IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Systematic Review of Security Issues for Cloud Computing

Sangeetha G[1], Divya V K[2]

Research Scholar, Computer Science, Bharathiar University, Coimbatore, India[1]

Information Science and Engineering, BMS College of Engineering, Bangalore, India[2]

Abstract: Cloud computing, undoubtedly, has become the buzzword in the IT industry today. Looking at the potential impact it has on numerous business applications as well as in our everyday life, it can certainly be said that this disruptive technology is here to stay. Many of the features that make cloud computing attractive, have not just challenged the existing security system, but have also revealed new security issues. This paper provides an insightful analysis of the existing status on cloud computing security issues based on a detailed survey carried by the author. It also makes an attempt to describe the security challenges in cloud computing and also endeavours to provide future security research directions.

Keywords: Computing, Cloud Computing Security, Trusted Third Party, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

I. INTRODUCTION

Clouds are large pools of easily usable and accessible virtualized resources. These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing optimum resource utilization. It's a pay-per-use model in which the Infrastructure Provider by means of customized Service Level Agreements (SLAs) offers guarantees typically exploiting a pool of resources. Organizations and individuals can benefit from mass computing and storage centers, provided by large companies with stable and strong cloud architectures.

Cloud computing incorporates virtualization, on-demand deployment, Internet delivery of services, and open source software. From one perspective, cloud computing is nothing new because it uses approaches, concepts, and best practices that have already been established. From another perspective, everything is new because cloud computing changes how we invent, develop, deploy, scale, update, maintain, and pay for applications and the infrastructure on which they run. Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth.

II. CLOUD COMPUTING SERVICES

A. Infrastructure-as-a-Service

The Infrastructure as a Service is a provision model in which an organization outsourcers the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Characteristics and components of IaaS include: 1. Utility computing service and billing model. 2. Automation of administrative tasks. 3. Dynamic scaling. 4. Desktop virtualization. 5. Policy-based services. 6. Internet connective Infrastructure-as-a-Service like Amazon Web Services provides virtual server instances with unique IP addresses and blocks of storage on demand. Customers use the provider's application program interface (API) to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed it's sometimes referred to as utility computing. Infrastructure as a Service is sometimes referred to as Hardware as a Service (HaaS).

B. Platform-As-A-Service

Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.54235

incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts. On the downside, PaaS involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve.

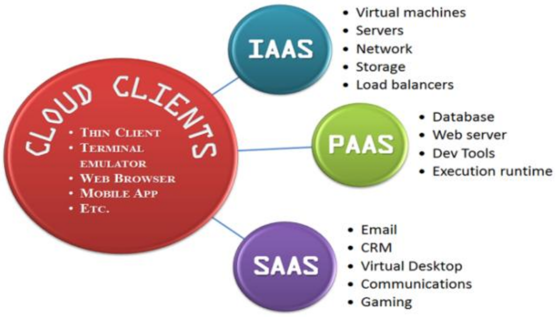

Fig1. Cloud Computing Services

C. Software-As-A-Service

No Software as a service sometimes referred to as "software on demand," is software that is deployed over the internet and/or is deployed to run behind a firewall on a local area network or personal computer. With SaaS, a provider licenses an application to customers either as a service on demand, through a subscription, in a "pay-as-you-go" model, or at no charge. This approach to application delivery is part of the utility computing model where all of the technology is in the "cloud" accessed over the Internet as a service. SaaS was initially widely deployed for sales force automation and Customer Relationship Management (CRM). Now it has become commonplace for many business tasks, including computerized billing, invoicing, human resource manage - ment, financials, content management, collaboration, document management, and service desk management.

III. PROBLEMS ASSOCIATED WITH CLOUD COMPUTING

Most security problems stem from:

- Loss of control
- Lack of trust (mechanisms)
- Multi-tenancy

These problems exist mainly in 3rd party management models

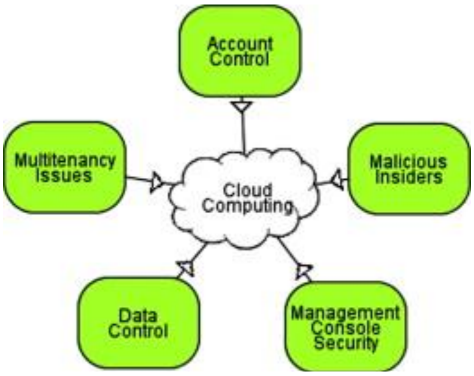

Fig 2. Problems associated with cloud computing

Self-managed clouds still have security issues, but not related to above.

