Dr. T. Uma Devi et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 1, March 2018, pp. 315-318

Analysis report on cloud generic security challenges and its possible solutions with limitations

Dr T. Uma Devi[1], K.Venkateswara Rao[2]

[1]Associate Professor, GIS-GITAM University, VIZAG,
[2]Research Scholar, GIS-GITAM University, VIZAG,

Abstract: Today Cloud computing became a backbone for many enterprise and personal applications, by providing the efficient and scalable services as SaaS, PaaS and IaaS. On Demand consumption, pay per use billing policy and sophisticated network and internal architecture made this cloud more interesting. To catch up the advantages of cloud many application managers started cloud adoption in recent years. Although the cloud users are happy about cloud services and support, they are still thinking about cloud adoption due to the main reason cloud security and privacy, which was revealed by many researches and surveys. Managing cloud user's application data, process, storage and infrastructure at cloud service provider's side is leading to have many doubts on service provider accuracy, reliability and trustworthiness. There are several factors from cloud computing privacy and security, which impacts on service provider trustworthiness are Data privacy and Security, Recovery Management, Virtual Machine Security, Data Availability and Integrity etc. In this cloud analysis paper, we presented the detailed description about the security challenges in cloud. My research analysis outlined this information, which helps in understanding about each cloud security concept with possible solutions and their limitations. As part of my research on cloud privacy and security, this analysis helps me in choosing the research theme, aim and scope by considering all challenges.

Keywords: cloud computing, privacy and security, security challenges, Data security, security proposals

I. INTRODUCTION

The NIST Definition [1] Cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.After the cloud architecture designed by NIST, the characteristics has been exhibited by the cloud computing as follows:

Pay per use service: In this procedure the billing happens based on the amount of utilization of cloud resources and services. This kind of billing attracted the middle class entrepreneurs to adopt the cloud services for their real time applications.

On-Demand Resources: Instead of reserving a certain amount of resources for a process, using on-demand mechanism cloud allocates the required amount of resources (memory, processor speed, storage, network resources, band width etc.) to the customer applications. This method not only saves the resources, but also supports the efficient utilization of cloud resources.

Rapid Elasticity: As per the need of resources for processing, they will be allocated in cloud real time execution. The sudden high demand and low demand of resources are balanced using this rapid elasticity feature.

Resource Pooling: Behalf of static allocation of resources to the running cloud applications, cloud introduced the resource pooling mechanism by integrating all the available resources like memory, storage and process. As per need the resources will be allocated using the state of the art algorithms to manage the resources efficiently and to balance the load on cloud.

Although the features and characteristics of cloud are attracting, still the adoption ratio and percentage are very less than the expectations by market analysts. The main reason for this less adoption ratio is trustworthiness on cloud architecture due to the privacy and security challenges [2]. As on privacy and security of cloud data cannot be assured by any service provider. Since beginning, the real time cloud incidents on privacy and security also proving the same.

As per the cloud environment design cloud service provider is responsible for data processing and storage. Managing cloud user's application data, process, storage and infrastructure at cloud service provider's side is leading to have many doubts on service provider accuracy, reliability and trustworthiness [3]. Cloud service provider may be honest but curious (HBC) in accessing cloud data and attributes. Apart from service providers trustworthiness issue, there are several factors from cloud privacy and security, which impacts on providers trustworthiness are SLA Agreements, Security Breaches, Recovery Management, Data privacy and Security, Virtual Machine Security, Data Availability and Integrity etc. Several past researches, surveys and fellow scholars are concluded the above mentioned cloud privacy and security challenges, which has to be address by the upcoming research's on cloud computing. Through understanding about the cloud computing

privacy and security challenges, is very important before addressing them with respective solutions.

In this cloud analysis paper, we presented the detailed description about the security challenges in cloud. My research analysis outlined this information, which helps in understanding about each cloud security concept with possible solutions and their limitations. Second sections describes the literature review, third section discusses about the cloud privacy and security challenges and currently available solutions in detail, whereas fourth section concludes the paper.

II. LITERATURE REVIEW

In this section, we discuss about the cloud service models designed and approved by NIST[1]. We can do classify the proposed privacy and security challenges [2] based on the possible cloud service models. NIST approved cloud service major models are SaaS, IaaS and PaaS.

Each service model is providing its own services and characteristics to the relevant end users. Based on the service offered by the service models [1], we can do identify the possible cloud privacy and security challenges [3].This section discusses about the possible security problems in cloud service models.

