THREATS OF CLOUD COMPUTING AND ITS SECURITY-A SURVEY

Deepak Painuli[1], Divya Mishra[2]
[1,2]Quantum School of Technology, India

Abstract
Cloud computing means we can store and access the data over the internet rather than in the hard drive. So it is also known as internet computing. With the help of cloud computing the services like servers, applications are delivered to an organization's computer through internet. So its growth increases severe security concerns. Security has been a constant matter for internet and Open Systems, when we are dealing with security cloud suffers a lot. Lack of security is the only hurdle in wide adoption of cloud computing. Many security issues like securing user data, user authentication or authorization, application protection or portability and measuring the utilization of cloud by cloud provider affect cloud computing to great extent. The wide acceptance www has raised security risks along with the uncountable benefits, so is the case with cloud computing. The evolution boom of cloud computing has introduced lots of security challenges for the user and vendor. How the end users of cloud computing know that their information is not having any availability and security issues? Every one poses, Is their information secure? This study aims to address the major critical security threats in cloud computing, which will equip/empower both end users and service provider to know about the important security issues associated with cloud computing. Our work will enable researchers and security professionals to know about users and vendors concerns and critical analysis about the different security models and tools proposed.

Keywords: Cloud Computing, Internet, Security, Phishing, Measurement, Survey method.

I.INTRODUCTION

Cloud computing is not a new technology but rather a new delivery model for information and services using existing technologies. It uses the internet infrastructure to allow communication between client side and server side services/applications. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs both offer services. Mostly a layer of abstraction is provided by cloud between the low level architecture involved and the computing resources. Based on different-2 services, cloud poses different-2 architecture to be used. The data is stored on to centralized location called data canters having a large size of data storage. The data as well as processing is somewhere on servers. So, the clients have to trust the provider on the availability as well as data security. This paper surveys the concept of "cloud" computing, and its threats related to security.

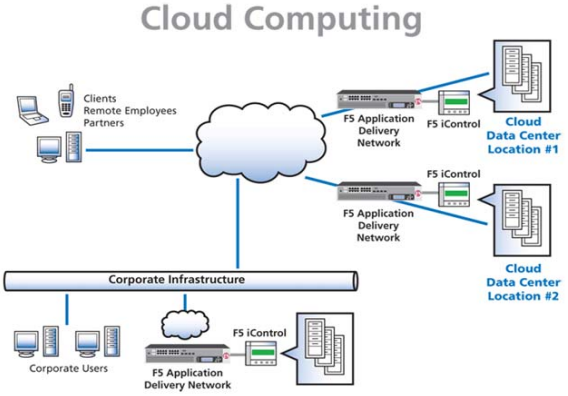

Figure 1

II.CLOUD SERVICE MODELS

A. IaaS (Infrastructure as a Service)

IaaS is the most flexible and lowest-level cloud computing service model where pre-configured infrastructure resources (hardware, servers, storage, networking etc.) are provided to users over a virtual interface like internet. Unlike PaaS and SaaS, rather than including applications, IaaS simply enables access to the infrastructure needed to power or support that software by complementing self-provisioned, on demand and metered cloud storage and network capability. IaaS can offer additional network bandwidth for a business website server, supplementary storage for company data backups, or even it can enable high power computing access, which was only accessible to those with supercomputers earlier. Popular IaaS offerings like Amazon EC2, IBM SoftLayer, and Google's Compute Engine (GCE) are silently powering a huge portion of the backbone of the internet, whether users realize it or not.

B. PaaS (Platform as a Service)

PaaS as a cloud service model, which operates at lower level than SaaS, where the cloud provides platform to end users from which they can develop, deploy and manage applications. PaaS services classically comprise a base operating system and a suite of development tool and applications. The requirement for building and maintaining the infrastructure used to develop applications by organizations is eliminated by PaaS . PaaS is also referred as 'middleware', addressing on how it conceptually resides somewhere in between SaaS and IaaS. There are various popular PaaS platform's like IBM BlueMix, Google's App Engine, Apache's Stratos, Microsoft Azure and SAP Cloud Platform etc. which are helping to rationalize and streamline software development.

