International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

PERFORMANCE EVALUATION OF NETWORK & CLOUD BASED NETWORK AND EFFECTIVE IMPLEMENTATION TECHNIQUE TO CONTROL VULNERABILITIES

Sachin Gupta[1], Dr. S.N. Panda[2], Dr. Bharat Bhushan[3]

[1] Research Scholar
Punjab Technical University
Jallandhar, Punjab, India

[2]Department of Computer Science,
RIMT, Mandi Gobindgarh (Punjab), India

[3]Department of Computer Science & Applications,
G.N. Khalsa College,Yamuna Nagar (Haryana), India

ABSTRACT

Cloud computing is model that makes orientation to the two essential concepts: 'abstraction' and 'virtualization' to amplify the capacity and competence of IT by providing on demand network access to shared pool of computing resources without investing in new infrastructure. But as more and more information about enterprises are placed in cloud, concerns about how to secure the cloud environment to keep the data secure are also beginning to grow. So before shifting to cloud computing user must know about various threats present in this new system. In this paper, study about various attacks and vulnerabilities that facade threats to cloud is presented. This paper also concerned with the comparative study of attacks and different security issues arises due to the nature of cloud computing.

Keywords: Cloud Computing; Security; Vulnerabilities; Penetration.

International Journal of Computing and Business Research (IJCBR)

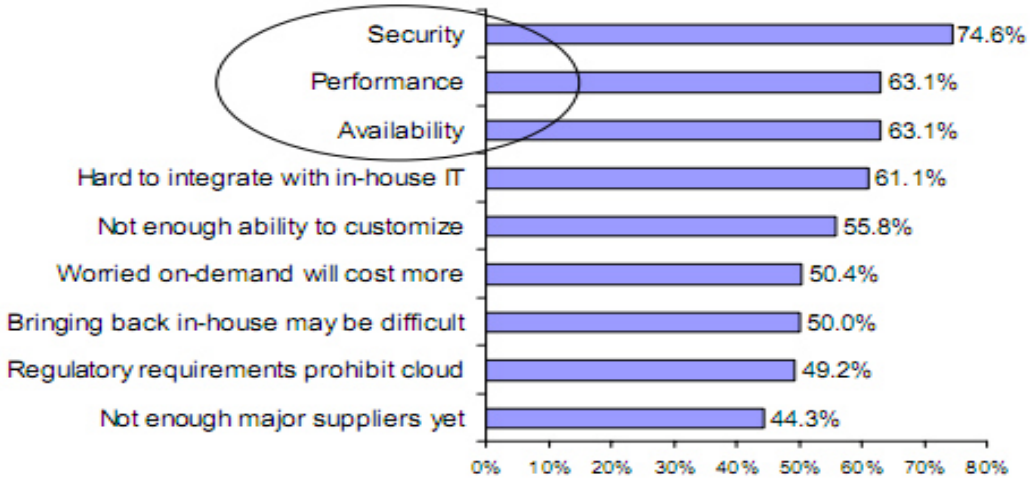
ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

INTRODUCTION

Cloud computing refers to the distributed computing on internet that uses the aspects of various technologies: Grid Computing (Distributed network that provides dependable, consistent and inexpensive access to various computational capabilities), Internet Computing (Provides distributed platform on internet), utility computing (pay-as you-grow), Autonomous computing (system manage themselves without any external interference), Edge computing (for load balancing). Today various small and medium size companies moved towards cloud environment because now they are capable to compete with the larger infrastructure companies by simply gaining fast access to best business application and drastically boost their infrastructure resources at negligible cost. While the cloud offers these advantages there are various issues and risks that reduce the growth of cloud computing.

According to the recent IDC enterprise survey figure 1 shows 74% IT companies has to be taken security as a top challenge prevents the adoption of cloud services.



Source: IDC Enterprise Panel August 2008

Figure 1 various issues/challenges to cloud model.

