Volume 2, Issue 1, January 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Cloud Computing Security Issues in Infrastructure as a Service

Pankaj Arora*
M.*Tech* CSE, *IGCE.*
Punjab Technical univ.

Rubal Chaudhry Wadhawan
Asstt.prof (CSE), IGCE
Punjab technical univ.

Er. Satinder Pal Ahuja
Associate Professor & HOD (CSE),IGCE
Punjab technical Univ.

Abstract— **Cloud computing is current buzzword in the market. It is paradigm in which the resources can be leveraged on per use basis thus reducing the cost and complexity of service providers. Cloud computing promises to cut operational and capital costs and more importantly let IT departments focus on strategic projects instead of keeping datacenters running. It is much more than simple internet. It is a construct that allows user to access applications that actually reside at location other than user's own computer or other Internet-connected devices. There are numerous benefits of this construct. For instance other company hosts user application. This implies that they handle cost of servers, they manage software updates and depending on the contract user pays less i.e. for the service only. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. 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

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 COMPUTNG 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. Plateform-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 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.

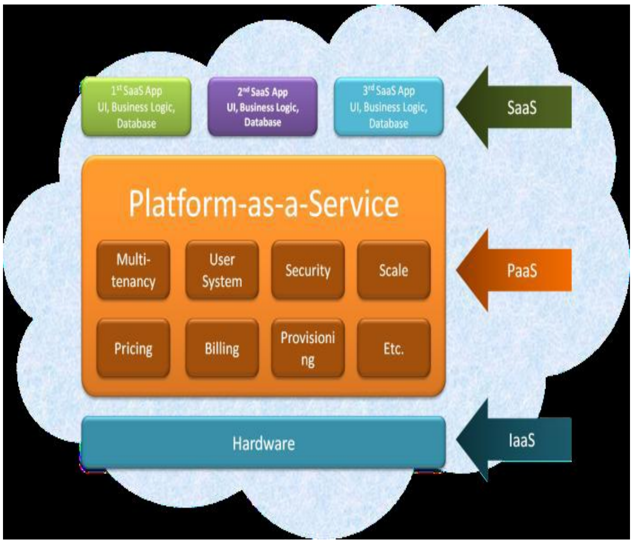

1st SaaS App UI, Business Logic, Database
2nd SaaS App UI, Business Logic, Database
3rd SaaS App UI, Business Logic, Database
SaaS
Platform-as-a-Service
Multi-tenancy
User System
Security
Scale
PaaS
Pricing
Billing
Provisioning
Etc.
Hardware
IaaS

Fig 1: 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 management, financials, content management, collaboration, document management, and service desk management.

III. CLOUD COMPUTNG SECURITY ISSUES

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

A. *Security*

Where is your data more secure, on your local hard driver or on high security servers 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. However, 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 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 your own resident servers. The cloud servers also experience downtimes and slowdowns, what 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.

D. *Legal Issues*

Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose "availability zones" . On the other hand, worries stick with safety measures and confidentiality from individual all the way through legislative levels.

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. Compliance

Numerous regulations pertain to the storage and use of data require regular reporting and audit trails, cloud providers must enable their customers to comply appropriately with these regulations. Managing Compliance and Security for Cloud Computing, provides insight on how a top-down view of all IT resources within a cloud-based location can deliver a stronger management and enforcement of compliance policies. In addition to the requirements to which customers are subject, the data centres maintained by cloud providers may also be subject to compliance requirements.

G. 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 .

H. Long-term Viability

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application.

IV. CLOUD COMPUTNG MODELS

A. Public Cloud

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

The main benefits of using a public cloud service are:

1. Easy and inexpensive set-up because hardware, application and bandwidth costs are covered by the provider.
 Scalability to meet needs.
2. No wasted resources because you pay for what you use.
3. The term "public cloud" arose to differentiate between the standard model and the private cloud, which is a proprietary network or data center that uses cloud computing technologies, such as virtualization. A private cloud is managed by the organization it serves. A third model, the hybrid cloud, is maintained by both internal and external providers. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform

