Sanctuary Threats and Safety Mensuration on Cloud Computing

Shruthi BM[1], Priyanka KR[2]
[1, 2] Department of CSE
[1, 2] GSSS Institute of Engineering and Technology for Women, Mysuru, India

Abstract- *Cloud computing may be defined as management and provision of resources, software, applications and information as services over the cloud (internet) on demand. Cloud computing is a model for enabling 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 service provider interaction. With its ability to provide users dynamically scalable, shared resources over the Internet and avoid large upfront fixed costs, cloud computing has recently emerged as a promising hosting platform that performs an intelligent usage of a collection of services, applications, information and infrastructure comprised of pools of computer, network, information and storage resources. However along with these advantages, storing a large amount of data including critical information on the cloud motivates highly skilled hackers thus creating a need for the security to be considered as one of the top issues while considering Cloud Computing. In this paper we explain the cloud computing along with its open secure architecture advantages in brief and emphasize on various security threats in cloud computing also the existing methods to control them along with their pros and cons.*

Keywords- Identity and Access Management (IAM), Software-as-a Service (SaaS), Transparent Cloud Protection System (TCPS), Infrastructure-as-a-Service (IaaS).

I. INTRODUCTION

Cloud computing is the collection of virtualized and scalable resources, capable of hosting application and providing required services to the users with the "pay only for use" strategy where the users pay only for the number of service units they consume. A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way.

1.1. Characteristics of cloud computing

1. On-demand self-service. A consumer can unilaterally provision computing capabilities.

2. Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.

3. Resource pooling. The provider's computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

4. Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.

5. Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

II. OPEN SECURITY ARCHITECTURE OF CLOUD COMPUTING

Cloud computing can be defined as the provision of computing services via the Internet such as Applications (Software-as-a-Service (SaaS), Platforms, Infrastructure-as-a-Service (IaaS), Process orchestration and integration.

Figure 1 shows the open secure architecture of cloud computing. The Open Security Architecture cloud computing pattern is an attempt to illustrate core cloud functions, the key roles for oversight and risk mitigation, collaboration across various internal organizations, and the controls that require additional emphasis.

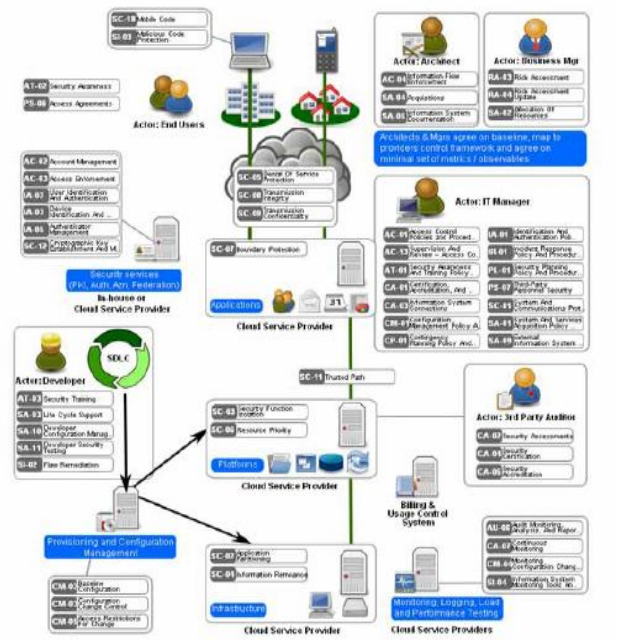

Fig 1: Cloud Computing Model

There are a number of key control areas that should be considered carefully before moving the computing operations to cloud services: Contractual agreements, Certification and third-party audits, Compliance requirements, Availability, reliability, and resilience, Backup and recovery, Service levels and performance, Decommissioning. If the process is comprised of a number of cloud services, then supporting services such as security, load monitoring & testing and provisioning and configuration management are required.

III. FEASIBILITY OF CLOUD COMPUTING

3. 1. Advantages of Cloud Computing:

The following are some of the major advantages of cloud computing:

- **Virtualization.** Virtualization is defined as decoupling and separation of the business service from the infrastructure needed to run it.
- **Elasticity.** Elastic nature of the infrastructure allows to rapidly allocate and de-allocate massively scalable resources to business services on a demand basis.
- **Cost Reduction.** Reduced costs due to operational efficiencies, and more rapid deployment of new business services**.**

3.2. Obstacles and opportunities of cloud computing

The following table shows the top ten obstacles and opportunities of cloud computing.

