Vulnerability Assessment Methods in Cloud Computing

Manoj L. Bangare[#1]

[#]*Research Scholar,Department of Computer Engineering ,COEP ,Pune*

Abstract— **Cloud computing is an emerging technology which is a big step in virtual computing. In cloud computing services are provides to clients via internet. One of the service provided by cloud computing is IaaSi.e. Infrastructure as a Service. In this service, customers can hire fundamental computing resources like processing, networking, storage, etc. IaaS is focused in this paper. Though cloud computing has various benefits like improved system efficiency, reduced cost, reduced hardware and so on. Despite of these benefits their exists some challenges in cloud computing. Most significant of the challenges is security. The cloud provides virtual computing environment to multiple tenants, here competitive businesses may co-exist. The sensitive information is hosted here may be attacked. Incidents of invasions against campus-networks have increased significantly in recent years.The aim of such invasions is to obtain unauthorized privileges or to promote authority levels by exploiting vulnerabilities in servers, operating system or software applications. Our aim is to provide the most effective tools and solutions to measure and assess vulnerability of a generic IaaS cloud system. We have surveyed various techniques and tools for the assessment of vulnerability and recommend their effectiveness in IaaS.**

Keywords— Cloud Computing, Vulnerabilities, assessment methods, security

I. INTRODUCTION

Cloud computing has redefined the way, computers are used. With increase in number of users, applications and businesses, importance of proper vulnerability management has increased. Vulnerabilities in cloud computing are increasing exponentially every year. With increase in vulnerabilities the need to efficiently classify, manage and analyze them has also increased. Due to complexity of modern software systems it is difficult to build software without vulnerabilities. So, the obvious solution to this problem is to find vulnerabilities and to patch them.

Vulnerability can be defined as weakness in Security system. The weakness of system can make system susceptible to attack. Attackers can steal, corrupt or damage data by hacking the system. As solution to this problem many tools and techniques are implemented but, most of them have following drawbacks:

1. Several security officers are forced to work non-stop.
2. It is practically not possible to manage in-house tools.
3. Not all tools are scalable.
4. Tools are not automated.

Importance of vulnerability cannot be underestimated. According to a survey of challenges in cloud computing, most common challenge is security.It was observed that security in public cloud is the major concern for more than 70% participants, and that for private cloud is to around 45% people [1].In the graph given below, we can see that top most position is achieved by security.

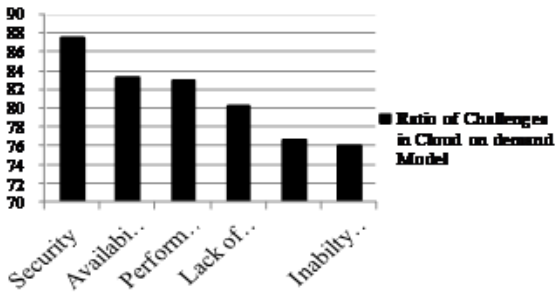


Figure 1 : Ratio of Challenges in Cloud Computing

Other than above challenges, there are few more challenges in cloud computing, which are:

1. Low technology maturity.
2. Less skill set than required.
3. Organizational challenges.
4. Complexities in integrating infrastructure.

As the technological development progresses, these challenges will cease to exist.

This paper is organised as follows, in following section we discuss IaaS cloud assessment procedure. After that we discuss vulnerabilities and how to deal with them. Then we end with conclusion.

II. IAAS CLOUD ASSESMENT PROCEDURE

A Before discussing more important things, we will define some common terminologies used in cloud computing. National Institute of Standards and Technology (NIST) precisely subdivided cloud computing into three distinct models, which offer differing capabilities to the consumer[2].

- Software as a service(SaaS):

In SaaS model, the cloud service provider makes software and cloud infrastructure available to client. The underlying physical settings of cloud like operating system, network and storage are controlled by service provider. Due to this client interfaces like web browsers can access these applications.

