Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Prediction of Security Issues Associated With the Cloud, Its Various Dimensions and Different Cloud Security Control As a Advanced Research Used in Computer Science and Electronics Engineering

[1]Er. Kapila Purohit, [2]Er. Bhawna Sharma, [3]Er. Bhubneshwar Sharma
[1, 2] M.Tech Student, Department of Computer Science and Engineering, Arni University, H.P., India
[3] Assistant Professor, Department of Electronics and Communication Engineering, Arni University, H.P., India

Abstract: Cloud Computing appears as a computational paradigm as well as a distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing Cloud Computing combines a number of computers.

Keywords: Cloud computing, its potentials, and computing resources.

I. CLOUD COMPUTING SECURITY ISSUES

Security concerns relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form Security controls in Cloud Computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, Cloud Computing may present different risks to an organization than traditional IT solutions. Unfortunately, integrating security into these solutions is often perceived as making them more rigid as shown in diagram 1 .Moving critical applications and sensitive data to public cloud environments is of great concern for those corporations that are moving from one point to other.

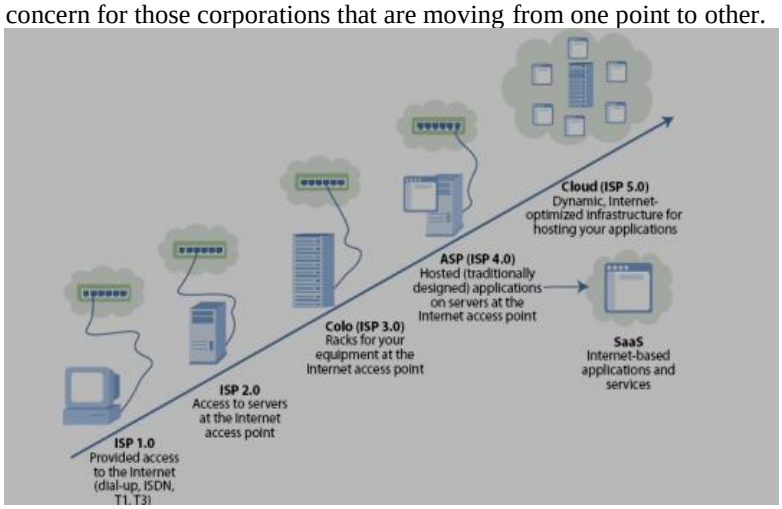

Figure1 Diagram for cloud computing hosting

1. Some members of Open Data Center Alliance, a consortium that includes top IT companies of the world such as SAP, Infosys, Deutsche Telekom, Disney and more, are believed to be cloud enthusiasts. However, a recent survey of the members reveal that around 66 percent of the consortium's members are concerned regarding data security, which is deferring their efforts for cloud computing. A similar survey done in previous years indicated that around 80 percent of the members were skeptic about entering cloud computing due to security concerns.
2. Security issues over cloud computing is definitely one of the major concerns that many companies are trying to recognize. However, some companies are also concerned about regulatory issues. Market observers say that 47 percent of the participants in the survey worry that they will be tied to one provider of cloud storage as shown in diagram 2.
3. Amazon Web Services is a prominent cloud computing provider in the industry. The department is the fastest growing department of Amazon. However, in Oct. 2012, services failed for a while. Users who had their files stored with Amazon Web Services were unable to access their documents.