Table 3.1: Obstacles and opportunities of cloud Computing

No	Obstacle	Opportunities
1	Availability/Business Continuity	Use Multiple Cloud Providers
2	Data Lock-In	Standardize APIs; Compatible SW to enable Surge or Hybrid Cloud Computing
3	Data Confidentiality and Auditability	Deploy Encryption, VLANs, Firewalls
4	Data Transfer Bottlenecks	FedExing Disks; Higher BW Switches
5	Performance Unpredictability	Improved VM Support; Flash Memory; Gang Schedule VMs
6	Scalable Storage	Invent Scalable Store
7	Bugs in Large Distributed Systems	Invent Debugger that relies on Distributed VMs

IV. CLOUD COMPUTING SECURITY THREATS

1. Abuse and Nefarious Use of Cloud Computing.

Abuse and nefarious use of cloud computing is the top threat identified by the CSA. A simple example of this is the use of botnets to spread spam and malware. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines.

2. Insecure Application Programming Interfaces.

As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.

3. Malicious Insiders.

The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or how they monitor them. Transparency is, in this case,vital to a secure cloud offering, along with compliance reporting and breach notification.

4. Shared Technology Vulnerabilities.

Sharing infrastructure is a way of life for IaaS providers. Unfortunately, the components on which this infrastructure is based were not designed for that. To ensure that customers don't thread on each other's "territory", monitoring and strong compartmentalization is required.

5. Data Loss/Leakage.

Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe.

6. Data Loss/Leakage.

Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe.

7. Unknown Risk Profile.

Security should always in the upper portion of the priority list. Code updates, security practices, vulnerability profiles, intrusion attempts - all
things that should always be kept in mind.

V. SECURITY IN CLOUD COMPUTING

- **Infrastructure Security.** The security challenges at various levels namely network level, host level and application level are not specifically caused by cloud computing instead are exacerbated by its use. The issues of infrastructure security and cloud computing can be addressed by clearly defining trust boundaries by understanding which party provides which part of security.
- **Data Security and Storage.** Data security is a significant task, with a lot of complexity. Methods of data protection, such as redaction, truncations, obfuscation, and others, should be viewed with great concern. Not only are there no accepted standards for these alternative methods, but also there are no programs to validate the implementations of whatever could possibly be developed. Homomorphic encryption can be used for data security encryption.
- **Identity and Access Management (IAM).**The key critical success factor to managing identities at cloud providers is to have a robust federated identity management architecture and strategy internal to the organization.
- **Security Management.** From a security management perspective, a key issue is the lack of enterprise-grade access management features. The scope of security management of cloud services will vary with the service delivery model, provider capabilities, and maturity. Customers will have to make trade-offs with respect to the flexibility and control offered by the SPI services. The more flexible the service, the more control you can exercise on the service, and with that come additional security management responsibilities.
- **Privacy.** Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust and this need to be considered at every phase of design. The key challenge for software engineers to design cloud services in such a way as to decrease privacy risk and to ensure legal compliance. The following tips are recommended for cloud system designers, architects, developers and Testers.
- **Audit and Compliance.** A programmatic approach to monitoring and compliance will help prepare CSPs (Cloud Service Provider) and their users to address emerging requirements and the evolution of cloud business models. To drive efficiency, risk management, and compliance, CSPs need to implement a strong internal control monitoring function coupled with a robust external audit process.
- **Security-as-a [cloud] Service.** Security-as-a-service is likely to see significant future growth for two reasons. First, a continuing shift in information security work from in-house to outsourced will continue. Second, several other information security needs are present for organizations currently, but they will accelerate in need and complexity with the growing adoption of cloud computing. The two proactive controls are important to the growth of cloud computing: identity management that is inter-cloud and scalable to the cloud size, and key management.