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

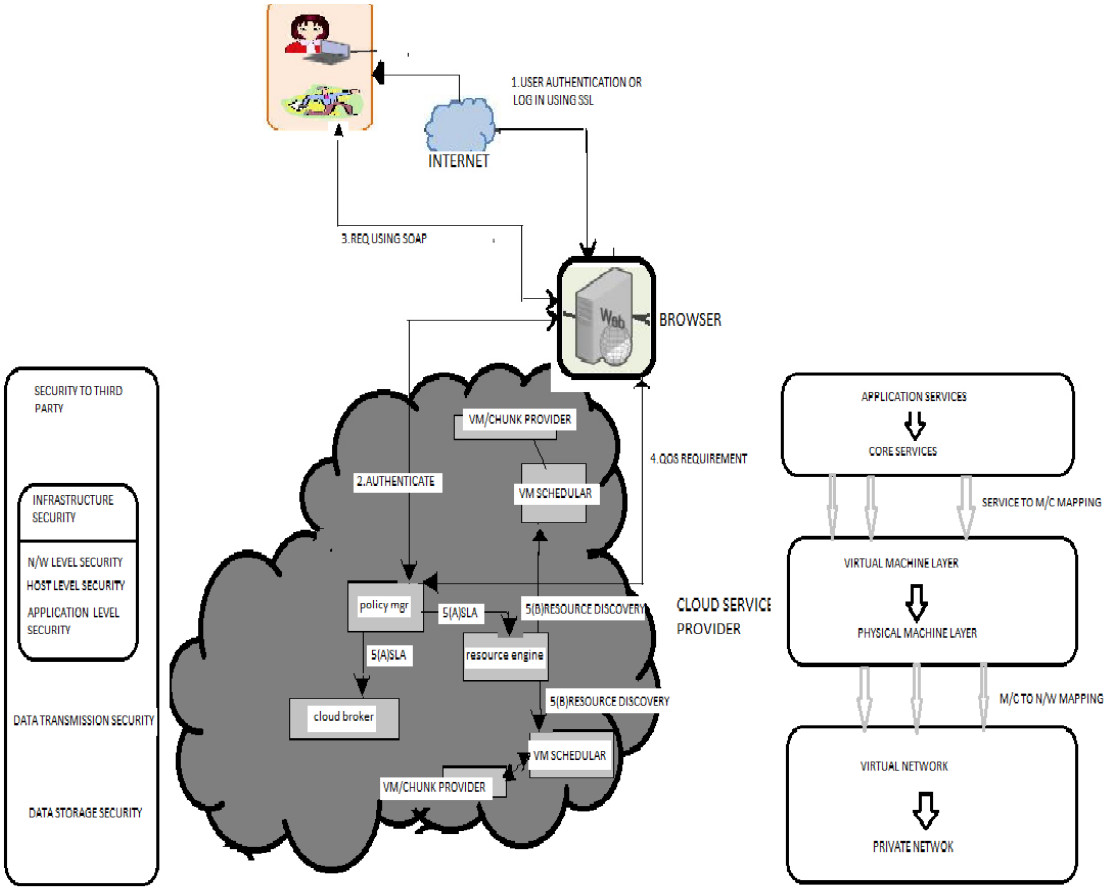


Figure 2 explain the basic level communication between user and service provider and dependency among various layer of cloud that poses great impact on security risks, necessary for understanding the complexity of security aspects in cloud environment.

In figure (2), during *communication process* consumers are front end and cloud service providers are back end. For resource pooling various steps are included:

- User authentication and login process: In this web browser collects all necessary information about consumer using various security technologies/protocols like SSL/SSH/TLS.
- Web browser provides all information to policy manager which authenticate the consumer using public key infrastructure, certification authority and others.
- After that consumer request to browser for required services using Simple Object Access Protocol [XML or REST format + transfer protocols].

- Now web browser delegates the QOS requirements to policy manager, which evaluate the requirements according to service level agreement (SLA). For SLA policy manager also use cloud broker and resources engine.
- For resource discovery cloud broker collects the information about other cloud and their services and resource engine delegates the service requirement to VM schedulers which collaborates the required service from various VM / chunks provider.

Dependency among cloud layers: The application layer and core layer depends upon VMs layer and physical machine layer which further depend upon virtual network layer and physical network layer so damage at any layer also have great impact on other layers.

Complexity of security aspects: When we think about security of organization's core IT infrastructure there is need to provide security at network level, host level, application level and when we talk about data security two aspects are included 'data transmission security and data storage security'.

Security Principles: The fundamental basis for developing secure cloud environment is based on various security principles:

Confidentiality: The prevention of unauthorized disclosure of information that may be intentionally or unintentionally refers to the confidentiality.

Integrity: The concept of cloud information integrity is based on two principles

- Prevention of modification of data from unauthorized users and preventing the unauthorized modification of data by authorised user.

Availability: This Principle ensures the availability of cloud data and computing resources when needed.

Authentication: It refers to the process of testing the user's identity and ensures that users are who they claim to be.

Authorization: It refers to the privileges that are granted to individual or process for enabling them to access any authorized data and computing resources.

Accountability: This is related to the concept of non-repudiation where the person cannot deny from the performance of an action. It determines the action and behaviour of single individual within cloud system.

Analysis of attacks and vulnerabilities in cloud computing environment/system: In traditional on premises deployment model the data of enterprise must resides within its boundary and follow their own access control and security policies. Whereas in cloud computing data reside at distributed data centres of cloud with the lack of control and without the knowledge of how their data resides. Due to the nature of cloud system there are many questions that arise as to weather a cloud is secure enough or not.

Before understanding the security management in cloud, it must be necessary to analyse the various possible vulnerabilities and attacks in cloud environment.

Network level attacks: During resource pooling process all data or services flow over the network needs to be secured from following attacks to prevent the leakage of sensitive information or other vulnerabilities:

- *Denial of service/distributed denial of service attack*: This attack can overwhelm target's resources so that authorised user is abstained from getting the normal services of cloud. DDOS is also based on DOS attack which can be distributed for more significant effects. This attack is a cause of failure of availability.
- *Eavesdropping* is an interception of network traffic to gain unauthorized access. It can results in failure of confidentiality.
- *Man in the Middle attack* is also a category of eavesdropping. The attack set up the connection with both victims that makes conversation and making them believe that they talk directly but infect the conversation between them is controlled by attack.
- *Replay attack:* The attacker intercepts and save the old messages and then send them later as one of participants to gain access to unauthorized resources.
- *Back Door:* The attacker gain access to network through bypassing the control mechanisms using "back door" such as modem and asynchronous external connection
- *Impersonation* is vulnerability in which malicious node modify the data flow route and lure the node to wrong positions.
- In *Sybil attack* a malicious user pretends to be distinct users after acquiring multiple identities and tries to create relationship with honest user if malicious user is successful to compromise one of the honest user then attack gain unauthorized privileges that helps in attacking process.
- *Byzantine failure* is a malicious activity which compromised a server or a set of server to degrade the performance of cloud.

