ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
DIIF 0.876

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 8, AUGUST 2015, PP 457-462

Security Issues' in Cloud Computing and its Solutions

Joga Singh
Department of Computer Science and Engineering
Global Institute of management & Emerging Technologies,
Amritsar, India
jogasingh66@gmail.com

Supreet Kaur
Department of Computer Science and Engineering
Global Institute of management & Emerging Technologies,
Amritsar, India
ksupreet9@gmail.com

Jasjit Kaur
Assistant Professor
Department of Computer Science and Engineering
Global Institute of management & Emerging Technologies,
Amritsar, India
jasjitkaur29@yahoo.com

Abstract -Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.

Keywords: Cloud Security, Virtualization.

I.INTRODUCTION

Cloud computing is predicted to be the next big revolution in the computing industry. Cloud is a dynamically scalable, network based computing environment where the resources required by the user are allocated as per requirement and revoked when the user task completes. It follows a utility based model in which the user pays as per resource utilization at the cloud. This characteristic of cloud computing makes it cheaper than the existing computing environments. The Cloud can cater to end user with its unlimited and highly scalable pool of resources. These resources may be in the form of memory, processing time, processing power, application software, software development platforms, storage space etc. Cloud computing can effectively address the computing needs of users of versatile scales ranging from an individual to large organizations. It can cater to resource needs of all. One aspect of the cloud which prevents users from using cloud services is data security. There are user concerns about the security and privacy of data at the cloud. Cloud security is a multifaceted and highly complex issue. The data owner's especially large organizations fear possible data misuse by the cloud provider without their knowledge. This concern is a major deterrent in the path of shifting operations to the cloud. An effective security model addressing all these concerns is provided in this paper. This paper proposes a hybrid cloud computing model which effectively handles the issues related to cloud data security including confidentiality, integrity, authentication and authorization. Our model handles both external as well as internal data security threats. It makes use of a hybrid cloud architecture using both private as well as public cloud. A dual layer of security is used in our model. One is authentication based on username and password and the other, the condition that the user should possess the key to decrypt a password stored at the cloud, without which the password filled by the user and the password stored cannot be compared.

ISSN (Online): 2349-7084

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 8, AUGUST 2015, PP 457-462

This completes the user authentication phase of our security model. For user authorization, a user role is associated with each user and stored at the cloud database. The user can only perform operations with respect to this role. This role is the one determined by the entity known as data owner in our model. Also, for processing data at the cloud and keeping it safe from the cloud, a cryptographic process is proposed. If the user is authenticated and authorized then the operations requested on the data are performed including manipulation and processing of the data. This is done by the invocation of a cryptographic process which takes a key defined by the data owner in executable form as input from cloud database and loads into memory. This process decrypts the data, caters it to requesting processes and encrypts it before storing it back. Symmetric key encryption, which is highly efficient, is used for both decrypting and encrypting data. Since the key is in executable form so it is safe from any modifications by the cloud provider. Also the cryptographic process is made a part of the operating system therefore, eliminating the control of cloud on this process

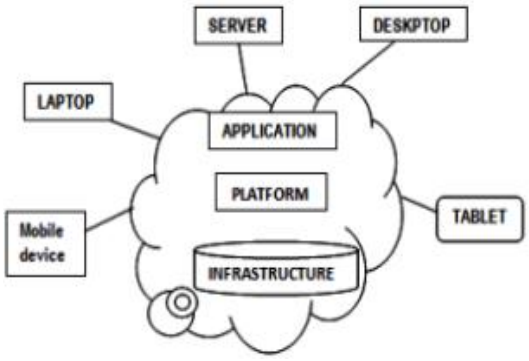

Fig. 1. Concept of Cloud Computing

II.RELATED WORK

There are number of models and techniques proposed for increasing data security and access control at the cloud. These works propose encryption for securing data at the cloud, analyze the various risks involved with keeping data at the cloud, propose the establishment of Trusted Third party services at the cloud and so forth. The work done by Lan Zhou [1] in the area of cloud computing proposes a technique using role based encryption to help secure data at the cloud. In this technique, the data at the cloud is encrypted and the keys to decrypt this data also include the role, the user possessing the key can exercise on the data. The technique is efficient and easy to implement but has serious problems. For instance, if the cloud needs to process the data, then the data decryption is inevitable. In such a situation, the unauthorized users have no access to the data but the cloud will have access to all the data in decrypted form. Therefore, the data can be misused by the cloud provider without the knowledge of the data owner. This problem is solved by our model, using a process that enters the memory before any user data is read. This process has a symmetric key embedded in it for both encrypting and decrypting the data. Therefore, the data is decoded and encoded in the memory only. Since it is hard to read memory while data is being processed, therefore the data is never revealed to the cloud provider. Another work includes the cloud computing model proposed by Dimitrios Zissis [2], which relies on the concept of Trusted Third party services in order to make the cloud more secure and trusted among organizations for keeping sensitive data. Although this technique can be useful for cultivating trust among the users but it also has its own set of problems. There may be issues when the cloud client decides to shift from one cloud provider to the other. Also the Cloud provider may or may not follow the third party completely. Switching from one cloud provider to another may not be feasible in such a model. Our proposed model has no such problem, as it can be easily implemented at every cloud with a very low cost associated with it. Another work done in the direction of making the cloud more secure includes Rhonda Farrell's paper [3] which discusses the various kinds of risks associated with cloud computing in general. These risks are evaluated with respect to various cloud computing models such as PaaS, IaaS and SaaS. The paper does not discuss anything regarding the solution to these problems and hence only creates awareness about the various security

