Cloud Computing Security Issues in Infrastructure as a Service

Varsha Bansal[1],
[1]M.Tech
Department of Computer Science and Engineering
GITAM, MDU Rohtak

Mr. Ashish Kumar Sharma[2],
[2]Assistant Professor
Department of Computer Science and Engineering
C.F.I.S, GITAM, MDU Rohtak

Dr. Neetu Sharma[3]
[2]Head of Department
Computer Science & Engineering & C.F.I.S,
GITAM, Kablana, Jhajjar, Haryana

Cloud computing is a style of computing which is having dynamically scalable virtualized resources provide as a service over the internet .It reduces the time required to procure heavy resources and boot new server instances in minutes allowing one to quickly scale capacity, both up and down, as ones requirement changes. Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer will certainly affect the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. This paper presents an elaborated study of IaaS components' security and determines vulnerabilities and countermeasures. Service Level Agreement should be considered very much importance.

Keywords— ***Computing, Cloud Computing Security, Service Level Agreement (SLA), Infrastructure as a Service (SaaS)***

I. INTRODUCTION

Cloud technology is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks (public/ private), i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing all run in cloud[1].

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. Cloud computing uses the internet and central remote servers to maintain data and applications. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. In the recent time E-Governance is being implemented in developing countries to improve efficiency and effectiveness of governance. This approach can be improved much by using cloud computing instead of traditional ICT.

II. CLOUD COMPUTNG SERVICES

1)Infrastructure as a service (IaaS)

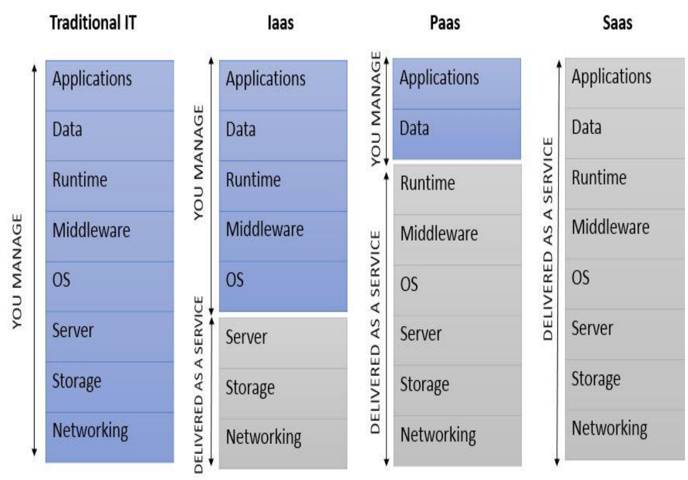
IaaS clouds often offer additional resources like as virtual-machine disk-image library,raw blockstorage,file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. IaaS-cloud providers supply these resources on-demand from their large pools of equipment installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds (dedicated VPN). To deploy their applications, cloud users install operating-system images and their application software on the cloud infrastructure. In Iaas, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill IaaS services on a utility computing basis: cost reflects the amount of resources allocated and consumed.

2) Platform as a service (PaaS)

This type of cloud computing deliver development environments as a service. You build your own applications that run on the provider's infrastructure and are delivered to your users via the Internet from the provider's servers. Like Legos, these services are constrained by the vendor's design and capabilities, so you don't get complete freedom, but you do get predictability and pre-integration. Prime examples include Coghe ad and the new Google App Engine. For extremely lightweight development, cloud-based abound, such as Yahoo Pipes or Dapper.net.

3) Software as a service (SaaS)

On the customer side, it means no upfront investment in servers or software licensing; on the provider side, with just one app to maintain This types of cloud computing delivers a single application through the browser to thousands of, costs are low compared to conventional hosting. SaaS is also common for HR apps and has even work edits way up the food chain to ERP, with players such as Workday. And some who could have predicted the sudden rise of SaaS desktop applications, like as Google Apps and Zoho-Office[2].



III. CLOUD COMPUTNG SECURITY ISSUES

In the last few years, cloud computing has grown from being a promising business concept for the fastest growing segments of the IT industry.

A. Security

Where is your data more secure, on high security servers or on your local hard driver in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. In the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft .

B. Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center(VDC) rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users .

C. Reliability

Servers in the cloud have the same problems as you can have in your own resident servers. The cloud servers also experience downtimes and slowdowns, the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

E. Open Standard

Open standards are critical to the growth of cloud computing. Most cloud providers expose APIs which are typically well-Documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs and there are a number of open standards under development, including the OGF's Open Cloud Computing Interface. The Open Cloud Consortium (OCC) is working to develop consensus on early cloud computing standards and practices.

F. Freedom

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data in a form that retains their freedom of choice and protects them against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring[3] .

