attack from inside your organization may seem unlikely, but the insider threat does exist. Employees can use their authorized access to an organization's cloud-based services to misuse or access information such as customer accounts, financial forms, and other sensitive information.

Malware Injection: Malware injections are scripts or code embedded into cloud services that act as "valid instances" and run as SaaS to cloud servers. This means that malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves.

Misuse of Cloud Services: hackers and authorized users to easily host and spread malware, illegal software, and other digital properties.

Insecure APIs: Application Programming Interfaces (API) give users the opportunity to customize their cloud experience.However, APIs can be a threat to cloud security because of their very nature. Not only do they give companies the ability to customize features of their cloud services to fit business needs, but they also authenticate, provide access, and effect encryption.

Denial of Service Attacks: Unlike other kind of cyberattacks, which are typically launched to establish a long-term foothold and hijack sensitive information, denial of service assaults do not attempt to breach your security perimeter. Rather, they attempt to make your website and servers unavailable to legitimate users.

Data Loss: Data on cloud services can be lost through a malicious attack, natural disaster, or a data wipe by the service provider. Losing vital information can be devastating to businesses that don't have a recovery plan

Insufficient identity, credential, and access management: Bad actors masquerading as legitimate users, operators, or developers can read, modify, and delete data; issue control plane and management functions; snoop on data in transit or release malicious software that appears to originate from a legitimate source,

Advanced persistent threats (APTs): APTs are a parasitical form of cyber-attack that infiltrates systems to establish a foothold in the IT infrastructure of target companies, from which they steal data. APTs pursue their goals stealthily over extended periods of time, often adapting to the security measures intended to defend against them. Once in place, APTs can move laterally through data center networks and blend in with normal network traffic to achieve their objectives.

2. Cloud Deployment Models

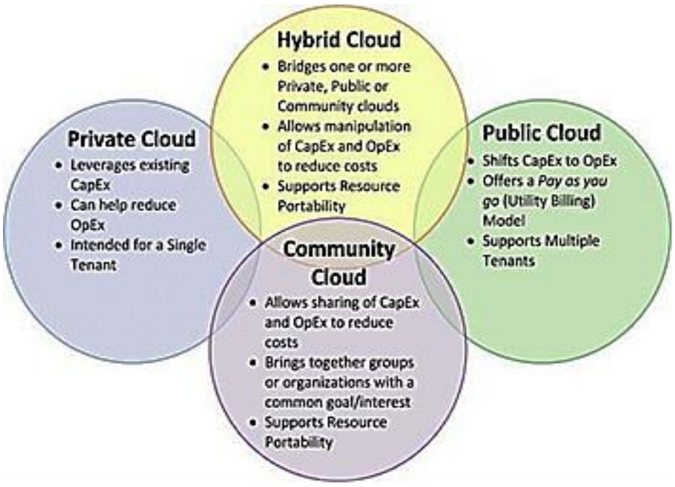
Hybrid Cloud
• Bridges one or more Private, Public or Community clouds
• Allows manipulation of CapEx and OpEx to reduce costs
• Supports Resource Portability
Private Cloud
• Leverages existing CapEx
• Can help reduce OpEx
• Intended for a Single Tenant
Public Cloud
• Shifts CapEx to OpEx
• Offers a Pay as you go (Utility Billing) Model
• Supports Multiple Tenants
Community Cloud
• Allows sharing of CapEx and OpEx to reduce costs
• Brings together groups or organizations with a common goal/interest
• Supports Resource Portability

Figure 1. Cloud Deployment Models

According to National Institute of Standards and Technology (NIST) there are four set of deployment models as shown in figure 1 [1],[22].

(a) Public Cloud –here cloud infrastructure is accessed and managed by any outside organization or any third party service providers. These are less secure in comparison to other models due to the fact that applications and data shared on a public cloud are not always under attack. This model is flexible enough to address random demand for optimization of cloud environment [16].

- Private Cloud – here any private organization manages and operates this model which ensures the consistent security and private issues of cloud computing. In this model infrastructure and applications are pooled together for sharing among its users. Here cloud resources and applications are managed by the organization itself who is implementing this cloud. This is more secure because of its internal usage as only own organization and specified users only can access the services offered by the cloud infrastructure [15].
- Community Cloud - here cloud computing infrastructure is shared among members from a specific community or organizations with common issues regarding security, projects, applications, research and jurisdiction because of the requirement of a shared and common central cloud computing facility irrespective of the solution needed. Community cloud can be considered as a cluster of private clouds.
- Hybrid Cloud – here two or more cloud computing models are combined to form a composite cloud but individually their internal properties remain intact. Here two or more clouds are linked to external cloud services which are centrally managed, considered as a single unit and a secure network takes care of all the clouds inside it [17]. Hybrid cloud can provide virtual cloud services by using all the facilities available in its cluster of private and public clouds and provide more secure control of data and applications to make information access possible through internet.Various aspects of security and service providers for all the four deployments models for a cloud computing system is described in table 1.