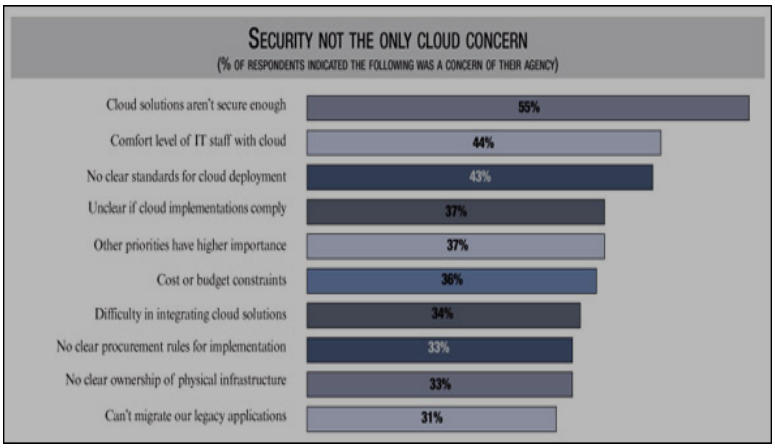

Figure 2. Security not the cloud concern

II. SECURITY VISIBILITY AND ITS DIMENSIONS

1. The paucity of security visibility that most providers offer their customers is itself getting plenty of visibility [1]. Obviously, when using a public cloud service, companies must balance the competing factors of control, visibility and cost. This can be a significant issue—reduced visibility results in diminished situational awareness and a questionable understanding of risk. When planning a move to the cloud, an organization needs to recognize this lack of visibility and determine how to best leverage what insight they can get their hands on. Really, this means designing mitigating controls [2].
2. At the infrastructure and platform levels, this is straightforward: Log more information in your applications and set systems up to generate alerts when signs of compromise or malicious use are spotted (for example, when files are modified, records are changed more frequently than usual, or resource usage is abnormally high). For software as a service (SaaS), though, these precautions will require more thought. SaaS providers are beginning to distinguish themselves via security features. Organizations vetting SaaS providers should consider how they will handle risk awareness—does the provider offer usage data that is granular enough to recognize changes in usage? (Monthly billing doesn't really cut it, unless the risk scenario is a malefactor who only attacks on the 29th of the month.)
3. If a malicious user attempts to access data stored in the cloud, how will the company learn of this? If sensitive data is modified or destroyed, is there a way for you to be notified quickly? Frequently, providers will offer a wider variety of information via an API than they do in their dashboard [3]. While this does require that you get code written that can leverage the API, modern APIs are usually easy to work with, and the information you gain as a result will be valuable to risk-sensitive organizations.

III. CLOUD SECURITY ARCHITECURE

Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management [4] the security management address these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind cloud security architecture, they can usually be found in one of the following categories

1. Deterrent controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. [Some consider them a subset of preventive controls [5]

2. Preventive controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified [6].

3. Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue. System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure [7].

4. Corrective controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control [8].

IV. CLOUD SECURITY CONTROLS

It is generally recommended that information security controls be selected and implemented according and in proportion to the risks, typically by assessing the threats, vulnerabilities and impacts [10]. While cloud security concerns can be grouped into any number of dimensions (e.g. Gartner named seven while the it is being identified fourteen areas of concern), three are outlined below in diagram 3.