Attacks and vulnerabilities based on security techniques: If any security technique has weakness in implementation it can cause various vulnerabilities:

- *Inside channel attack* gain the information from physical implementation of cryptosystem to break the security. The information is like technical knowledge on which encryption implement, time information, power consumption and others.
- *SSL/SSH/TLS* use the cryptography techniques to secure the data but any crucial flow in implementation of cryptography algorithm can make stronger cryptography technique to weak technique which is a main target of hackers.

Language and malicious program injection based attack: One of the most frequently discovered vulnerabilities in cloud are a direct result of language and programmes that are as follow.

- *Buffer overflow* is a favourite exploit for hacker which takes the advantage of programme that is waiting for user's input. But in place of user the hacker would enter the input or command which results to move the control to attack code.
- *Trojan horses/Malware* are the unauthorized program that are contained or injected by malicious user within legitimate program to perform unknown and unwanted function.
- *XML Signature wrapping Attack* is well known attack on protocols like SOAP that use XML format to transfer the request for services. In this, attack moves the original body of SOAP message to newly inserted wrapping element writing within SOAP header and create a new body which contains the operation that an attack wants to perform.

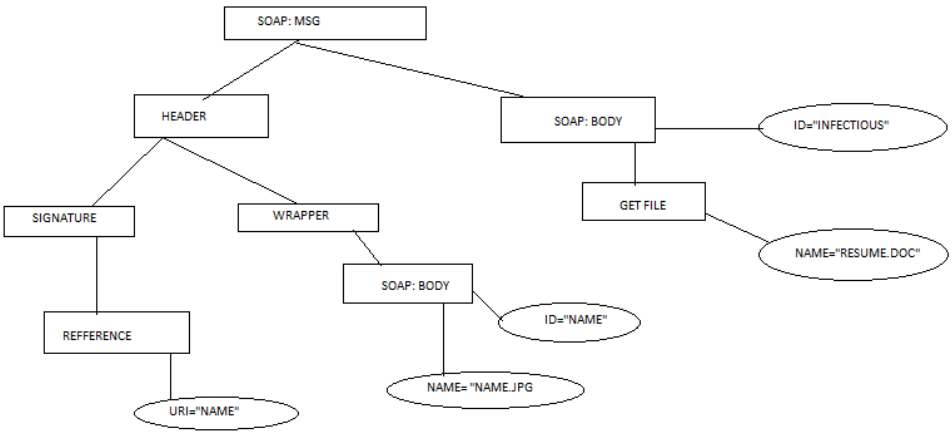


FIG: 3 Example of SOAP message after attack

Web application attacks: Web browser is one of the way of providing the web application virtually to users but at the same time they also creates vulnerabilities that has detrimental impact on costumers as well as on cloud system

- *Weak authentication or weak username, password* is one of the main target of malicious users to gain unauthorized access to the services.
- *SQL injection flaws*, in which malicious SQL code is erroneously executed in database backend.
- *Cross-site-scripting (XSS),* in which the malicious java script code is executed erroneously by browser.

Virtual Machine based vulnerabilities: Following are the various VM based vulnerabilities create challenges and issues for service providers.

- Any malicious programme in VM also transferred between other VMs using shared clipboard technology which is an issue for security.
- Many VMs co-exist on same server share CPU, memory, I/O have virtual boundaries. So securing the virtual boundaries is also a challenge for service provider.
- Hypervisor is main controller that maps the physical resources to virtual resources. So if any hypervisor is compromised, it is possible to trace the VMs operations unencrypted.

Comparison of attacks and vulnerabilities according to their impact on response time, growth level and penetration

- *Impact on response time*: According to NIST SP 800-61 report figure 4(a), 4(b), 4(c) shows the negative effect of various threats on to the response time of cloud system environment

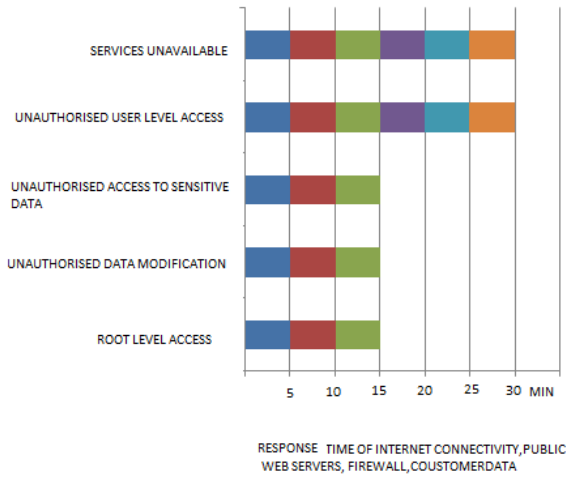


FIG: 4(a) Attack's impact on response time of internet Connection, public web server, firewall, customer data

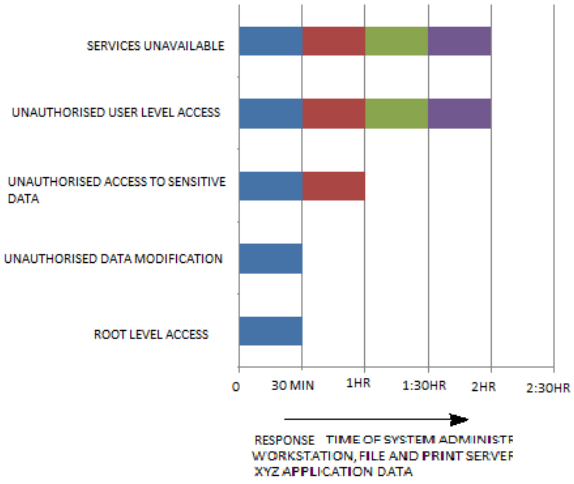


FIG: 4(b) attacks impact on response time of system administrator, file and Print server, XYZ application data