Table 1. Cloud Computing Deployment Models

Models	Managed By	Infrastructure		Accessible and Consumed By
		Owned By	Located	
Public	Third Party Provider	Third Party Provider	Off Premises	Un-trusted
Private	Organization	Organization	On Premises	Trusted
	Third Party Provider	Third Party Provider	Off Premises	
Community	Third Party Provider	Third Party Provider	On Premises	Trusted & Un-trusted
Hybrid	Organization & Third Party Provider	Organization & Third Party Provider	Off Premises & On Premises	

Service Delivery Models for a Cloud Computing

While implementing a cloud, its platform, storage, software and networking infrastructure is provided as its services which can be made flexible according to the requirements of the user as shown in the Figure 2.

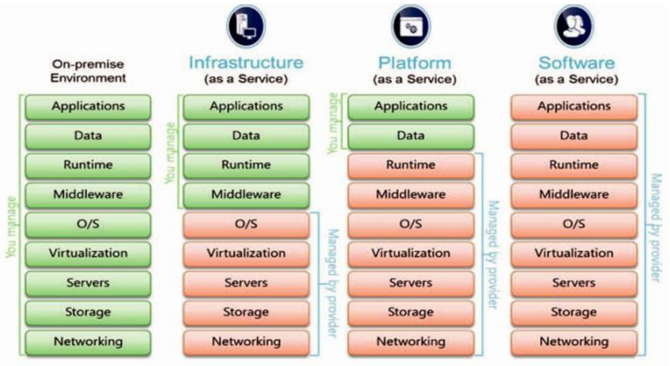

Figure 2. Service Model for delivery of a Cloud Computing Model

Infrastructure as a Service (IaaS) – here central and dedicated resources are shared with contracted clients only at pay-per-use charge to minimize huge initial cost of establishing the cloud which saves a lot amount of money from installing separate servers, networking devices and processing power. Here the basic advantage is to add or remove any application with ease and cost effective manner [13].Though cost is the deciding factor for a cloud to implement but IaaS provides only basic security and it will require a higher level of security mechanism for applications moving into the cloud. Amazon and GoGrid leased their virtual servers under IaaS.

Platform as a service (PaaS) – in this platform software and development tools are provided on the service provider's system. It helps to develop applications without having knowledge of internal procedures and processes of cloud computing system. PaaS offers a full software development environment from planning, designing, testing and implementing it to client side. Here all virtual machines should be made secure from malicious attacks. Cloud middleware WOLF and Windows Azure are under this platform.

Software as a Service (SaaS) – here application are hosted by any vendor and customers can access these applications over a network. SaaS is more popular delivery model because of its support to web services and service oriented architecture (SOA). It usually works on the model of pay-as-you-go to subscription model. SaaS offers an architecture which allows many simultaneous users i.e. multi-tenancy. Here security of the web browser is vital and important because software is generally accessed using a web browser. Some of the mechanisms available for data protection on the cloud are Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options. Examples of SaaS are Facebook and SalesForce

III. RESULTS AND DISCUSSION

Cloud Computing Challenges

Security: it is the most important issue in making cloud popular and most used with application. Still for a user it is a most concerned task to use his private data on other's network, running his software on other's platform. There have been cases of data loss, phishing, running remotely on a cluster of machines (botnet) in case of cloud computing and these are still a problem which is the most sought after issue in using cloud computing securely. For attackers it is very convenient and cost effective to initiate their attack using services available on a cloud infrastructure [14].

Cost model: on one hand cloud computing reduces the cost of infrastructure; it increases the cost of data communication on the other hand. The cost of implementation is even more in hybrid cloud deployment model [14].

Charge Model: cloud offers very elastic cost model due to which cost analysis has become more complex. Its multi-tenancy approach cost in huge sums in SaaS deployment because of its responsibility of re-design and re-development of software and hence cost of providing new features, performance and security encouragements raises the overall charge model. Hence it is very important to have a suitable charge model in case of Saas model [14].

Service Level Agreement (SLA): to ensure the quality, availability, performance and reliability of the resources, users need to have a Service Level

Agreement (SLA) from the service provider to ensure all these issues. SLA must ensure maximum

Issue of Migration: organizations still have concern over security and privacy issues in migrating to cloud services. At present information technology management and application related to personal use are easily movable application to cloud platform. Here organizations prefer SaaS over IaaS because of the fact that many of the marginal functions are outsourced to the cloud environment whereas basic and core applications are kept in own control. This also shows that almost 31.5% of the organization will move to cloud computing for their storage needs in the next three years but still it is to be improved a lot [24].

Issue of Cloud inter-operability: this a feature which ensures smooth data flow across different clouds and application within that or data flow between local applications. Inter-operability operates through various levels like optimizing assets and computing resources of cloud for which any organization is paying and need to put their core applications intact within their secured periphery and another level is like to outsource marginal functions of an organization to cloud service from other vendors[29].