- Platform as a Service(PaaS):

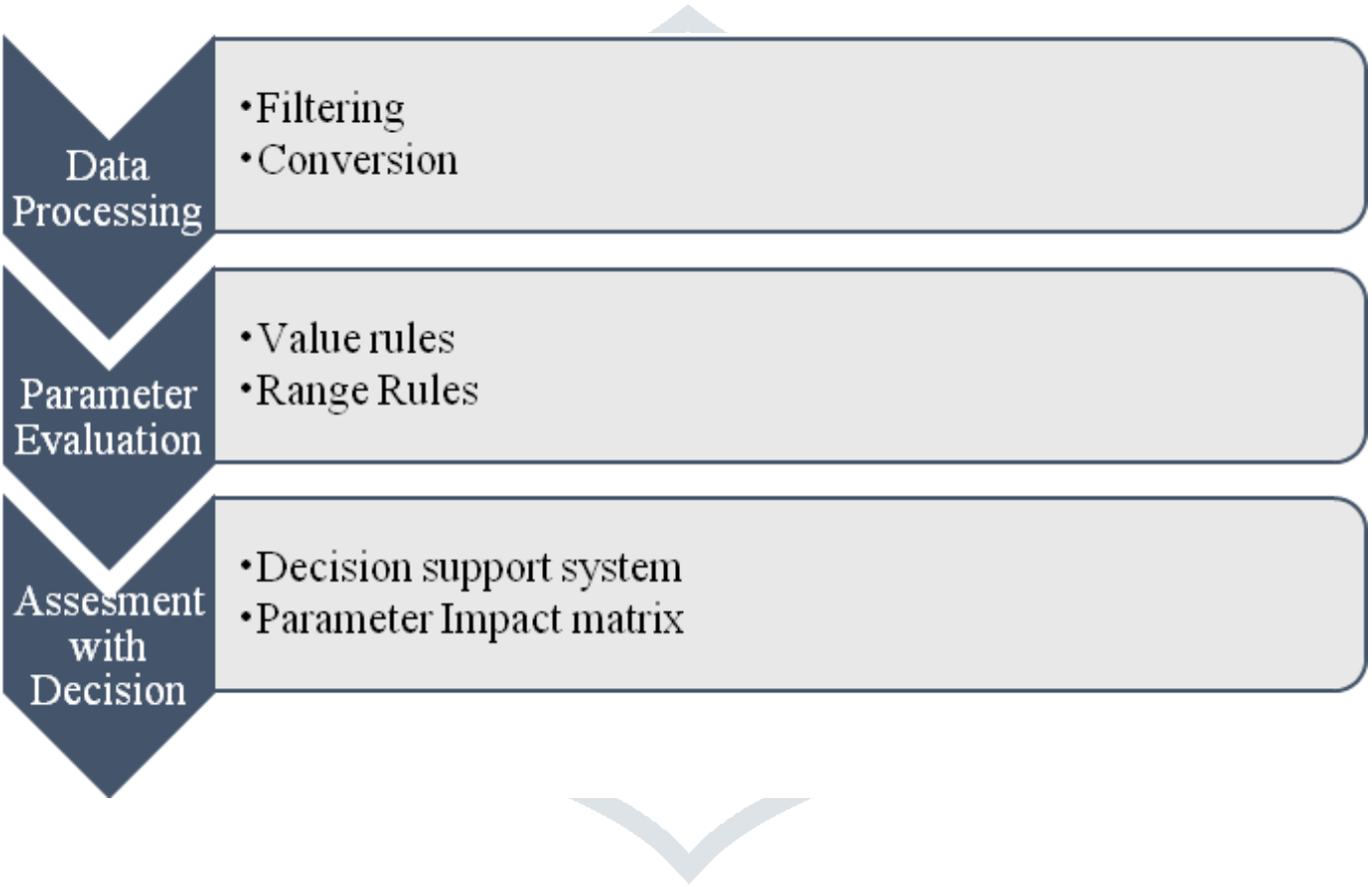
The PaaS model gives client ability to run software on cloud. In this model, the customer has ability to deploy his own applications or create his own applications by using tools supported by cloud provider. Though control over physical settings is restricted to cloud service provider, client of this model are able to fully managed deployed applications.

- Infrastructure as a Service (IaaS):

In IaaS model, consumer can provision computing resources like storage, processing and networks. Most of well-known cloud services like Amazon EC2 deploy this model. Users are charged according to amount of utilized resources. In this paper we will be concentrating on this model.