Infrastructure as a service (IaaS): This cloud service model is providing the raw hardware environment for cloud customers. Server systems (Processors), virtual machines, Storage disks, operating systems, high speed networks and utilities are givenon pay per use rental basis for cloud customers. Cloud users (cloud application owners) are responsible for utilizing the raw hardware services by wrapping up the high level facilities like platforms and software's. As IaaS is providing very low level of services, the security risks also less when compared to other services but they are significant. Some popular IaaS services available in today IT market are oracle itual box, Xen, Hyper-V and VM Ware etc.

As provider and consumer both are managing the infrastructure after any threat, identification of the person who done attack became complex. Any infrastructure (hardware) component compromised to attacks effects on total cloud reliability. So here, provider should thoroughly test infrastructure components in various degrees to ensure its security before offering services to customers.

Platform as a service (PaaS): In this service model of cloud, along with infrastructure services, it provides operating systems, middle wares and dynamic runtime environments to make the job of cloud migration feasible for cloud customer. With PaaS cloud customer just need to deploy the application on top of the ready to deploy platform without thinking about any other components. As this is providing more services, there is a chance of occur more vulnerabilities in this service model. Google App Engine and Microsoft Azure are the best examples of Platform as service models of cloud.

The scope of service provider controlling environment has been increased with this model, which cause to raising uncertainties on cloud service provider. In this case service consumer limited to his application data and security management.

Software as a service (SaaS): In this model of cloud, the entire application will be managed by the cloud service provider, cloud customer just a responsible person/organization for their cloud end users. All subscribed users can access this SaaS model services on demand through internet. End users need to send the raw data as input to process and return the results back by SaaS. As data is also handling by the service provider in this service model, so there are even more chances of having malicious attacks on cloud to compromise privacy and security of users. Office-365, Net Suite, Google Docs are the best examples of SaaS application.

Satisfying the SLA agreements to assure the quality of service, implementing the anonymous policies to made good governance, following the privacy policies to make the services compliance, defending the internal and external attacks to assure the security are the mainly focusable areas of cloud SaaS model.

III. CLOUD SECURITY CHALLENGES AND POSSIBLE SOLUTIONS WITH LIMITATIONS

In this section we discuss about the generic security challenges of cloud in a detailed manner. The term generic we have used to clarify that, these challenges are limited to neither specific service model nor deployment model. These challenges are common occurrences of all cloud environments at different phases of design and implementation. Henceforth, each cloud provider should concentrate on these challenges to make their cloud secure.

There are several factors from cloud computing privacy and security, which impacts on service provider trustworthiness are SLA Agreements, Security Breaches, Recovery Management, Data privacy and Security, Virtual Machine Security, Data Availability and Integrity etc. In this cloud analysis paper, we presented the detailed description about the security challenges in cloud. My research analysis outlined this information, which helps in understanding about each cloud security concept with possible solutions and their limitations.

Data Privacy and Security: Since beginning of cloud, there has been lot of focus on this area by former researchers [4, 5, 6] due to its importance in real life. Data privacy and security defines that the data which is received, processed and stored in cloud should be defended from unauthorized access and malicious attacks either from internal or external environment of cloud. In general datastored in public clouds is sharable among multiple clients. The sensitive and regulated data of cloud access mechanism should be kept under secure policies. There are several practices are following today to assure the privacy and security of cloud data are Encryption methods, Data Isolation, Data Sanitization, PKI based authentications etc. Although these methods are having some capability to control the malicious attacks on cloud data, they are suffering from their own limitations, which become obstacles to adopt them in cloud with full-fledged manner.

Erase and Recovery Management: Data stored in cloud on persistence basis has to be removed on demand by data owner. In general the sensitive and processed information stored on cloud storage units, which is very valuable and private (personal). This erasing process of data should be confirmed by cloud service provider and also audited by the third party to ensure that the data has been completely removed (purged) from data storage units. If the erasing process not happened properly, leads to recover the erased sensitive data from storage units is called as data theft.

To avoid theft of data from storage units in case of recovery and to ensure the execution of purging process, present cloud architects are suggesting the third party auditing's, data overriding techniques and data breaking mechanisms. Earlier proposed third party auditing's subject to trustworthiness and data revealing of cloud. Later introduced data overriding techniques [1, 3] helps in overriding the deleted content with some random text after deletion of data from disk segments. In case of huge deletions of data from storage unit, cloud has to run a long overriding task which is extra burden on cloud processor. The final data breaking process after data deletion also suffers from managing the segments begin and end points, maintaining the track of segments on disk, identifying the storage relations among segments became hurdles for implementing this data breaking process.