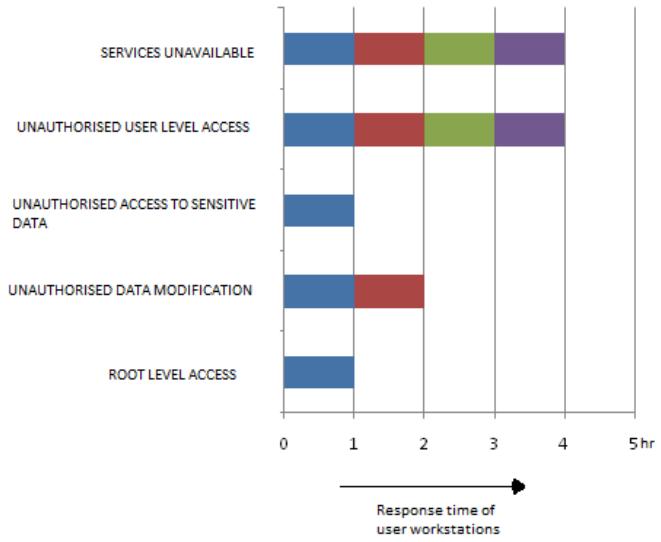


FIG: 4(c) attack's impact on response time of user workstations

- *Growth level of vulnerabilities*: According to IBM X-Force trend and risk report figure 5 shows about more than 8000 new vulnerabilities, a 27% rise from 2009. This report presents the expanding threat landscape in which various attacks are launched against computing environment.

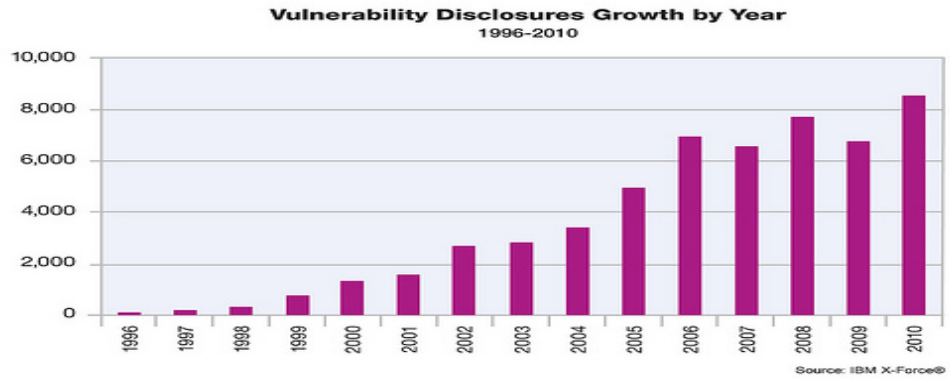


Figure5 Rise in vulnerabilities over time

This report shows that about 49% vulnerabilities are targeted at web applications in 2010 in which cross site scripting and SQL injection flaws are top majority issues.

According to ARBOR NETWORKS report figure 6 shows the dramatically increase in DDOS attack about 51% rise from 2009 which broke 100 Gbps barrier for first time.

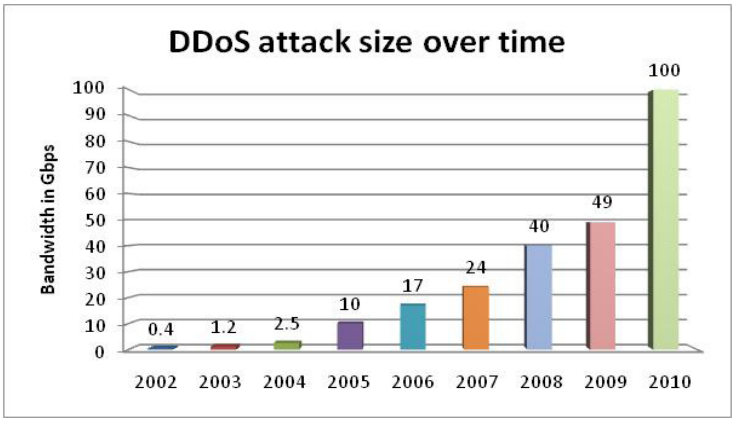


Figure 6 Increase in DDOS attack size over time

SOURCE: ARBOR NETWORKS 'DDOS ATTACK THROUGH 2010'BY Richard Wray Technical Director EMEA.

Figure 7 shows the growth of application layer attacks in which HTTP and DNS are top target of vulnerabilities about 84% and 76% respectively.

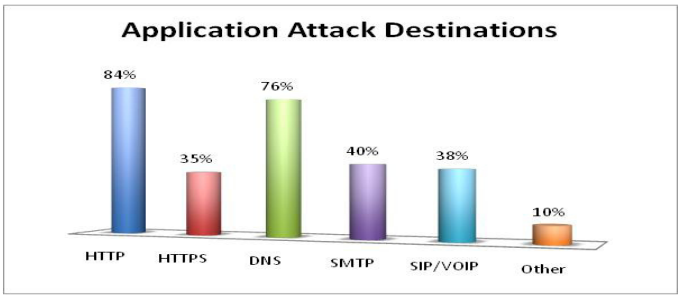


Figure 7 Target of application attacks

SOURCE: ARBOR NETWORKS 'DDOS ATTACK THROUGH 2010'BY Richard Wray Technical Director EMEA.

