A Survey on the Security Issues in Cloud Computing

B.Vani [#1], R.Cynthia Monica Priya[*2]
[1]Asst.Professor, Shrimad Andavan Arts and Science College, Trichy, India
[2]Asst.Professor, Bishop Heber College, Trichy, India

***Abstract*—** Cloud computing is a recent paradigm that deals with hosting and delivering services over the internet. Its knack to reduce both the software and hardware costs makes it more familiar. Virtualization provides the end users a variety of services from the hardware to the application level. The pay per use is the most distinguished feature. The facility to scale the computing infrastructure up and down is another remarkable feature. Location transparency, resource pooling, ubiquitous network access are the other important characteristics of cloud computing. Anything that grows popular suffers from certain weakness. This paper makes a survey on the various security issues such as confidentiality, integrity and availability. The various threats that may take over and the available defense strategies for each issue have been surveyed.

Keywords—*availability, cloud computing, confidentiality, integrity, security.*

I. INTRODUCTION

Cloud computing remains a model for establishing a convenient, on–demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or interaction by the service provider [1]. Cloud computing refers to both applications provided as services over the internet and the systems software and hardware that contribute those services.

A. *Cloud Architecture*

In a cloud stack each layer represents one service model. There are three service models in cloud computing. They are cloud software as service (SaaS), cloud platform as a service (PaaS) and cloud infrastructure as a service (IaaS).

- ✓ *SaaS* - It is located at the top of the stack. The cloud provider offers software applications as service. It also maintains a suite of management tools and facilities for managing the cloud system.
- ✓ *PaaS* - It occupies the middle layer. The cloud provides platform to deploy applications created by the users. The cloud provider creates a platform to application developers. Examples include Google App Engine.
- ✓ *IaaS* - It is offered in the bottommost layer. The resources are managed physically or virtually and the services are offered in forms of network, storage or computational capability [2]. The figure given below represents the cloud stack.

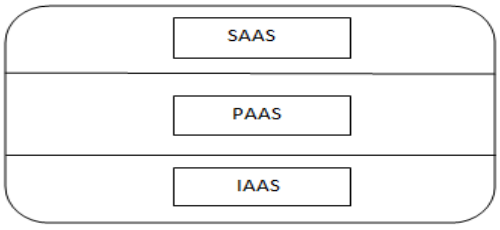

Fig. 1 Cloud Stack

B. *Deployment Models*

Cloud computing categorizes four main deployment models. Each model has specific characteristics that lend support to the needs of the users [3].

Private Cloud: This infrastructure is owned or leased by an enterprise. They are operated for the benefit of a single organization.

Public Cloud: This infrastructure is made available to the general public and is owned by cloud services vendor. Amazon web services, Google App Engine, Salesforce.com are some of the public cloud deployment vendors.

Community Cloud: The cloud infrastructure is shared one that is employed and supported by many companies. These clouds may be managed by organizations or a third party and may exist on or off premises.

Hybrid Cloud: This cloud deployment scheme is a composition of two or more clouds, namely private,

community or public. Each model remains unique but is bound together by standardized or proprietary technology that favors data and application portability.

C. Challenges

Cloud computing has become a very successful and popular business model due to its extremely good features. However, these features also cause serious security issues. Three of the most common challenges are outsourcing, multi-tenancy and massive data and intense computation.

II. LITERATURE SURVEY

Security issues in cloud computing have been discussed by various authors in different perspectives. Gruschka et al., [4] proposes a security ecosystem model based on three participants of the cloud system namely service user, service instance and the cloud provider. Six different attacks are being classified. They include user to service, service to user, user to cloud, cloud to user, service to cloud and cloud to service. Subashini et al., [5] have considered the security issues based on service delivery models. Grobauer et al., [6] have distinguished the general security issues from the cloud-specific security issues. Rachna et al., have provided various security concerns and their solutions. The security algorithms [7] have also been discussed. Chimere et al., [8] have studied various real world cases in which companies were infiltrated by attacks. Santosh et al., [9] have investigated various cloud computing system providers and their concerns on the various security issues. Sabarish et al., [10] have addressed various security challenges related to cloud service provider. Shilpashree et al., [11] have thrown light on the various security threats in cloud computing along with the existing methods to control them. This paper makes a detailed study on security attributes namely confidentiality, integrity and availability. The threats and defense mechanism for each attribute have been highlighted.