Virtual Machine Security: Today cloud architectures are mainly promoting the virtual data processing techniques by creating the virtual machines [7, 8] as processing nodes from remote systems. These virtual machines made the process models loosely coupled and on-demand switchable among several running jobs. These virtual machines created a new layer in traditional cloud architecture to introduce remote data processing capabilities and distribution of data processing among nodes. Virtual machines, virtual storage units, abstracted resources and virtualization management systems are the main components of the newly introduced virtual layer. Although this virtual machine is making the data process job feasible, it opens the new windows to attackers to target the attacks on executing data. Protecting these virtual machines from adversaries remains a big challenging task till today.

There are several methodologies were proposed by former researchers to secure the virtual machines of cloudare Hypervisors, virtual network protection systems, intelligent and knowledge based attack monitors etc.Hypervisors are the inbuilt monitoring systems of cloud, which are scheduling and tracing the virtual machines all the time. Later these hypervisors are moderated as security checkpoints to monitor the activities of virtual machines to ensure the identification of malicious activities. This hypervisor is limited to identify the activities, which are happening inside the cloud. Virtual network protection systems are external collection of components which are appointed for monitoring the external behavior of virtual machines in a cloud environment. it works like as a third party auditing on cloud data management. Like other external monitoring systems, virtual network protection systems cannot insist into the internal activities of virtual networks. This is the main limitation, which made this protection system remains unreliable and dependable.Recently Intelligent and Knowledge based unsupervised attack monitoring systems [7] were introduced in cloud environment. These systems monitors the activity log of cloud environment and implements the analysis using cyclic graph models. This is a clear analysis model, which pinpoints each activity of cloud with detailed analysis using its unsupervised learning methods. Providing the useful and reliable data as training input data is very important in this analysis model. It can only recognizes existed problems using training data where as it needs some knowledge to identify the new bugs. Predication of upcoming bugs is not possible with the knowledge based supervised attack models, which helps in prevention of attacks from second time onwards.

These are today prominent generic security challengesof cloud among several. The lack of research on these challenges leads the cloud as insecure and unreliable. If we proposed the fine grained solutions to these cloud security challenges the chances of cloud adoption with reliability increases more.

IV. CONCLUSION

Many IT surveys and statistics are confirmed that Cloud Computing is a rising technology today.Need of Cloud Computing and it's importance, wide utilization and adoption statistics, extreme low cost services with high quality, future demands and research gaps are opened the gates for research scholars. Most of the survey's on cloud adoption revealed that "Cloud Security and Privacy challenges" are the main obstacle in cloud service adoption and migration. There are several factors from cloud computing privacy and security, which impacts on service provider trustworthiness areData privacy and Security, Recovery Management, Virtual Machine Security, Data Availability and Integrity etc. In this cloud analysis paper, we presented the detailed description about the security challenges in cloud. My research analysis outlined this information, which helps in understanding about each cloud security concept with possible solutions and their limitations.

V. REFERENCES

[1]. NIST Cloud Computing Reference Architecture, September 2016 by NIST.

[2]. B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[3]. Meiko Jensen, JorgSchwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[4]. X. Zhang, N. Wuwong, H. Li, and X. J. Zhang, "InformationSecurity Risk Management Framework for the Cloud Computing Environments", In

Proceedings of 10th IEEE International Conference on Computer and Information Technology, pp. 1328-1334, 2010.

[5]. K. Ren, C. Wang, and Q. Wang, "Security challenges for the publiccloud," Internet Computing, IEEE, vol. 16, no. 1, jan.-feb. 2012, pp. 69–73.

[6]. D. Fernandes, L. Soares, J. Gomes, M. Freire, and P. Incio,"Security issues in cloud environments: a survey," InternationalJournal of Information Security, vol. 13, no. 2, 2014, pp. 113–170.

[7]. R. B. Uriarte and C. B. Westphall, "Panoptes: A monitoring architectureand framework for supporting autonomic clouds," in Network Operations and Management Symposium (NOMS), 2014 IEEE. IEEE, 2014,pp. 1–5.

[8]. K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusiondetection for grid and cloud computing," IT Professional, vol. 12, no. 4,2010, pp. 38–43.