- *Penetration of various attacks*: Figure 1 shows the dependency among various layers of cloud i.e.

Application service layer ⇨ **Core service layer** ⇨ **Virtual machine layer** ⇨ **Physical machine layer** ⇨ **Virtual network layer** ⇨ **Physical network layer**

Where A ⇨ B Shows that any attack on layer A also effect on layer B. Figure 8 shows the penetration level of various attack

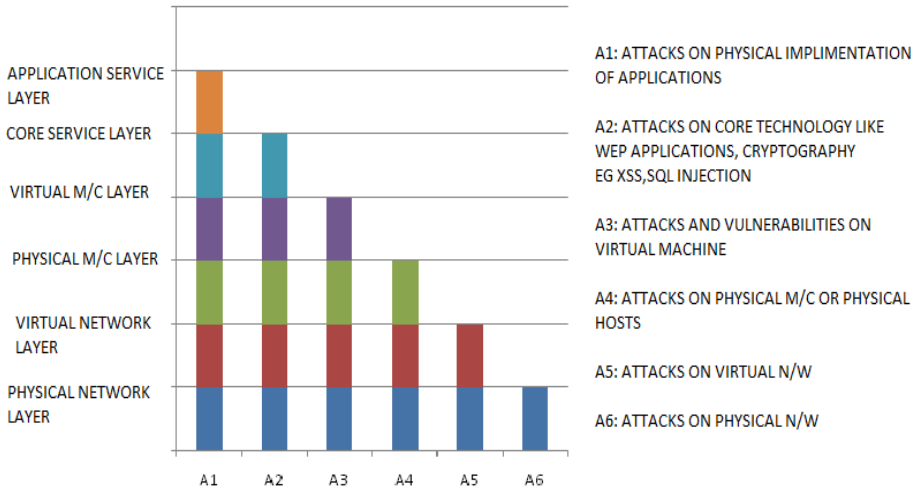


Figure (8) Penetration level of various attacks

Issues and challenges in cloud computing security:

- As virtualized network offers protection of data from local access but at the same time VM has more complex layers of resource allocation. So various detection and prevention schemes can also be applied with more complexity.
- Cryptography techniques are used to overcome the vulnerabilities but it is also common to find crucial flows in encryption algorithm implementation which turns the strong encryption into weak one and results more vulnerabilities.
- Due to the limited knowledge of cloud infrastructure, it is difficult to configure the firewall correctly, managed and updated causes it to be at risk.

CLOUD COMPUTING AND VULNERABILITY ISSUES

Cloud Computing means provides computing over the internet and this word is basically inspired by the cloud. In this, data is stored at remote location and available on demand. It allows clients to use applications without installation the file at any computer with internet facility. By data outsourcing user can get the information from anywhere more efficiently and has no burden

on data storage and avoid the extra expenses on software, hardware, information resources and data maintenances and used more efficiently.

Vulnerability means anything which has a capability to harm anybody or absence of security system or exploit the system security policy. Vulnerability means any programming error or misconfiguration with the help of which an intruder gain unauthorized access to a system. A Security risk may be classified as vulnerability. Vulnerability is basically run on computer and that helps in unauthorized access of reading, creation, modification or deletion of files anywhere on the network. World is mounting with the emerging technologies. The computer networks and packet transmission systems are also growing in parallel, hence to manage and provide security to packet, a secured system is required. Networks seize or simply intercept is one of the challenges in the fast growing world of Cyber Crime. The network establishments including cloud frameworks and distributed computing systems are facing various types of threats on routine basis. To efficiently transmit information across a network, there is need of an improved and reliable architecture.

Dennis Longley and Michael Shain, Stockton Press, ISBN 0-935859-17-9, defines vulnerability as:

In computer security, a weakness in automated systems security procedures, administrative controls, Internet controls, etc., that could be exploited by a threat to gain unauthorized access to information or to disrupt critical processing.

In computer security, a weakness in the physical layout, organization, procedures, personnel, management, administration, hardware or software that may be exploited to cause harm to the ADP system or activity.

In computer security, any weakness or flaw existing in a system. The attack or harmful event, or the opportunity available to a threat agent to mount that attack.

In cloud computing environment, the most fundamental aspect is how services are delivered? Which mainly dependent on cloud deployment models (provides hosting environment). There are three primary types of cloud computing which are available to service consumer:

PUBLIC CLOUDS

A public cloud is hosted, operated, and managed by third party vendor from one or more data centres. The service is offered to multiple customers over common infrastructure; In a public cloud, security management and day- to- day operations are relegated to third party vendor, who is responsible for the public cloud service offering. Hence, the customer of the public cloud service offering has a low degree of control and oversight of the physical and logical security aspects of a private cloud. There are a few challenges listed below that are preventing wide scale adoption of public clouds.

- **Security:** The biggest roadblock is the potential security issues due to multitenant nature of public clouds. There are security and privacy concerns with sharing same physical hardware with unknown parties that need to addressed.

- **Reliability and Performance:** Performance and reliability of the applications are important criteria for defining the success of an enterprise's business because organizations lose control over IT environment in some critical applications.