IV. CONCLUSION

Adoption of cloud computing system as a necessity is always under threat from security issues where cloud systems are more prone to attacks from unauthorized users or unwanted activities from outside or inside of the cloud. Before actually moving into a cloud infrastructure, it must be ensured that proper security measures have been taken in to account or not. It is a proved and verified fact that cloud computing platform provides a cost effective mechanism to share hardware and software resources and it has ability to scale up or down according to the requirements of user. The charges are almost zero if user is not using the facilities. In this paper risks of security incorporated in cloud computing environment such as Confidentiality, Integrity, Availability and Authenticity (CIAA) and issues like DoS, network security, data security and locality in SaaS models, network and host intrusion in PaaS and IaaS also have been discussed

V. REFERENCES

[1]. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," US Nat'l Inst. of Science and Technology, 2011; http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[2]. "Security Guidance for Critical Areas of Focus in Cloud Computing", Cloud Security Alliance, Dec. 2009; https://cloudsecurityalliance.org/csaguide.pdf.

[3]. T. Ristenpart et al., "Hey, You, Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Communications Security (CCS 09), ACM Press, 2009, pp. 199–212.

[4]. Bisong, A. and Rahman, S.S.M. (2011), "An Overview of the Security Concerns in Enterprise Cloud Computing", International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103.

[5]. Kuyoro, S.O., Ibikunle, F. and Awodele, O. (2011), "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks, 3(5), 247-255.

[6]. Ogigau-Neamtiu, F. (2012), "Cloud Computing Security Issues", Journal of Defense Resource Management, 3(2), 141-148.

[7]. Petre, R. (2012), "Data mining in Cloud Computing", Database Systems Journal, 3(3), 67-71.

[8]. Qaisar, S. and Khawaja, K.F. (2012), "Cloud Computing: Network/Security Threats and

Countermeasures", Interdisciplinary Journal of Contemporary Research in Business, 3(9), 1323-1329.

[9]. Rashmi, Sahoo, G. and Mehfuz, S. (2013), "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", International Journal on Cloud Computing: Services and Architecture, 3(4), 1-11. Doi: 10.5121/ijccsa.2013.3401.

[10]. Singh, S. and Jangwal, T. (2012), "Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues", International Journal of Computer Science & Information Technology, 4(2), 17-31.

[11]. Suresh, K.S. and Prasad, K.V. (2012), "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, 2(10), 110-114.

[12]. Youssef, A.E. (2012), "Exploring Cloud Computing Services and Applications", Journal of Emerging Trends in Computing and Information Sciences, 3(6), 838-847.

[13]. J. Brodkin. (2008, Jun.), "Gartner: Seven cloud-computing security risks", Infoworld, Available: <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853?page=0,1> [Mar. 13, 2009].

[14]. S. Ramgovind, M. M. Eloff, E. Smith, "The Management of Security in Cloud Computing", In PROC 2010 IEEE International Conference on Cloud Computing 2010.

[15]. S. Arnold (2009, Jul.), "Cloud computing and the issue of privacy", KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[16]. A Platform Computing Whitepaper, "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010.

[17]. Global Netoptex Incorporated, "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

[18]. C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser, "Business Models in the Service World." IT Professional, vol. 11, pp. 28-33, 2009.

[19]. M.Carroll, A.Van der Merwe, P.Kotze, "Secure cloud computing: Benefits, risks and controls", Information Security South Africa (ISSA), pp. 1-9, September 2011.

[20]. S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol. 34, Issue 1, pp. 1-11, July 2010.

[21]. D. Zissis, D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, 2011.

[22]. National Institute of Standards and Technology, "NIST Cloud Computing Program, 2010", <http://www.nist.gov/itl/cloud/> [Accessed on: 18 October 2011].

[23]. Grobauer, T. Walloschek, E. Stocker, "Understanding Cloud Computing Vulnerabilities, Security & Privacy", IEEE, vol. 9, Issue 2, pp. 50-57, March 2011.

[24]. F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010]. (http://techcrunch.com/2010/06/15/ipad-breach-personal-data/).

[25]. Mr. M. VEERABRAHMA CHARY, Mrs.N.SUJATHA," A Novel Additive Multi-Keyword Search for Multiple Data Owners in Cloud Computing ." International Journal of Computer Engineering In Research Trends., vol.3, no.6, pp. 308-313, 2016.

[26]. G.Lucy, D.Jaya Narayana Reddy, R.Sandeep Kumar," Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data." International Journal of Computer Engineering In Research Trends., vol.2, no.12, pp. 919- 923, 2015.

[27]. G.Dileep Kumar, A.Sreenivasa Rao," PrivacyPreserving Public Auditing using TPA for Secure Searchable Cloud Storage data." International Journal of Computer Engineering In Research Trends., vol.2, no.11, pp. 767-770, 2015.

[28]. N. Meghasree, U.Veeresh, Dr.S.Prem Kumar," Multi Cloud Architecture to Provide Data Privacy and Integrity." International Journal of Computer Engineering In Research Trends., vol.2, no.9, pp. 558- 564, 2015.

[29]. P.FARZANA, A.HARSHAVARDHAN," Integrity Auditing for Outsourced Dynamic Cloud Data with Group User Revocation." International Journal of Computer Engineering In Research Trends., vol.2, no.11, pp. 877-881, 2015.