Cloud Assessment Procedure

The cloud assessment procedure is an easy-to-follow guided process. This process is described in flowchart below:



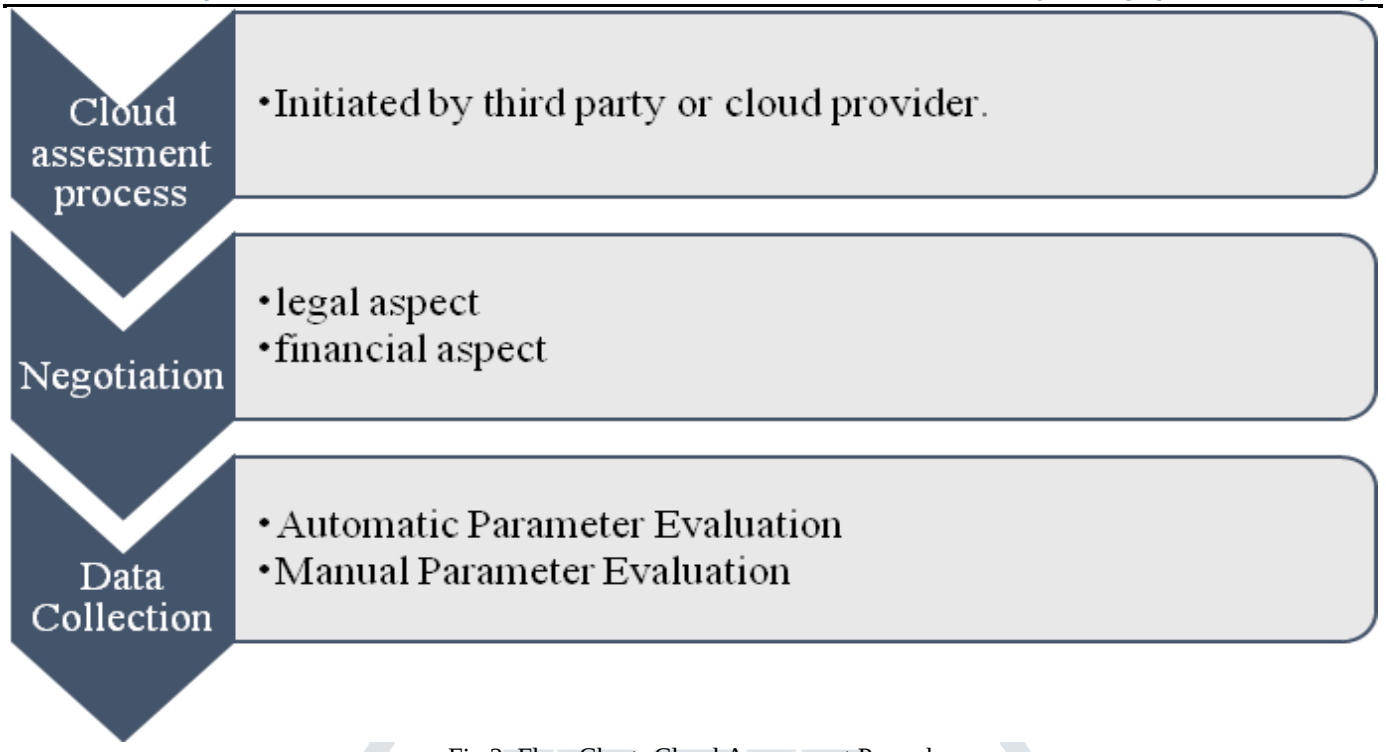


Fig 2 :Flow Chart- Cloud Assessment Procedure

The main elements of the assessment procedure are the following[3]:

1. Negotiation Phase:

In negotiation phase, service requirements like focus of assessment and special assessment target are identified.

2. Data collection Phase:

In data collection phase, data regarding cloud infrastructure, services and procedures is collected. The evaluation parameter is defined in advance. Manual data collection is carried out by auditor. The automatic data collection is carried out by CloudScope. Various measurement tools are integrated with internal architecture.

3. Data Processing Phase:

In data processing phase, data sets are collected, filtered, processed and converted to a single value. This value is then stored as evaluation parameter result.