III. SECURITY ISSUES THREATS AND DEFENSE MECHANISMS

The various security issues such as confidentiality, integrity and availability have a number of threats. However, as threats increase so does the defense mechanisms. Fig. 2 provides a conceptual view of the entire paper.

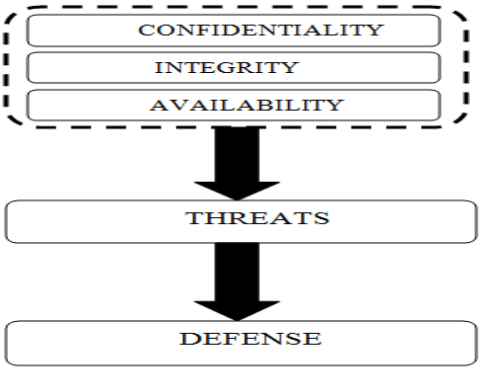

Fig.2 Conceptual chart

1) Confidentiality: It refers to the prevention of unauthorized disclosure of information [12]. Customers outsource their data and computation tasks on cloud servers, which are managed by untrustworthy service providers. Thus confidentiality remains a big question.The following are the threats associated with confidentiality:

- *Cross-VM (Virtual Machine) attack via side channels:* Ristenpart et al., [13] addresses the existence of cross-vm attacks in Amazon EC2 platform. Such an attack exploits the nature of multi-tenancy. Aviram et al., [14] considers timing side-channels as a great threat to security as they exist pervasively and are difficult to control as there is massive parallelism and shared infrastructure.

- *Malicious SysAdmin:* The threat discussed above shows how other people may plunger confidentiality. But it is shocking to know that the privileged sysadmin of the cloud provider may perform attacks. These attacks are being performed by accessing the memory of the customer's VM. An example would be Xenaccess, a user space library which allows a sysadmin to access the VM's memory at runtime [15].

The various defense mechanisms available for overcoming the various threats are as follows:

- *Placement prevention:* Cloud providers may allow the users to decide the location of their VM's, which will reduce the success rate of placement.

- *Co-residency Detection:* Elimination of co-residency may remain as a solution for avoiding cross–VM attack. However, this hinders the chances of reduction in cost and resource utilization. The best solution to this would be to share the infrastructure with friendly VM's. They may be of the same customer or other trustworthy customers. HomeAlone employs side channel as a detection tool and detects co-residency. The

idea behind this is to monitor the activities of the "friendly" Vm's in a selected portion of L2 (Level 2) cache, a multilevel storage strategy, and then analyze the cache usage.

- *No Hypervisor:* A hypervisor otherwise called a virtual machine monitor (VMM) is a piece of computer software or hardware that not only creates but also runs virtual machines. It aims to reduce the degree of shared infrastructure by removing the hypervisor while still maintaining the key features of virtualization. However, it requires changing the hardware that seems impractical for current cloud infrastructures.

- *Trusted Cloud Computing Platform (TCCP):* Santos et al., [16] presents a trusted cloud computing platform that offers a closed box execution environment for IaaS services. TCCP offers confidential execution of guest virtual machines and allows customers to make sure that the service is secure before launching their VM.

- *Extended views:* The fear of losing the data controls remains a nightmare for customers. Desscher et al., [17] provides a solution for upholding the data control by storing encrypted VMs on the cloud environments. This method ensures access control since only the authorized users are provided access. However this approach ensures security before VM is launched and not during runtime.

2) Cloud Integrity: Integrity deals with the honesty in storing data. Any deviations such as loss or alteration of data are to be detected. The threats to cloud integrity are as follows:

- *Data manipulation/loss:* The data may be stored on large servers which are questionable for both security and reliability [15]. Data may be modified accidently or maliciously. Further, administration errors due to backup and restore, data migration and changing of memberships in P2P systems may result in data loss [18]. Owners loss of control of data may favor adversaries to shoot up attack.

- *Lack of honesty in remote servers:* The integrity of data is questionable in an outsourced computation. The lack of transparency of computation details may urge servers to provide incorrect computing results. There may be certain computations which require huge computing resources for which the cloud would remain "lazy"[19].