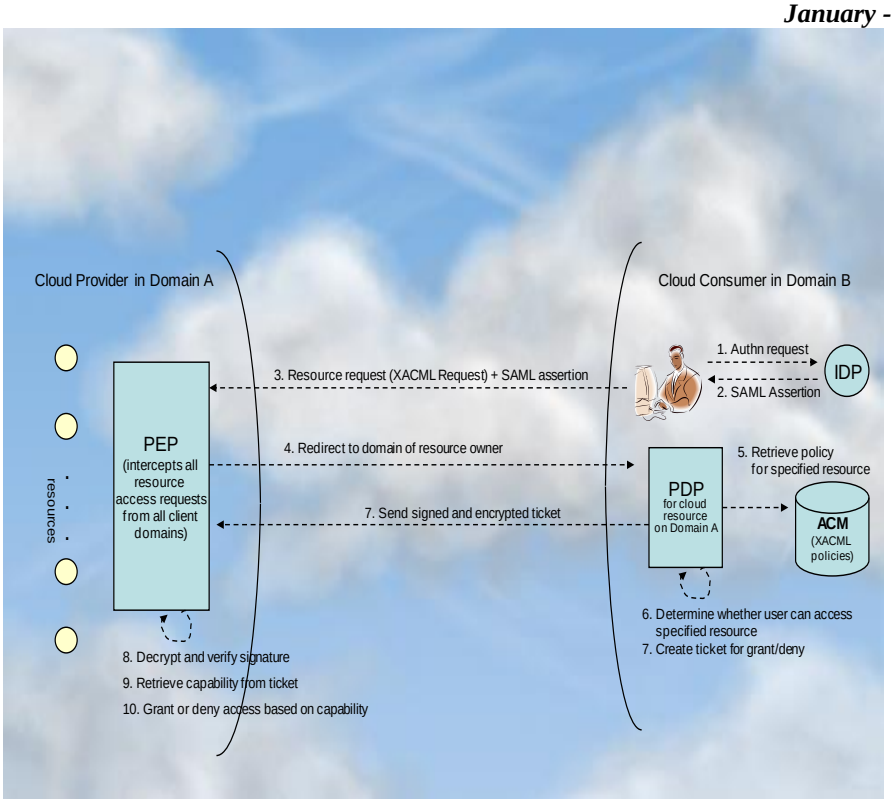

Figure3. Diagram of cloud provider and cloud consumer

V. CONCLUSION

Cloud computing is considered to be the best technology for knowing various issues related to security and various controls and its dimensions. With the passage of next four to five years we will see this technology be the best technology for understanding all aspects for its control.

REFERENCES

[1] Mather, Tim; Kumaraswamy, Subra; Latif, Shahed (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc. ISBN 9780596802769.

[2] Winkler, Vic (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Elsevier. ISBN 9781597495929.

[3] Ottenheimer, Davi (2012). Securing the Virtual Environment: How to Defend the Enterprise Against Attack. Wiley. ISBN 9781118155486.

[4] Chandramouli R, Mell P (2010) State of Security readiness. Crossroads 16(3):23-25

[5] Jaeger T, Schiffman J (2010) Outlook: cloudy with a chance of Security challenges and improvements. IEEE Security Privacy 8(1):77-80

[6] Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security: Challenges and solutions. In: the 7th International Conference on Informatics and Systems (INFOS), Potsdam, Germany. Washington, DC, USA: IEEE Computer Society. pp 1-8

[7] Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. Washington, DC, USA: IEEE Computer Society. pp 35-41

[8] Wu H, Ding Y, Winer C, Yao L (2010) Network Security for virtual machine in Cloud Computing. In: 5th International conference on computer sciences and convergence information technology (ICCIT). DC, USA: IEEE Computer Society Washington. pp 18-21

[9] Xiaopeng G, Sumei W, Xianqin C (2010) VNSS: a Network Security sandbox for virtual Computing environment. In: IEEE youth conference on information Computing and telecommunications (YC-ICT). Washington DC, USA: IEEE Computer Society. pp 395-398

[10] Popovic K, Hocenski Z (2010) Cloud Computing Security issues and challenges. In: Proceedings of the 33rd International convention MIPRO. IEEE Computer Society Washington DC, USA. pp 344-349

AUTHORS BIBLIOGRAPHY

Er. Kapila Purohit received Bachelor's Degree in Computer Science Engineering from School of Engineering & Technology, Bapror (Rajpura) and pursuing her master's degree in Computer Science and Engineering Department from Arni University Kathgarh, Indora, (H.P) she pursues a broad range of research interests that include DBMS, RDBMS, Software Engineering, Expert System.

Er. Bhawana Sharma received Bachelor's Degree in Computer Science Engineering Arni University Kathgarh,Indora,(H.P) and pursuing her master's degree in Computer Science and Engineering Department from Arni University Kathgarh,Indora,(H.P) she pursues a broad range of research interests that include software engg , web technology, network programming

Er. Bhubneshwar Sharma was born in 1986. He received Bachelor's Degree in Electronics and Communication Engineering from Jammu University in 2007 and received Master's degree in Electronics and Communication Department from Punjab in 2009. He is currently working as Assistant Professor in the Department of Electronics and Communication Engineering in Arni University, Himachal Pradesh, India. He has published research papers in International Journals and presented his work at conferences. He pursues a broad range of research interests that include Digital signal processing, neural networks, Wireless sensor networks. He has also got certificates of publication of their research work.