4. Parameter Evaluation Phase:

In the parameter evaluation Phase, parameter is set for evaluation using predefined evaluation rules.

5. Cloud Assessment Phase:

In cloud assessment phase, evaluated parameter is multiplied by parameter impact matrix. According to decision rule, official assessment result is sent to cloud provider.

TABLE I
VULNERABILTY ASSESMENT METHODS AND COUNTER MEASURES

Sr. No.	Name of Vulnerability	Type	Counter Measures/ Assessment Tools
1	Insecure interfaces and APIs	IaaS	• Identify and access management guidance. • Web Application Scanner
2	Unlimited allocation of Resources	IaaS	• Cloud providers should implement policies to offer limited computational resources.
3	Data-related vulnerabilities	IaaS	• Destruction strategy should be specified on SLA.
4	Vulnerabilities in Virtual Machines	IaaS	• PALM • VNSS
5	Vulnerabilities in Virtual Machine Images	IaaS	• Mirage
6	Vulnerabilities in Hypervisors	IaaS	• Hypersafe • TCCP • TVDc
7	Vulnerabilities in Virtual Networks	IaaS	• Virtual network framework. It should be based on shared networks: bridged and routed.

1. Insecure Interfaces and APIs

Cloud computing provides services, which are accessed via through APIs like SOAP, REST or HTTP with XML or JSON. The security of cloud is dependent on these interfaces. Problems regarding insecure interfaces and APIs include weak credentials, insufficiently authorized checks and insufficient data validation. Another security hole in application is a fixed bug.

Counter measures are:

- **Identity and access management guidance**

Cloud Security Alliance provides security in cloud computing. It is a non-profit organization. It has issued a report that provides list of recommended best practices to ensure identities and access management. The report issued includes access management, centralized directory, identity management, user access certifications, role-based access control, identity and access reporting and separation of duties.

- **Web application scanners**

Web applications are targeted because they are exposed to public and potential attackers. Web application scanner scans web applications for identifying security vulnerabilities. Application similar to web application scanner is web application firewall. It routes all traffic via itself to inspect specific threats.

2. Unlimited Allocation of Resources

Unlimited allocation of resources is caused by inaccurate modelling of resource usage. It can lead to overbooking or over-provisioning.

Counter Measure:

Cloud providers should implement policies to offer limited computational resources.

3. Data-related Vulnerabilities

Data related vulnerabilities include, difference in location of data may cause difference in jurisdiction, also due to incomplete data deletion, and data cannot be deleted completely. As data back-up is done by third part providers it cannot be trusted. Information of data location is kept disclosed. Data is not encrypted or decrypted, but it is stored, processed and transferred in clear plain text.

Counter Measure:

Destruction strategy for data should be specified on the SLA.

4. Vulnerabilities in Virtual Machine

Vulnerabilities in virtual machine are caused by colocation of virtual machines and also by unrestricted allocation and deallocation of resources with virtual machines. It is also caused by uncontrolled migration and uncontrolled snapshots. Uncontrolled rollback also leads to vulnerabilities in virtual machines.

Counter Measures:

PALM:

Protection Aegis for Live Migration is a secure live migration framework for preserving integrity and privacy after migration. This system is implemented based on Xen and GNU Linux. This system adds to downtime due to encryption and decryption.

VNSS:

VNSS is a security framework that can customise security policies for each virtual machine. It also provides continuous protection via a virtual machine migration. It is implemented using firewall technologies and userspace tools.

5. Vulnerabilities in virtual machine images

Vulnerabilities in virtual machine include mismanaged placement of VM images in public repositories. It is impossible to patch VM images since they are dormant artefacts.

Counter Measure:

Mirage:

Mirage is virtual machine image management system in cloud computing. It provides following security features like image filters, access control framework, repository maintenance services and provenance tracking. The only limitation to this approach is that filters are not able to scan all malware or remove sensitive data from images. Filters also raise privacy concerns because they have to access content of images that may contain confidential data.

6. Vulnerabilities in Hypervisors

Vulnerabilities in hypervisors are caused by complexities in hypervisor code and flexible configuration of hypervisors, that may exploit needs of organization.