VI. PROPOSED SOLUTIONS FOR SECURITY THREATS

6.1. Mirage Image Management System

The security and integrity of VM images are the foundation for the overall security of the cloud since many of them are designed to be shared by different and often unrelated users. This system addresses the issues related to secure management of the virtual-machine images that encapsulate each application of the cloud**.**

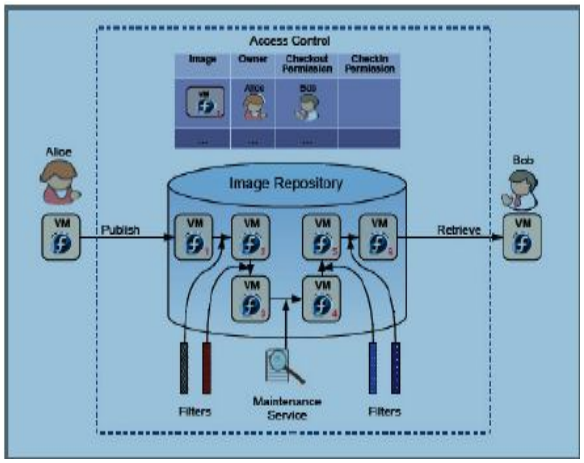

Fig 2: Architecture of Mirage Image Management System.

It consists of 4 major components**:**

1. Access Control. This framework regulates the sharing of VM images. Each image in the repository has a unique owner, who can share images with trusted parties by granting access permissions.
2. Image Transformation by Running Filters. Filters remove unwanted information from images at publishes and retrieval time. Filters at publish time can remove or hide sensitive information from the publisher's original image. Filters at retrieval time filters may be specified by the publisher or the retriever.
3. Provenance Tracking. This mechanism that tracks the derivation history of an image.
4. Image maintenance. Repository maintenance services, such as periodic virus scanning, that detect and fix vulnerabilities discovered after images are published**.**

6.2. Client Based Privacy Manager

Client based privacy manager helps to reduce the risk of data leakage and loss of privacy of the sensitive data processed in the cloud, and provides additional privacyrelated benefits.

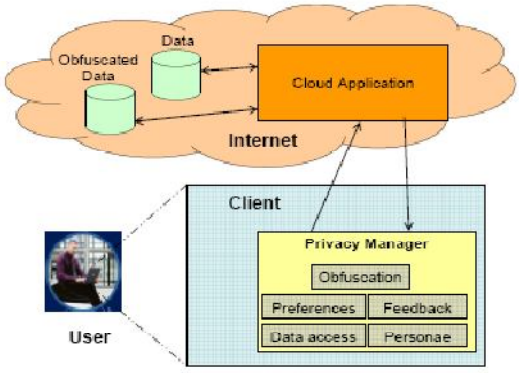

Fig 3: Architecture of the privacy manager.

The main features of the privacy manager are:

Obfuscation. This feature can automatically obfuscate some or all of the fields in a data structure before it is sent off to the cloud for processing, and translate the output from the cloud back into de-obfuscated form. The obfuscation and de-obfuscation is done using a key which is chosen by the user and not revealed to cloud service providers.

Preference Setting. This is a method for allowing users to set their preferences about the handling of personal data that is stored in an unobfuscated form within the cloud. This feature allows the user greater control over the usage of his data.

Data Access. The Privacy Manager contains a module that allows users to access personal information in the cloud, in order to see what is being held about them, and to check its accuracy. This is an auditing mechanism which will detect privacy violations once they have happened.

Feedback. The Feedback module manages and displays feedback to the user regarding usage of his personal information, including notification of data usage in the cloud. This module could monitor personal data that is transferred from the platform.

Personae. This feature allows the user to choose between multiple personae when interacting with cloud services.

6.3. Transparent Cloud Protection System (TCPS)

TCPS is a protection system for clouds aimed at transparently monitoring the integrity of cloud components. TCPS is intended to protect the integrity of guest Virtual Machines (VM) and of the distributed computing middleware by allowing the host to monitor guest VMs and infrastructure components.