IV. CLOUD COMPUTNG MODELS

A. Public Cloud

A public cloud is built over the Internet, which can be accessed by any user who has paid for the service. Public clouds are owned by service providers. They are accessed by subscription. Many companies have built public clouds, namely Google App Engine, Amazon AWS(Amazon web services), Microsoft Azure, IBM Blue Cloud, and Sales Force.com. These are commercial providers that offer a publicly accessible remote interface for creating and managing VM instances within their proprietary infrastructure. A public cloud delivers selected set of business processes. The application and infrastructure services are offered quite flexible price per use basis[4].

B. Private Cloud

The "private cloud" is built within the domain of an intranet owned by a single organization. Therefore, they are client owned and managed. Their access is limited to the owning clients and their partners. Their deployment was not meant to sell capacity over the Internet through publicly accessible interfaces. Private clouds give local users a flexible and agile private infrastructure to run service workloads within their administrative domains. A private cloud is supposed to deliver more efficient and convenient cloud services. They can have the impact on the cloud standardization, while retaining greater customization and organizational control[4].

C. Community Cloud

Private cloud (also called internal cloud or corporate cloud) is a marketing term for a proprietary computing architecture that provides hosted services to a limited number of people behind a firewall. Advances in virtualization and distributed computing have allowed corporate network and datacenter administrators to effectively become service providers that meet with the requirements of their "customers" within the corporation. Marketing media that uses the words "private cloud" is designed to appeal to an organization that needs or wants more control over their data than they can get by using a third-party hosted service such as Amazon's Elastic Compute Cloud (EC2) or Simple Storage Service (S3).

D .Hybrid Cloud

A hybrid cloud is a Cloud Computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in-house storage for operational customer data. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities.

V. ALL CLOUD MODELS ARE NOT THE SAME

Although the term Cloud Computing is widely used, it is important to note that all Cloud Models are not the same.
like, it is critical that organizations don't apply a broad brush one-size fits all approach to security across all models. Cloud Models can be segmented into Software as a Service (Saas), Platform as a service (PaaS) and Integration as a Service (IaaS). When an organization is considering Cloud Security it should consider both the differences and similarities between these three services of Cloud Models.

VI. IAAS COMPONENTS

IaaS delivery model consists of several main components that havebeen developed through past years, nevertheless, employing those IaaS delivery model consists of several components that have components together in a shared and outsourced environment carries multiple challenges. Security and Privacy are the most significant challenges that may impede the Cloud Computing adoption. Breaching the security of any component impact the other components' security, consequently, the security of the entire system will collapse. In this section we study the security issue of each component and discuss the proposed solutions and recommendations.

A.Service Level Agreement (SLA)

Cloud Computing emerges a set of IT management complexities, and using SLA in cloud is the solution to guarantee acceptable level of QoS(quality of services). SLA encompasses SLA contract definition, SLA monitoring, and SLA enforcement. SLA contract definition and negotiation stage is important to determine the benefits and responsibilities of each party, any misunderstanding will affect the systems security and leave the client exposure to vulnerabilities. On the other hand, monitoring and enforcing SLA stage is crucial to build the trust between the provider and the client. To enforce SLA in a dynamic environment such Cloud, it is necessary to monitor QoS attributes continuously. Web Service Level Agreement (WSLA) framework developed for SLA monitoring and enforcement in SOA. Using WSLA for managing SLA in Cloud Computing environment was proposed in by delegating SLA monitoring and enforcement tasks to a third party to solve the trust problem. Currently, cloud clients have to trust providers' Service level agreement monitoring until standardizing Cloud Computing systems and delegating third-parties to mediate SLA monitoring and enforcement[5].

B. Utility Computing

Utility Computing is not new concept; it plays an essential role in Grid Computing deployment. It packages the resources (e.g., computation, storage, etc...) as metered services and delivers them to the client. The power of this model lies in two main points: First, it reduces the total cost, i.e., instead of owning the resources, client can only pay for usage time (pay-as-you-go). Second, it has been developed to support the scalable systems, i.e., as an owner for a rapid growing system you need not to worry about denying your service according to a rapid increase of users or reaching peak in demand. Obviously, Utility Computing shapes two of the main features of the Cloud Computing.The first challenge to the Utility Computing is the complexity of the Cloud Computing, for example, the higher provider as Amazon must offer its services as metered services. Those services can be used by second level providers who also provide metered services. In such multiple layers of utility, the systems become more complex and require more management effort from both the higher and the second level providers. Amazon DevPay5, an example for these systems, allows the second level provider to meter the usage of AWS services and bill the users according to the prices determined by the user. The second challenge is that Utility Computing systems can be attractive targets for attackers, so an attacker may aim to access services without paying, or can go further to drive specific company bill to unmanageable levels. The provider is the main responsible to keep the system healthy and well functioning, but the client's practice also affects the system.