- **Vendor Lock-in:** Cloud computing services offered by different vendors are not governed by any standards as of today. Depending on the vendor, the applications have to undergo changes to adapt to the service.

- **Leveraging Existing Investment:** Most large organizations that have already invested in their own data centers would see a need to leverage those investments as an important criterion in adopting cloud computing.

- **Corporate Governance and Auditing:** Performing governance and auditing activities with the corporate data abstracted in the public cloud poses challenges that are yet to be addressed.

- **Maturity of the Solutions:** Some of the PaaS offering like AppEngine offer limited capabilities like only a subset of JDO API.

PRIVATE CLOUDS

To overcome all above challenges enterprises adopt the private clouds which is managed or owned by an organization to provide the high level control over cloud services and infrastructure. In other words private cloud is build specifically to provide the services within an organization for maintaining the security and privacy. As such, a variety of private cloud patterns have emerged:

- **Dedicated:** Private cloud hosted within a customer- owned data center or at a collection facility, and operated by internal IT departments.
- **Community:** Private clouds located at the premises of third party; owned, managed, and operated by a vendor who is bound by customer SLAs and contractual clauses with security and compliance requirements.
- **Managed:** Private cloud infrastructure owned by customer and managed by a vendor.

HYBRID CLOUDS

This model comprised both the private and public cloud models where organization might run non- core application in a public cloud, while maintaining core applications and sensitive data in-house in a private cloud.

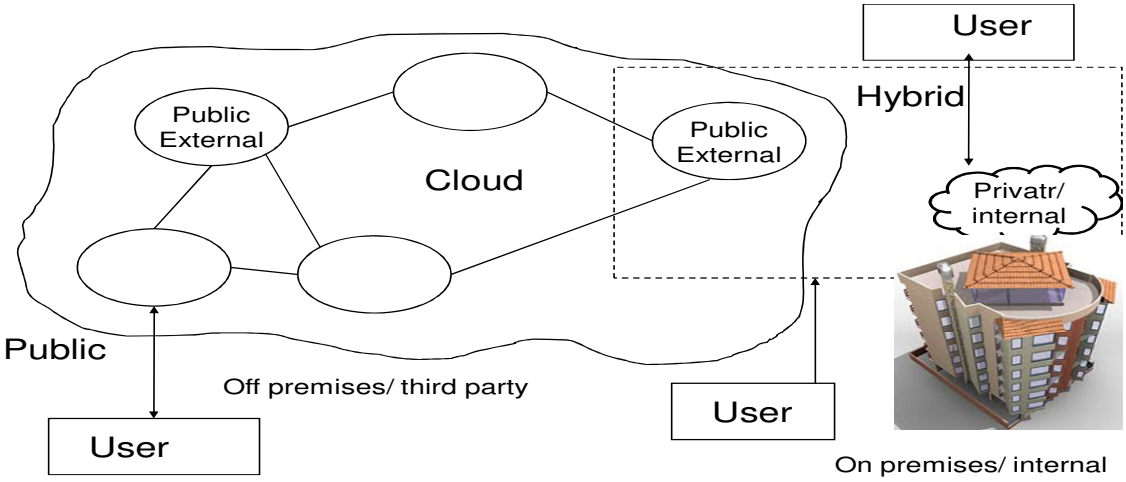


FIGURE: PUBLIC, PRIVATE, AND HYBRID MODELS OF CLOUD

Source: Hai jin, Shadi Ibrahim, Tim Bell, Wei Gao, Dachuan Huang and Songwu, "Cloud types and services", Hand Book of cloud computing, Springer Ist edition, 2010.

Tim Marther, SubraKumaraswamy, ShahedLatif, "Cloud Security and Privacy An Enterprise Perspective on Risks and Compliance", O'REILLY, January 2011, ISBN 13:978-81-8404-815-5.

REVIEW OF LITERATURE

With the advent of Globalization, the Business as well as Defense Applications needs highly secured and consistent architecture so that packets can be transmitted in the network without any risk. Trust is the groundwork of the relationship which is established by a business organization with their customers, vendors, and employees. The speed at which computer network communications is taking place is increasing. It is therefore important to make the routines that send and receive network communication packets as efficient as possible such that information can be transmitted as fast as possible.

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
Volume 4 Issue 3 September 2013

CLOUD COMPUTING

Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. The market research and analysis firm IDC suggests that the market for Cloud Computing services was $16billion in 2008 and will rise to $42billion/year by 2013. It has been estimated that the cost advantages of Cloud Computing to be three to five times for business applications and more than five times for consumer applications. According to a Gartner press release from June 2008, Cloud Computing will be “no less influential than e-business”.

Cloud computing is still an evolving paradigm. But to understand what cloud computing is and is not, it is important to understand that how this model of computing has evolved from previous computing paradigms, weather its’ really different or just progressive step in computing to solve the problems that are left unsolved from last three decades. According to historical perspective there are different phases in computing paradigms shift. In Figure, the seven phases of computing paradigms, in phase 1 various users shared the powerful mainframe by using the terminal as an interface. In phase 2 stand- alone PCs become enough to fulfil the requirements of users without sharing the mainframe with any once else. In phase 3, computer network is used to share the resources by allowing the multiple computers, PCs, laptops and servers to connect to each other. Phase 4 allow the various local networks to connect with each other to form the global network called internet for remote application and resource sharing. As in computer networks the (CN), multiple computers are connected in two ways: wired and wireless network, in phase 5 wireless network give birth to mobile wireless computing which provide mobile users with ubiquitous communication capability and resource access regardless of its location. Phase 6 brought us the grid computing which provides the shared computing power and storage resources through distributed computing system. In phase seven, cloud computing exploits all available resources on the Internet in a scalable and simple way.