issues associated with the cloud. Our model solves most of the issues that are mentioned in the paper by Rhonda Farrell [3]. Another paper by Klaus Julisch [4] proposes the use of virtual information security management system, which can help improve information security, but the proposed technique is complex as compared to the one proposed in our paper. Our proposed model helps reach an optimal security level without compromising on performance and is better than most proposed models, as tested on Hadoop simulator. The results are promising and the level of security is high compared to other proposed models thereby enhancing data security at the cloud on all fronts.

III.SECURITY ISSUES

A. Software as a Service (SAAS): SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM. SaaS users have less control over security among the three fundamental delivery models in the cloud. The adoption of SaaS applications may raise some security concerns.

B. Platform-as-a-service (PaaS) security issues:PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers. As with SaaS and IaaS, PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform . PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications. Same as SaaS, PaaS also brings data security issues and other challenges that are described as follows:

B1 Third-party relationships

Moreover, PaaS does not only provide traditional programming languages, but also does it offer third-party web services components such as mashups that combine more than one source element into a single integrated unit. Thus, PaaS models also inherit security issues related to mashups such as data and network security. Also, PaaS users have to depend on both the security of web-hosted development tools and third-party services

B.2 Development Life Cycle

From the perspective of the application development, developers face the complexity of building secure applications that may be hosted in the cloud. The speed at which applications will change in the cloud will affect both the System Development Life Cycle (SDLC) and security. Developers have to keep in mind that PaaS applications should be upgraded frequently, so they have to ensure that their application development

C. Infrastructure-as-a-service (IaaS) security issues

IaaS provides a pool of resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet. Users are entitled to run any software with full control and management on the resources allocated to them. With IaaS, cloud users have better control over the security compared to the other models as long there is no security hole in the virtual machine monitor. They control the software running in their virtual machines, and they are responsible to configure security policies correctly. However, the underlying compute, network, and storage infrastructure is controlled by cloud providers. IaaS providers must undertake a substantial effort to secure their systems in order to minimize these threats that result from creation, communication, monitoring, modification, and mobility. Here is some of the security issues associated to IaaS.

D. Virtualization

Virtualization allows users to create, copy, share, migrate, and roll back virtual machines, which may allow them to run a variety of applications. However, it also introduces new opportunities for attackers because of the extra layer that must be secured. Virtual machine security becomes as important as physical machine security, and any flaw in either one may affect the other. Virtualized environments are vulnerable to all types of attacks for normal infrastructures; however, security is a greater challenge as virtualization adds

ISSN (Online): 2349-7084

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 8, AUGUST 2015, PP 457-462

more points of entry and more interconnection complexity. Unlike physical servers, VMs have two boundaries: physical and virtual.

E. Shared resource

VMs located on the same server can share CPU, memory, I/O, and others. Sharing resources between VMs may decrease the security of each VM. For example, a malicious VM can infer some information about other VMs through shared memory or other shared resources without need of compromising the hypervisor . Using covert channels, two VMs can communicate bypassing all the rules defined by the security module of the VMM. Thus, a malicious Virtual Machine can monitor shared resources without being noticed by its VMM, so the attacker can infer some information about other virtual machines.

IV.SECURITY SOLUTION

A. Software as a Service (SAAS): Software-as-a-Service (SaaS) Security Solutions provide industry-leading Internet content security for individual users, small, medium and enterprise businesses, as well as service provider partners. These hosted service offerings leverage the strength of the Trend Micro Smart Protection Network™ to immediately and automatically protect customers' information and resources against the latest threats wherever they connect. Moreover, all SaaS solutions are hosted and maintained by Micro security experts, ensuring easy deployment and 24x7 availability. This also allows Service Providers to focus on quick application delivery with no capital expenditure (CAPEX) and therefore minimum financial exposure.

Worry-Free Business Security Services

Designed primarily for small business customers but also suitable for larger companies, it protects desktops and laptops wherever they are connected—in the office, at home, or on the road.

Hosted Email Security

A no-maintenance-required solution that delivers continuously updated protection to stop spam and email based malware before they reach the customer's network.

Email Security Platform for Service Providers

Provides email filtering, anti-spam, and antivirus within a centrally managed, highly scalable architecture—complete with a customizable user interface and tiered administration levels.