- **HyperSafe**

HyperSafe provides hypervisor control-flow integrity. It protects type I hypervisors using technologies, non bypassable memory lock down and restricted pointed indexing. Following four types of attack were conducted

1. Modify hypervisor code
2. Execute injected code
3. Modify the page table
4. Tamper from a return table.

The Hypersafe prevented all these attacks successfully. The overhead was low.

- **TCCP**

Trusted Cloud computing Platform offers closed box execution environments to users. The two important elements required are a trusted virtual machine monitor and a trusted coordinator. TCCP has downside that the transactions must be verified, this creates overload. This issue can be resolved by direct Anonymous attestation and privacy CA scheme.

7. Vulnerabilities in virtual Networks

Vulnerabilities in virtual networks are caused due to shared virtual bridges by several virtual networks.

Counter Measure:

- **Shared virtual bridges:**

In virtual network security, virtual network framework secures the communication among virtual machines. It has two configuration modes, bridged and routed. It consists of three layers routing layer, firewall and shared network layer. Security web services describe how to secure communication between applications. It is implemented through confidentiality, integrity, authorization and authentication.

III. Conclusion

Cloud computing is modern concept that provides many opportunities to users. Some of the limitations of cloud computing reduces its implementation. Overcoming vulnerabilities inn cloud will make organizations shift towards cloud. When cloud computing leverages other technologies, it also inherits their security issues. There are some solutions that help overcome vulnerabilities, but they are immature or practically impossible. In this paper, we have discussed vulnerabilities for IaaS cloud model. In this paper we have also discussed various vulnerabilities along with counter measures to overcome them. The cloud assessment procedure is also described in this paper. As an output, we can use processes and evaluation parameters for initiating cloud assessment service for cloud providers as well as customers.

FUTURE WORK

Cloud computing is said to be way of future. It has made applications and technologies accessible in recent years. Companies now require tremendous amount of data to succeed. It is important that sensitive data is well protected. In future, increment in implementation of vulnerability tools and techniques is expected for all three cloud models. Various technologies like CloudSpace are expected to evolve for betterment.

Acknowledgment

This work was performed as part of the research work sponsored by Savitribai Phule Pune University,Pune. The work was supported by funding from BCUD,Pune under the QIP programme of F.Y. 2015-17

References

[1] Rajesh P. Barnwal, Nirnay Ghosh and Soumya K. Ghosh, authors. Data and Application Security in Cloud, Published in Springer-Verlag Berlin Heidelberg 2014. DOI 10.10079

[2] Rahul Reddy Nadikattu. 2016 THE EMERGING ROLE OF ARTIFICIAL INTELLIGENCE IN MODERN SOCIETY. International Journal of Creative Research Thoughts. 4, 4 ,906-911.

[3] EveraldoAguiar, Yihua Zhang, and Marina Blanton authors, An Overview of Issues and Recent Developments in Cloud Computing and Storage Security springer 2014.

[4] Sikender Mohsienuddin Mohammad, "IMPROVE SOFTWARE QUALITY THROUGH PRACTICING DEVOPS AUTOMATION", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.251-256, March 2018, Available at :http://www.ijcrt.org/papers/IJCRT1133482.pdf

[5] M. Kozlovszkyauthor,Cloud Security Monitoring and Vulnerability Management, published in Springer 2016.

[6] RR Nadikattu, 2016 THE EMERGING ROLE OF ARTIFICIAL INTELLIGENCE IN MODERN SOCIETY. International Journal of Creative Research Thoughts. 4, 4 ,906-911.

[7] Mika D. Ayenson, Andre Guerlain Cloud Vulnerability Assesment in Major Qualifying Project Report submitted to the faculty of the WORCESTER POLYTECHNIC INSTITUTE.

[8] Sikender Mohsienuddin Mohammad, "AN EXPLORATORY STUDY OF DEVOPS AND IT'S FUTURE IN THE UNITED STATES", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.4, Issue 4, pp.114-117, November-2016, Available at :http://www.ijcrt.org/papers/IJCRT1133462.pdf

[9] Weibin Huang, Wushao Wen, and Da Yu, authors. Automated Vulnerability Assessment and Intrusion for Server Vulnerabilities, Published in Springer-2011.