C. SaaS (Software as a Service)

SaaS is a top level cloud computing service model which is sometimes called 'on-demand software' or "web based software". SaaS is a software distribution, licensing and delivery model where fully functional applications are delivered to end users over the internet on a subscription basis. End user can typically access SaaS offerings through web browser and can be billed on consumption basis or, more simply, with a flat monthly charge. SaaS applications run on servers thus freeing up end user from complex installation and maintenance of software by one's own. Microsoft Office365, Google Apps, Dropbox and Salesforce are most popular SaaS products for the workplace and are already in use by numerous businesses houses every day.

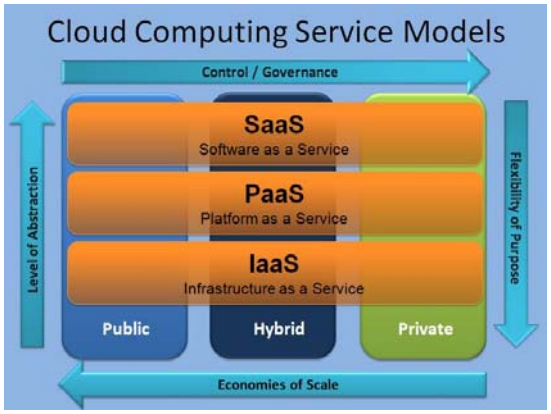

Figure 2

THREATS ON CLOUD COMPUTING
12 biggest threats are:

- **Data breaches**
- **Weak identity, credential and access management**

Insecure interfaces and APIs

- **System and application vulnerability**
- **Account hijacking**
- **Malicious insiders**
- **Advanced persistent threats**
- **Data loss**
- **Insufficient due diligence**
- **Abuse and nefarious use of cloud services**
- **Denial of service**
- **Shared technology issues**

III.LITERATURE REVIEW

Amin Soofi et. al. (2014) in his paper "Encryption Techniques for Cloud Data Confidentiality"[17] has reviewed the encryption techniques used for the data confidential. The suggestions of review are classified on the basis of type of approach, and the type of validation used to validate the approach.

K.S.Preeti et. al. (2014) in her work "Implementation of Private Cloud Computing Using Integration of JavaScript and Python" [18] has integration of two prevalent language's JavaScript and python, which is provided with a new level of compliance, which helps in

developing an understanding between Web Programming and Application Programming.

Deepika Saxena et. al. (2014) in her paper "A review on dynamic fair priority task scheduling algorithm in cloud computing" [19] provided a review on different task scheduling algorithms and made a review on a proposed task scheduling algorithm named "Dynamic right priority task scheduling algorithm" in cloud computing.

Mayanka Katyal et. al. (2014) in her paper" Application of Selective Algorithm for Effective Resource Provisioning in Cloud Computing Environment" [20] discusses a selective algorithm for allocation of cloud resources to the end-users on-demand basis. This algorithm is based on min-minimum and max-minimum algorithms. These are two conventional task scheduling algorithm. Certain heuristics used by selection algorithms to select between the two algorithms so that overall overhead of the tasks on the machines is reduced.

Shaveta Dargan (2014) in her paper "Security threats in cloud computing environment" focuses on the security threats of cloud and the countermeasures for the security problems.

Tejinder Sharma et. al. (2013) in his paper "Efficient and Enhanced Algorithm in Cloud Computing" [21] proposes an efficient and enhanced scheduling algorithm that can maintain the load balancing and provides better improved strategies through efficient job scheduling and modified resource allocation techniques. Load balancing ensures equal distribution of work among all the processors in the network as well as in the system at any instant.

Manish M.Potey et. al. (2013) in his paper "Cloud computing-Understanding risk, threats, vulnerability and control:A survey" define the types of cloud and its deployment models. The author also explains the threats on cloud and suggests some risk control models.

Kashif Muneer et. al. (2012) in his paper "Security threats /attacks present in cloud environment" identify the most vulnerable security threats/attacks in cloud computing, which will enable both end users and service provider to know the major security issues associated with cloud computing and relevant solution directives can be proposed to build up security in the Cloud environment. The author proposes secure cloud architecture for organizations to strengthen the security

Tim Mather et. al. (2010) in his book "Cloud security and policy" [1] has detailed about the cloud computing and what can be the threats if someone is using cloud to deliver applications. The author also suggests some security aspects.