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

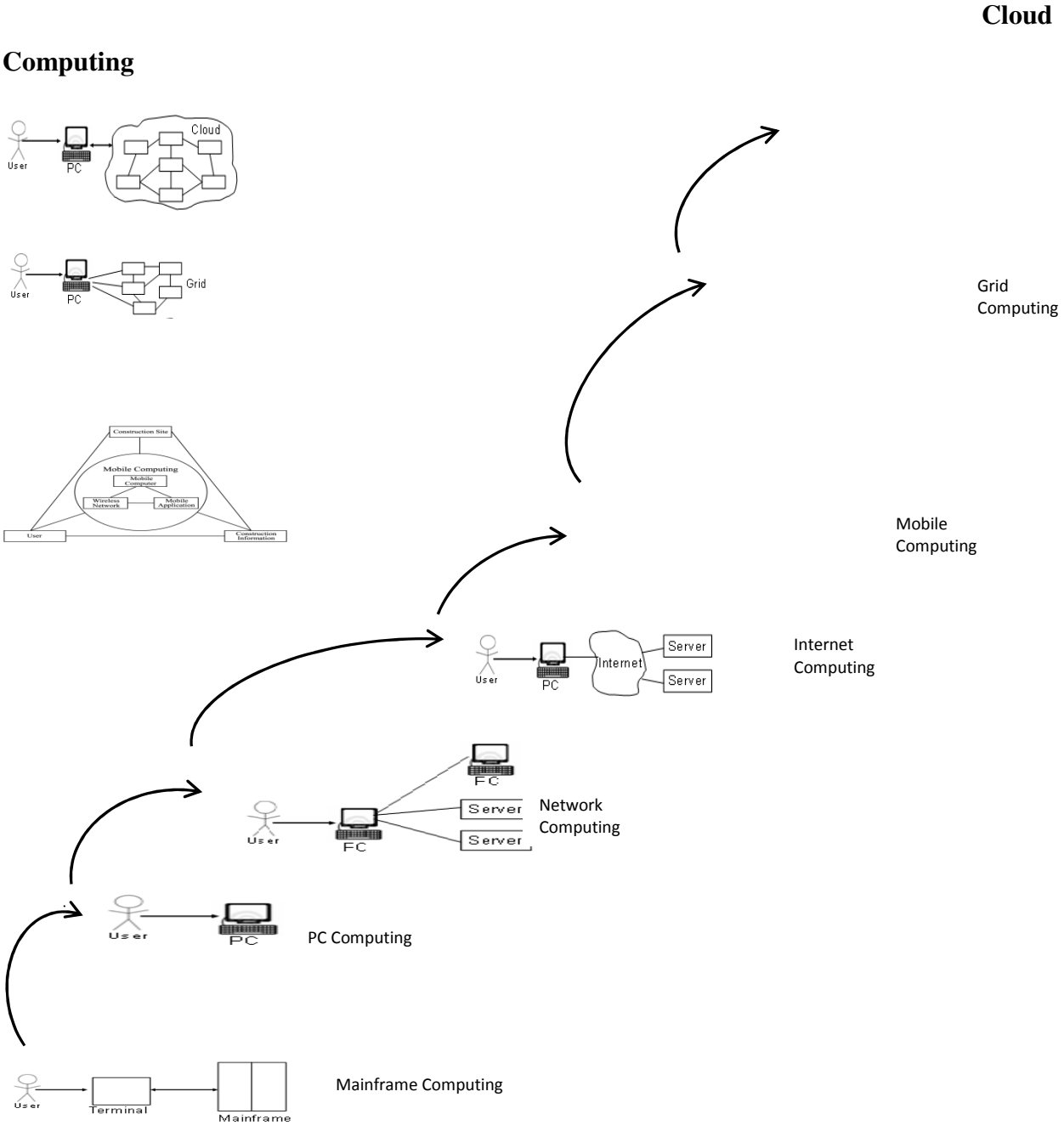


FIGURE 1: SEVEN COMPUTING PARADIGM SHIFTS

Source -Jeffrey Voas, Jia Zhang, "Cloud Computing: New Wine Or Just New Bottle?", Sponsored by IEEE Computer Society March-April 2009, Volume 11, Issue 2,

pp 15-17. Hai jin, Shadi Ibrahim, Tim Bell, Wei Gao, Dachuan Huang and Songwu, "Cloud types and services", Hand Book of cloud computing, Springer Ist edition, 2010.