A. Loss of Control in the Cloud

- Consumer's loss of control
    - ➢ Data, applications, resources are located with provider
    - ➢ User identity management is handled by the cloud
    - ➢ User access control rules, security policies and enforcement are managed by the cloud provider
    - ➢ Consumer relies on provider to ensure
- Data security and privacy
- Resource availability
- Monitoring and repairing of services/resources

B. Lack of Trust in the Cloud

- Defining trust and risk
    - ➢ Opposite sides of the same coin (J. Camp)
    - ➢ People only trust when it pays (Economist's view)
    - ➢ Need for trust arises only in risky situations
- Defunct third party management schemes
    - ➢ Hard to balance trust and risk
    - ➢ e.g. Key Escrow (Clipper chip)

Is the cloud headed toward the same path?

C. Multi-Tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
    - ➢ Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
    - ➢ Can tenants get along together and 'play nicely'?
    - ➢ If they can't, can we isolate them?
- How to provide separation between tenants?

D. Security Issues in the Cloud

In theory, minimizing any of the issues would help

1) Loss of Control:

Information and applications will always need to be on the cloud. How do we make it possible for customers to exercise more control?

2) Lack of trust:

Technology, policy and regulation, incentives in the form of contracts are a few mechanisms that may increase trust

3) Multi-tenancy:

There needs be a strong separation. While a private cloud takes away the reasons to use a cloud in the first place, VPC is still not a separate system.

A. Minimize Lack of Trust

1) Policy Language:

- Consumers have specific security needs but don't have a say-so in how these needs are handled. Consumers can't dictate their requirements to the providers as SLAs tend to be one sided. They are also largely unaware about what the provider is doing for them.
- Standard language to convey one's policies and expectations. This language need to be agreed upon and upheld by both parties. Moreover, there should be a standard language for representing SLAs and have the characteristics to be used in an intra-cloud environment to realize overarching security posture

DOI 10.17148/IJARCCE.2016.54235

- Create policy language with the following characteristics:
- Machine-understandable (or at least process able),
- Easy to combine/merge and compare
- Examples of policy statements are, “requires isolation between VMs”, “requires geographical isolation between VMs”, “requires physical separation between other communities/tenants that are in the same industry,” etc.
- Need a validation tool to check that the policy created in the standard language correctly reflects the policy creator’s intentions (i.e. that the policy language is semantically equivalent to the user’s intentions).

2) Certification:
Some form of reputable, independent, comparable assessment and description of security features and assurance

- Sarbanes-Oxley, DIACAP, DISTCAP, etc (are they sufficient for a cloud environment?)
- Risk assessment

– Performed by certified third parties
– Provides consumers with additional assurance

B. Minimize Loss of Control in the Cloud

- Monitoring
- Utilizing different clouds
- Access control management

C. Minimize Multi-tenancy in the Cloud

- Can’t really force the provider to accept less tenants
- Can try to increase isolation between tenants

– Strong isolation techniques (VPC to some degree)
– QoS requirements need to be met
– Policy specification

- Can try to increase trust in the tenants

– Who’s the insider, where’s the security boundary? Who can I trust?
– Use SLAs to enforce trusted behavior

IV. CONCLUSION

Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model.
However, resources are ubiquitous, scalable, highly virtualized; contain all the traditional threats, as well as new ones. In developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms of

- Loss of control
- Lack of trust
- Multi-tenancy problems

REFERENCES

[1] NIST (Authors: P. Mell and T. Grance), "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology Laboratory (October 7 2009).

[2] J. McDermott, (2009) "Security Requirements for Virtualization in Cloud Computing," presented at the ACSAC Cloud Security Workshop, Honolulu, Hawaii, USA, 2009.

[3] J. Camp. (2001), “Trust and Risk in Internet Commerce,” MIT Press

[4] T. Ristenpart et al. (2009) “Hey You Get Off My Cloud,” Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA

DOI 10.17148/IJARCCE.2016.54235