C. Cloud Software

There are many open source Cloud software implementations such as Eucalyptus and Nimbus 6; Cloud software joins the cloud components together. Either Cloud software is open source or commercial closed source. We can't ensure the vulnerability and bugs in available software, furthermore, cloud service providers furnish APIs (REST, SOAP, or HTTP with XML/JSON) to perform most management functions, such as access control from a remote location . For example, client can use the Amazon EC2 toolkits, a widely supported interface, to consume the services by implementing own applications or by simply using the web interfaces offered by the provider. In both cases, user uses web services protocols. SOAP is the most supported protocol in web services; many SOAP based security solutions are researched, developed, and implemented.
Extension for security in SOAP, addresses the security for web services. It defines a SOAP header (Security) that carries the WS-Security extensions and determines how the existing XML security standards like XML Signature and XML Encryption are applied to SOAP messages. Well known attacks on protocols using XML Signature for authentication or integrity protection would be applied to web services consequently affecting the Cloud services. Finally, an extreme scenario in showed the possibility of breaking the security between the browser and the clouds, and followed by proposal

to enhance the current browsers security. Indeed, these attacks belong more to the web services world, but as a technology used in Cloud Computing, web services' security strongly influences the Cloud services' security.

D. Platform Virtualization

Virtualization, a fundamental technology platform for Cloud Computing services, facilitates aggregation of multiple standalone systems into a single hardware platform by virtualizing the computing resources (e.g., network, CPUs, memory, and storage). Hardware abstraction hides the complexity of managing the physical computing platform and simplifies the computing resources scalability. Hence, virtualization provides multi tenancy and scalability, and these are two significant characteristics of Cloud Computing As the hypervisor is responsible for VMs isolation, VMs could not be able to directly access others' virtual disks, memory, or applications on the same host. IaaS, a shared environment, demands an accurate configuration to maintain strong isolation. Cloud service providers undertake a substantial effort to secure their systems in order to minimize the threats that result from communication, monitoring, modification, migration, mobility, and DoS. Virtualization risks and vulnerabilities affect particularly IaaS delivery model in addition to the recent proposed solutions to guarantee security, privacy, and data integrity for IaaS[6].

VII. SECURITY MODEL FOR IAAS

As a result of this research, we also discuss a Security Model for IaaS (SMI) as a guide for assessing and enhancing security in each layer of IaaS delivery model. SMI model consists of 3 sides: IaaS components, security model, and the restriction level. The front side of the cubic model is the components of IaaS which were discussed thoroughly in the previous sections. The security model side includes three vertical entities where each entity covers the entire IaaS components. The first entity is Secure Configuration Policy (SCP) to guarantee a secure configuration for each layer in IaaS Hardware, Software, or "SLA" configurations; usually, miss-configuration incidents could jeopardize the entire security of the system. As a result of this research, we propose a Security Model for IaaS (SMI) as a guide for assessing and enhancing security in each layer of IaaS delivery model could jeopardize the entire security of the system. The second is a Secure Resources Management Policy.

(SRMP) that controls the management roles and privileges. The last entity is the Security Policy Monitoring and Auditing (SPMA) which is significant to track the system life cycle. The restriction policy side specifies the level of restriction for security model entities. The level of restriction starts from loose to tight depending on the provider, the client, and the service requirements. Nevertheless, we hope SMI model be a good start for the standardization of IaaS layers. This model indicates the relation between IaaS components and security requirements, and eases security improvement in individual layers to achieve a total secure IaaS system.

VIII. CONCLUSION

In This paper I discuss about Various Layers of Infrastructure as a Service. We can also Provide Security by having a public key infrastructure on each layer that we discuss in this paper. The SLA's discuss only about the services provided and the waivers given if the services not met the agreement, but this waivers do not really help the customers fulfilling their losses. In this Paper I also discuss the Security holes associated with Iaas implementation. The security issues presented here concern the security of each IaaS component in addition to recent proposed solutions.

ACKNOWLEDGEMENT

I would like to express my appreciation to Mr. Ashish Kumar Sharma Assistant Professor for his guidance and support. Without his valuable assistance, this work would not have been completed.

I am also thankful to Dr. Neetu Sharma, the Head of Department of Computer Science and Engineering in Ganga institute of technology and management for her valuable cooperation and assistance.

REFERENCES

[1] https://www.tutorialspoint.com/cloud_computing/cloud_computing_overviewhtm
[2] [2].www.infoworld.com/article/2683784/cloud.../what-cloud-computing-really-means.ht...
[3] https://books.google.co.in/books?isbn=1466658894
[4] https://ameensheriffmca.files.wordpress.com/2014/07/unit-1-question-answer.docx
[5] www.isroset.org/pub_paper/ijsrcse/isroset-ijsrcse-001512.pdf
[6] www.ifet.ac.in/pages/intsymp15/TechnoVision%20'15/.../arivazhagan.pdfwww.slideshare.net/.../cloud-computing-security-issues-in-infrastructure-as-a-service-r...