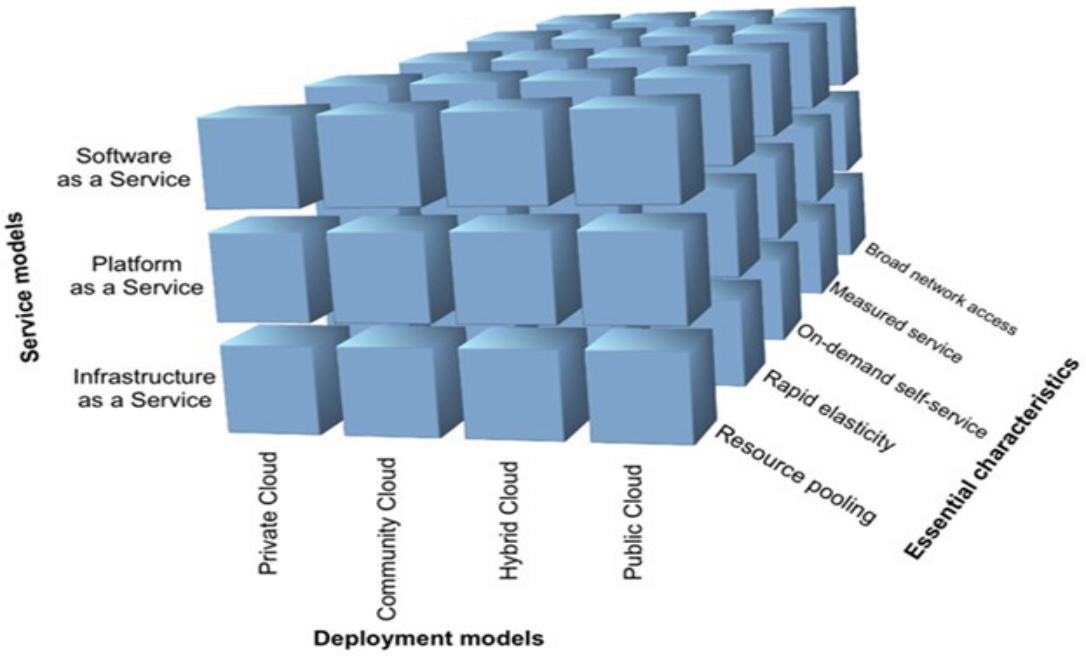


Figure 2: Visual model of NIST Working Definition of Cloud Computing

Source: Cloud Security Alliance. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing.

One of the main tenets of Cloud Computing is the `as-a-Service' paradigm in which `some' service is offered by a Service Provider (also known as a Cloud Service Provider) to a User (consumer) for use. This service can also be categorised according to the application domain of its deployment. Examples of application domains that offer services are: Financial e.g. Mint.com, Managerial e.g. Ever Note and Analytical e.g. Google Analytics. The agreed terms of use, indicating the actions that must be taken by both the provider and consumer, are described in a contract that is agreed upon before service provision. Failure to honour this agreement can lead

to denial of service for the consumer or legal liability for the service provider. This contract is often described as a Terms of Service or Service Level Agreement. Moreover, as part of this agreement the service provider will provide a Privacy Policy which outlines how the users data will be stored, managed, used and protected.

CLOUD SERVICE DELIVERY MODELS

The services offered are often categorised using the SPI Service Model. This model represents the different layers/levels of service that can be offered to users by service providers over the different application domains and types of cloud available. Clouds can be used to provide as-a-Service: software to use, a platform to develop on, or an infrastructure to utilize.

CONCLUSION

The cloud environment has scalable, expandable, virtualization and abstraction as basic aspects that makes cloud security become more complex. Various vulnerabilities and attacks discussed in this paper are main threats for cloud that cause many enterprises which have plan to migrate to cloud prefer using cloud for less sensitive data and store important data within enterprise boundary. So as a result, moving towards cloud computing require more safe and secure environment and our further study will also focus on various security schemes or algorithm that helps in providing secure cloud environment.

REFERENCES

[1] Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent Issued on August 18, 1998

[2] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, A Security, Privacy and Trust Architecture for Wireless Sensor Networks, 50th International Symposium ELMAR-2008, 10-12 September 2008, Zadar, Croatia

[3] Donna Andert, Robin Wakefield, and Joel Weise, Professional Services Security Practice, Sun BluePrints™ OnLine - December 2002, Trust Modeling for Security Architecture Development

[4] Security, Encryption, Acceleration, http://www.networkintercept.com

[5] Youlu Zheng, Shakil Akhtar, Networks for Computer Scientists and Engineers, Oxford University Press, 2009

[6] Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004

[7] Technical Standard Risk Taxonomy ISBN 1-931624-77-1 Document Number: C081 Published by The Open Group, January 2009.

[8] "An Introduction to Factor Analysis of Information Risk (FAIR)", Risk Management Insight LLC, November 2006;

[9] Matt Bishop and Dave Bailey. A Critical Analysis of Vulnerability Taxonomies. Technical Report CSE-96-11, Department of Computer Science at the University of California at Davis, September 1996

[10] Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization)

[11] Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257 ISBN 978-0-12-374354-1

[12] ISACA THE RISK IT FRAMEWORK (registration required)

[13] Kakareka, Almantas (2009) "23" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 393 ISBN 978-0-12-374354-1

[14] Technical Report CSD-TR-97-026 Ivan Krsul The COAST Laboratory Department of Computer Sciences, Purdue University, April 15, 1997

[15] The Web Application Security Consortium Project, Web Application Security Statistics 2009

[16] Ross Anderson. Why Cryptosystems Fail. Technical report, University Computer Laboratory, Cam- bridge, January 1994.

[17] Neil Schlager. When Technology Fails: Signi cant Technological Disasters, Accidents, and Failures of the Twentieth Century. Gale Research Inc., 1994.

[18] Hacking: The Art of Exploitation Second Edition

[19] Kiountouzis, E. A.; Kokolakis, S. A. Information systems security: facing the information society of the 21st century London: Chapman & Hall, Ltd ISBN 0-412-78120-4

[20] Bavisi, Sanjay (2009) "22" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 375 ISBN 978-0-12-374354-1