B. Platform-as-a-service (PaaS) security

Platform as a Service (PaaS) is one of three main forms of cloud computing, where companies rent hardware and software from a third party. The platform is accessed across a private network or the internet and used to build applications rather than owning, running and developing on an internal IT infrastructure. PaaS sits in the middle of these two models: SaaS and IaaS. Essentially a company rents the hardware, operating systems, storage and network capacity that IaaS provides but also software servers and applications environments. This gives customers a platform on which they can load their data and start the developing applications they need. But being between IaaS and SaaS means that there is a great deal of overlap at both ends of the PaaS spectrum. There is no real agreement on what PaaS is and where these three forms start and stop so perhaps an example is the best way to get the idea across.

C. Infrastructure-as-a-service (IaaS)

Data Leakage Protection and Usage Monitoring:

Data stored in IaaS infrastructure in both private and public cloud needs to be monitored closely [8]. This is essential when IaaS is deployed in public cloud. In this, it should be known that who is accessing the information, how it is accessed, location from where it is accessed and what happened to accessed information later. These problems can be solved by using modern Rights Management services applying restriction to business critical data. Policies for information need to be created and deployed. In addition, transparent process can be created that monitors information usage.

End to End Logging and Reporting

The effective deployment of IaaS demands comprehensive logging and reporting in place. Robust logging and reporting solutions helps to keep track of where the information is, who accesses it, which machines are handling it and which storage arrays are

responsible for it. These solutions are important for service management and optimization.

Authentication and Authorization

Robust authentication and authorization helps to get effective Data Loss Prevention (DLP) solution. For every application, just user name and password is not most secure authentication mechanism. Sometime two factor or multi-factor authentication is needed. We need to consider tiering access policies based on level of trust.

Infrastructure Hardening "Golden-image" VM and VM templates need to be hardened and cleaned [10]. This can be done while images are created. On regular basis, testing of these master images need to be done. E. End to end encryption IaaS as a service, both in public and private clouds, needs to take advantage of encryption from end-to-end. We can make use of whole disk encryption to encrypt all the data including user files on the disk. This prevents offline attacks. In addition to disk encryption, all communications to host OS and VMs in the IaaS infrastructure are encrypted. This can be done over SSL/TLS or IPSec.

D. Virtualization

Patching is Safer and More Effective

• You can quickly revert to a previous state if a patch is unsuccessful, making you more likely to install security patches sooner

• You can create a clone of a production server easily, making you more likely to test security patches and more likely to install security patches

• VMware Update Manager does patch scanning and compliance reporting, along with patch remediation for both online and offline VMs – again, making it more likely that security patches will be installed

More Cost Effective Security Devices

• You can put in place cost effective intrusion detection, vulnerability scanning, and other security related appliances, because you can put them in a VM instead of a physical server

Leveraging Virtualization to Provide Better Security

• Better Context – Provide protection from outside the OS, from a trusted context

• New Capabilities – view all interactions and contexts

• CPU

• Memory

• Network

• Storage

E. Shared resource

Virtualization enhances cloud security. First, VMs add an additional layer of software that could become a single point of failure. That is, virtualization lets us divide or partition a single physical machine into multiple VMs (as with server consolidation), giving each VM better security isolation and protecting each partition from DDoS attacks by other partitions. Security attacks in one VM are isolated and contained — VM failures don't propagate to other VMs. A hypervisor provides the same visibility as the guest OS but with complete guest isolation. This fault containment and failure isolation VMs provide allows for a more secure and robust environment. Furthermore, a sandbox provides a trusted zone for running programs.5 It can provide a tightly controlled set of resources for guest OSs, which lets us define a security testbed on which to run untested code and programs from untrusted third-party vendors. With virtualization, the VM is decoupled from the physical hardware; we can represent it as a software component and regard it as binary or digital data. This implies that we can save, clone, encrypt, move, or restore the VM with ease. VMs also enable higher availability and faster disaster recovery.

V.CONCLUSION

Although Cloud computing can be seen as a new phenomenon which is set to revolutionise the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

REFERENCES

[1] Lan Zhou, Vijay Varadharajan and Michael Hitchens. Enforcing Role Based Access Control for

secure data storage in the cloud. September, 2011, p. 1-10

[2] Dimitrios Zissis, Dimitrios Lekkas. Addressing Cloud computing security issues. December, 2010, p. 1-8

[3] Rhonda Farrell. Securing the Cloud—Governance, risk and Compliance issues reign supreme. November, 2010, p. 310-20

[4] Klaus Julisch & Michael Hall. Security and control in the cloud. November, 2010, p. 299-310

[5] S. Subashini, V. Kavitha. A survey on security issues in service delivery models of cloud computing. July, 2010, p. 1-7

[6] Derek Mohammed. Security in Cloud Computing: An analysis of key drivers and constraints. May, 2010, p. 123-29

[7] Sean Marston, Zhi Li, Shubhajyoti Bandyopadhaya, Juheng Zhang, Anand Ghalsasi. Cloud Computing the Business Prespective. December, 2010, p. 177-88