The various defense strategies such as Provable Data Possession (PDP), Dynamic PDP, High Availability and Integrity Layer (HAIL) [23], Third party auditor(TPA),Re-computation and Sampling, Auditing are discussed below:

- *Provable Data Possession (PDP):* Integrity checking on data is the topic that is under research of quite a long time [20][21]. It remains a great challenge to check integrity for the tremendous amounts of data that is stored remotely on untrustworthy cloud servers. Downloading huge amount of data and performing integrity check is computationally expensive and requires greater bandwidth. The PDP model [18] deals with preprocessing data in the setup phase so as to put down some metadata on the client side for verification purposes. As soon as the client feels that is necessary to check the integrity they send a request to the server which will respond based on the data content. On combining both the reply and the local meta data, the client is able to check the integrity. However, PDP is applicable to only static files which remain as a limitation.

- *Dynamic PDP:* It supports dynamic operations like append, insert, modify and delete [22]. The DPDP protocol introduces three new operations such as PrepareUpdate ,PerformUpdate and VerifyUpdate.

- *HAIL:* It deals with distributed setting where a client must spread over a single file across multiple servers which would result in redundancy.

- *TPA:* A trusted third party auditor is assigned the task of verifying the integrity. Wang et al., [24] suggests a TPA for checking the integrity of outsourced data in cloud environments.

- *Re-computation and Sampling*: Re-computation deals with computing again and comparing the results. Even though re-computation assures maximum accuracy in mistake detection, the cost associated is very high. Sampling [25] is a variation of re-computation and offers probabilistic guarantees for mistake detection.

- *Auditing:* Auditing [26], [27] deals with logging. A logging component records into a log file every critical event that it encounters. The log file is reviewed by one or more auditors. A limitation of auditing is that if the computation is understood better by the

attacker, then, it paves the way for the attacker to manipulate the data.

3) Cloud Availability: Availability is very important as it provides on-demand service at different levels and remains the most needed function of cloud computing. The various threats imposed are as follows:

- *Flooding Attack:* Flooding Attack deals with a massive amount of non-sensical requests that are sent to a particular service, which may hinder the working of it. There are two types [28] of flooding attacks namely direct-DoS (Denial of Service) and indirect-DoS. In direct-Dos the attacking target is determined, whereas in the case of indirect-DoS, the attack is initiated without a specific target.

- *Fraudulent Resource Consumption (FRC) attack:* The attackers, who behave as authenticated cloud service clients, continuously send requests to website hosting in cloud servers to consume bandwidth. This attack succeeds as it causes financial strain on the victim.

The various defense mechanisms such as service migration, FRC-attack detection are discussed below:

- *Service migration:* It is a DoS avoidance strategy that has been developed to deal with flooding attack. A monitoring agent located outside the cloud is set to detect bandwidth starvation. As soon as bandwidth degradation is encountered, the monitoring agent will stop services temporarily and move the current application to another subnet which is not known to the attacker.

- *FRC-attack detection:* The main goal of FRC detection is to distinguish FRC traffic from normal traffic. Different metrics such as Zipf's law [29] , Spearman's footrule are used. Zipf's law is used to measure relative frequency. Spearman's footrule is used to find the proximity between the two ranked lists and then the overlap between the lists provides the similarity between the training and the test data. Combining these three metrics paves the way towards FRC detection.

IV. CONCLUSION

This paper has surveyed the various security issues such as confidentiality, integrity and availability. The various threats and the available defense mechanisms have been surveyed. This survey will lead to future research directions as to devise further more defense mechanisms as and when new threats arrive. As long as security is assured this research area will be a journey.

REFERENCES

[1] Mell, P.,&Grance, T., " The NIST Definition of Cloud Computing" , NIST Information Technology Laboratory, http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, ,pp 1-2, 2011.

[2] Ross A. Lumley, "Cyber Security and Privacy in Cloud Computing: Multidisciplinary Research Problems in Business", pp 1-10, 2010.

[3] Minqi Zhou et al., "Security and Privacy in Cloud Computing: A Survey", Proc. of Sixth International Conference on Semantics, Publications, First Printing, pp 149-150, 2008.