Paul Cichonski et. al. (2008) in his book "Computer security incident handling guide"[2] provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines to be followed are independent of particular operating system, hardware platforms, applications or protocols.

IV.CONCLUSION

The paper starts with cloud computing then its service models .This paper also include the biggest threats on cloud. Security threats at host network, and application level, and the issues at each level with specific concern to cloud computing will have to be resolved in future. Another issue regarding security arises because of cloud APIs which are not yet standardized, so each cloud provider has its own specific APIs for managing its services which needs to be integrated across multiple vendors. This paper include survey of different authors about the security of cloud computing and its security.

REFERENCES

[1] Tim Mather, SubraKumarswamy, and ShahedLatif, Cloud Security and Privacy,s.l; O'Reilly, 2010

[2] T Grance, K Kent and B Kim. NIST SP80-61 computer security incident handling guide, 2008

[3] Gartner."Seven cloud computing security risks".http://www.infoworld.com July 2,2008

[4] Charles P Pfleeger, Security in Computing. Pearson Education.

[5] Vaquero, Luis Rodero-Merino Juan Caceres et. al "A break in clouds : Towards a cloud definition." ACM SIGOMM Computer Communication Review Archive, Volume 39, Issue 1 (January 2009).

[6] RichMaggini, Solari communication. "Cloud Computing is changing how wecommunicate",IEEE,2009.

[7] Jianfeng Yang, Zhibin Chen, "Cloud Computing Research and security issues", Professional Communication Conference, 2009.IECC 2009. IEEE International

[8] Adrian Seccombe, Alex Hutton, Alexander Meisel, et, al.Security Guidance for Critical Areas of focus in Cloud Computing V 2.1, Cloud Security Alliance , 2009

[9] Meiko Jensen JorgSchwenk, Nils Gruschka,Luigi Lo Icono, "On Technical Security Issues in Cloud Computing", 2009 IEEEconference on Cloud Computing.

[10] Kaufman, L.M. " Data Security in the World of Cloud Computing". Security& Privacy, IEEE, vol. 7 , pp. 61 -64 , July-Aug. 2009

[11] La'Quata Sumter, " Cloud Computing : Security Risk", ACM SE '10 Proceedings ofthe 48th Annual Southeast Regional Conference ACM New York, NY, USA ©2010

[12] ENISA, Cloud Computing: Benefits, risks and recommendation for information security,2010

[13] Dan Hubbard, Michael Sutton, AmerDeeba, Andy Dancer, et. al,Top Threats to cloud Computing v1.0, 2010

[14] Bernd Grobaur,TobiasWalloschek and Elmer Stocker, "Understanding cloud computing vulnerabilities",IEEE security and privacy, 10 Jun 2010, IEEE computer society digital library, IEEE Computer Society

[15] Minqui Zhou, Rong Zhang, wieXie, WeiningQian, Aoying Zhou, Security and Privacy in Cloud Computing : A Survey, 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG), IEEE Conferences.

[16] Kresimir Popovic ,Zeljko Hocenski, "Cloud Computing Security Issues and Challeges", MIPRO 2010 Proceedings of 33 International Convention ,IEEE,, May24-28, 2010,Opatija, Croatia.

[17] "NIST Cloud Computing Definition," NIST SP 800- 145

[18] Aized Amin Soofi, M.Irfan Khan and Fazal-e-Amin "Encryption Techniques for Cloud Data Confidentiality"- International Journal of Grid Distribution Computing Vol.7, No.4 (2014),

[19] K.S.Preeti,Vijit Singh, Manu Sheel Gupta "Implementation of Private Cloud Computing Using Integration of JavaScript and Python"- The Python Papers Monograph 2: 19 Proceedings of PyCon Asia-Pacific 2010

[20] Deepika Saxena, Dr. R.K. Chauhan "A review on dynamic fair priority task scheduling algorithm in cloud computing"- International Journal of Science, Environment ISSN 2278-3687 (O) and Technology, Vol. 3, No 3,2014

[21] Mayanka Katyal , Atul Mishra" Application of Selective Algorithm for Effective Resource Provisioning In Cloud Computing Environment"- International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol. 4, No. 1, February 2014

[22] Tejinder Sharma,Vijay Kumar Banga "Efficient and Enhanced Algorithm in Cloud Computing"-International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013.