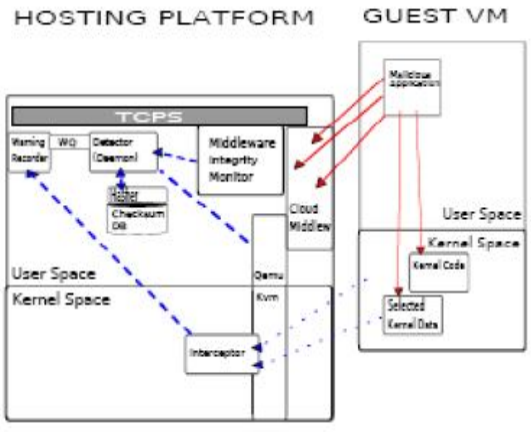

Fig 4: TCPS Architecture.

TCPS is a middleware whose core is located between the Kernel and the virtualization layer. By either actively or passively monitoring key kernel or cloud components. TCPS can detect any possible modification to kernel data and code, thus guaranteeing that kernel and cloud middleware integrity has not been compromised and consequently no attacker has made its way into the system.

All TCPS modules reside on the Host andQemu is leveraged to access the guest. Suspicious guest activity can be noticed by the Interceptor and they are recorded by the Warning Recorder into the Warning Queue where the potential alteration will be evaluated by the Detector component.

6.4. Secure and Efficient Access to Outsourced Data

Providing secure and efficient access to outsourced data is an important component of cloud computing and forms the foundation for information management and other operations**.**

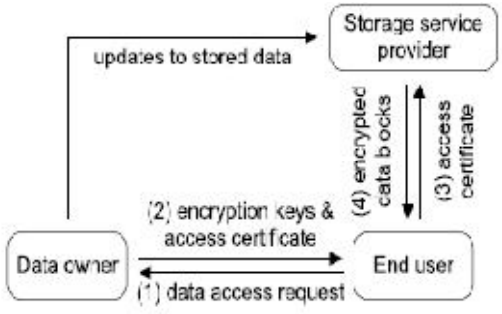

Fig 5: Illustration of application scenario

Figure 5 shows the typical owner-write-user read scenario. Only the owner can make updates to the outsourced data, while the users can read the information according to access rights. Since the data owner stores a large amount of information on the untrusted service provider, the owner has to encrypt the outsourced data before putting on the server.

VII. CONCLUSION

More than ten papers were surveyed regarding the cloud computing, advantages of cloud computing, risks in cloud computing and various approaches to solve those risks each with their pros and cons. Each algorithm is aimed at solving a particular risk. However cloud computing is still struggling in its infancy, with positive and negative comments made on its possible implementation for a large-sized enterprise. Several groups have recently been formed, such as the Cloud Security Alliance or the Open Cloud Consortium, with the goal of exploring the possibilities offered by cloud computing and to establish a common language among different providers. Cloud computing is facing several issues in gaining recognition for its merits. Its security deficiencies and benefits need to be carefully weighed before making a decision to implement it.

REFERENCES

[1] The NIST Definition of Cloud Computing, version 15, by Peter Mell and Tim Grance, October 7, 2009, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov)

[2] Wang, Lizhe; von Laszewski, Gregor; Kunze, Marcel; Tao, Jie. Cloud computing: A Perspective study, Proceedings of the Grid Computing Environments (GCE) workshop. Held at the Austin Civic Center: Austin, Texas: 16 November 2008.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. A view of cloud computing. Communications of the ACM , Volume 53 Issue 4, pages 50-58. April 2010.

[4] Open Security Architecture http://www.opensecurityarchitecture.org/

[5] Steve Bennett, Mans Bhuller, Robert Covington. Oracle White Paper in Enterprise Architecture – Architectural Strategies for Cloud Computing. August 2009. DOI= http://www.oracle.com/technology/architect/entarch/pdf/arc architectural_strategies_for_cloud_computing.pdf

[6] Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009. DOI = http://www.cloudsecurityalliance.org/topthreats/csathreats. v1.0.pdf

[7] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy : An Enterprise perspective of Risks and Compliance, O'Reilly Media, Inc., 2009

[8] Discovering Identity: Cloud Computing: Identity and Access Management DOI http://blogs.sun.com/identity/entry/cloud_computing_identity_and_access

[9] Siani Pearson. Taking Account of Privacy when Designing Cloud Computing Services. CLOUD '09: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, pages 44-52. May 2009.