[4] Gruschka, M. Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services," Cloud Computing, IEEE 3rd International Conference on Cloud Computing, pp. 276-279, 2010.

[5] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Network and Computer Applications, vol. 34, pp. 1-11, Jan. 2011.

[6] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE, vol. 9, issue no. 2, pp. 50-57, 2011.

[7] Rachna Arora, Anshu Parashar ,"Secure User Data in Cloud Computing Using Encryption Algorithms,"Vol. 3, Issue 4, pp. 1922-1926, Jul.-Aug. 2013.

[8] Chimere Barron, Huiming Yu and Justin Zhan, "Cloud Computing Security Case Studies and Research", Proceedings of the World Congress on Engineering 2013 Vol II, WCE 2013, July 3 - 5, 2013.

[9] Santosh Kumar and R. H. Goudar, "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey" International Journal of Future Computer and Communication, Vol. 1, No. 4, pp. 356-360, Dec. 2012.

[10] S.Sabarish, G.Basha, A.Padmashree, Secured Cloud Environment With A New Approach, International Journal of Internet Computing ISSN No: 2231 – 6965, VOL- 1, Issue 4, pp. 68-71, 2012.

[11] Shilpashree Srinivasamurthy, David Q. Liu, "Survey on Cloud ComputingSecurity",http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_67.pdf.

[12] M.Malathi, "Cloud Computing Issues-A Survey", International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume 2, Number 2, pp. 113-118, June 2012.

[13] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," Proc. 16th ACM conference on Computer and communications security, pp. 199-212, 2009.

[14] A. Aviram, S. Hu, B. Ford, and R. Gummadi, "Determinating timing channels in compute clouds," In Proc.ACM workshop on Cloud computing security workshop, pp. 103-108, 2010.

[15] B. D. Payne, M. Carbone, and W. Lee, "Secure and Flexible Monitoring of Virtual Machines," In Proc. ACSAC'07, http://www.acsac.org/2007/papers/138.pdf, 2007.

[16] N. Santos, K.P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," Proc. Conference on Hot topics in cloud computing, 2009.

[17] M. Descher, P. Masser, T. Feilhauer, A. Tjoa, and D. Huemer, "Retaining Data Control to the Client in Infrastructure Clouds," pp. 9-16, 2009.

[18] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," In ACM CCS, pp. 598-609, 2007.

[19] C. Wang, K. Ren, J. Wang, "Secure and Practical Outsourcing of Linear Programming in Cloud Computing," 2011.

[20] D. L. G. Filho and P. S. L. M. Baretto, "Demon-strating data possession and uncheatable data transfer," http://eprint.iacr.org/2006/150.

[21] Y. Deswarte, J.-J. Quisquater, and A. Saidane, "Remote integrity checking," Proc. Conference on Integrity and Internal Control in Information Systems (IICIS'03), Nov. 2003.

[22] Erway, A. K¨ upc¸¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," Proc. 16th ACM conference on Computer and communications security, pp. 213-222, 2009.
[23] K.D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," Proc. 16th ACM conference on Computer and communications security, pp. 187-198, 2009.
[24] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," Mar. 2010.
[25] Z. Xiao and Y. Xiao, "Accountable MapReduce in Cloud Computing," Proc. The IEEE International Workshop on Security in Computers, Networking and Communications (SCNC 2011), 2011.
[26] A. Haeberlen, P. Kuznetsov, and P. Druschel, "Peer Review: Practical accountability for distributed systems," In Proc. ACM Symposium on Operating Systems Principles (SOSP), Volume 41 Issue 6, pp. 175-188, , Dec. 2007
[27] F. Monrose, P. Wycko, and A. D. Rubin, "Distributed execution with remote audit," pp. 103-113, 1999.
[28] M. Jensen, J. Schwenk, N. Gruschka, and L.L. Iacono, "On technical security issues in cloud computing," IEEE International Conference on Cloud Computing, CLOUD'09, pp. 109-116, 2009.
[29] J. Idziorek and M. Tannian, "Exploiting cloud utility models for profit and ruin," IEEE International Conference on Cloud Computing (CLOUD), pp. 33-40, 2011.