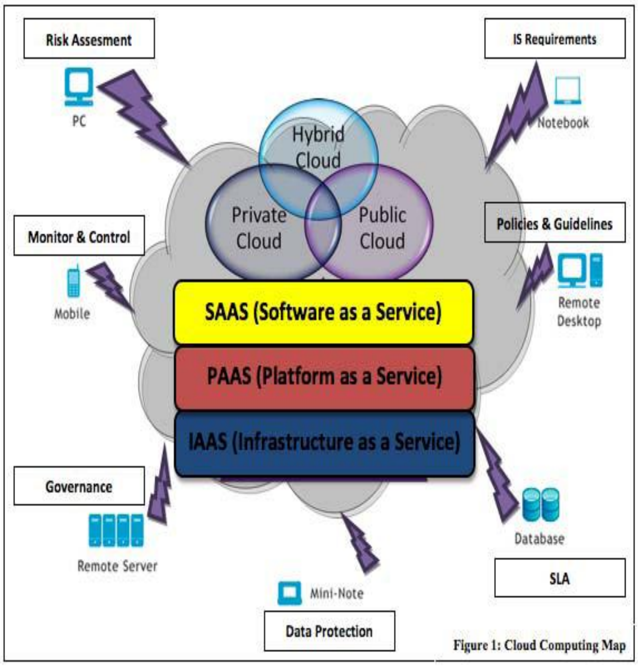


Fig. 2 Cloud Computing Models

B. 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 the needs 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).

C. 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.

D. Private Cloud

A community cloud may be established where several organizations have similar requirements and seek to share infrastructure so as to realize some of the benefits of cloud computing. With the costs spread over fewer users than a public cloud (but more than a single tenant) this option is more expensive but may offer a higher level of privacy, security and/or policy compliance. Examples of community cloud include Google's "Gov Cloud".

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. As such, 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 segments of Cloud Models:

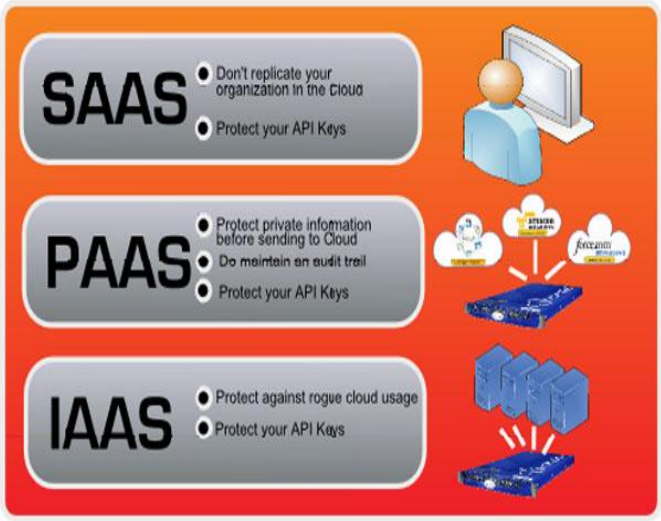

SAAS
Don't replicate your organization in the cloud
Protect your API Keys
PAAS
Protect private information before sending to Cloud
Do maintain an audit trail
Protect your API Keys
IAAS
Protect against rogue cloud usage
Protect your API Keys

Fig. 3 Cloud Computing Models

VI. IAAS COMPONENTS

IaaS delivery model consists of several components that have been developed through past years, nevertheless, employing those 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. SLA encompasses SLA contract definition, SLA negotiation, 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' SLA monitoring until standardizing Cloud Computing systems and delegating third-parties to mediate SLA monitoring and enforcement.

B. Utility Computing

Utility Computing is not new concept; it played an essential role in Grid Computing deployment. It packages the resources (e.g., computation, bandwidth, 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 (e.g., scalability, and pay as- you-go). 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 such 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. WS-Security, a standard 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. In this section, we discuss virtualization risks and vulnerabilities that affect particularly IaaS delivery model in addition to the recent proposed solutions to guarantee security, privacy, and data integrity for IaaS.

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 as shown in Fig.4. SMI model consists of three 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. 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. 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 IaaScomponents and security requirements, and eases security improvement in individual layers to achieve a total secure IaaS system.

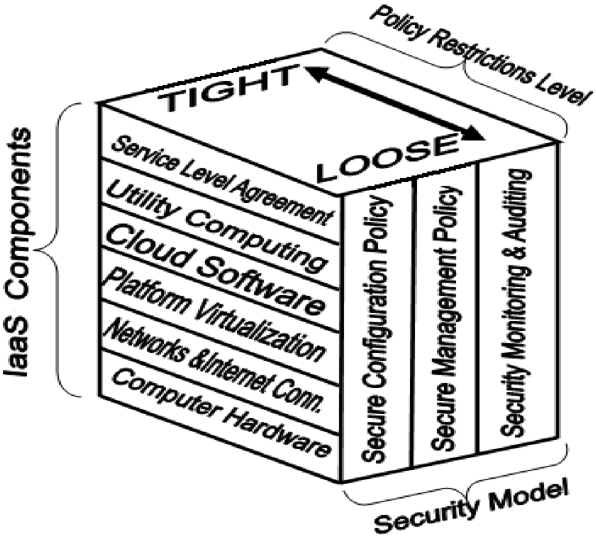
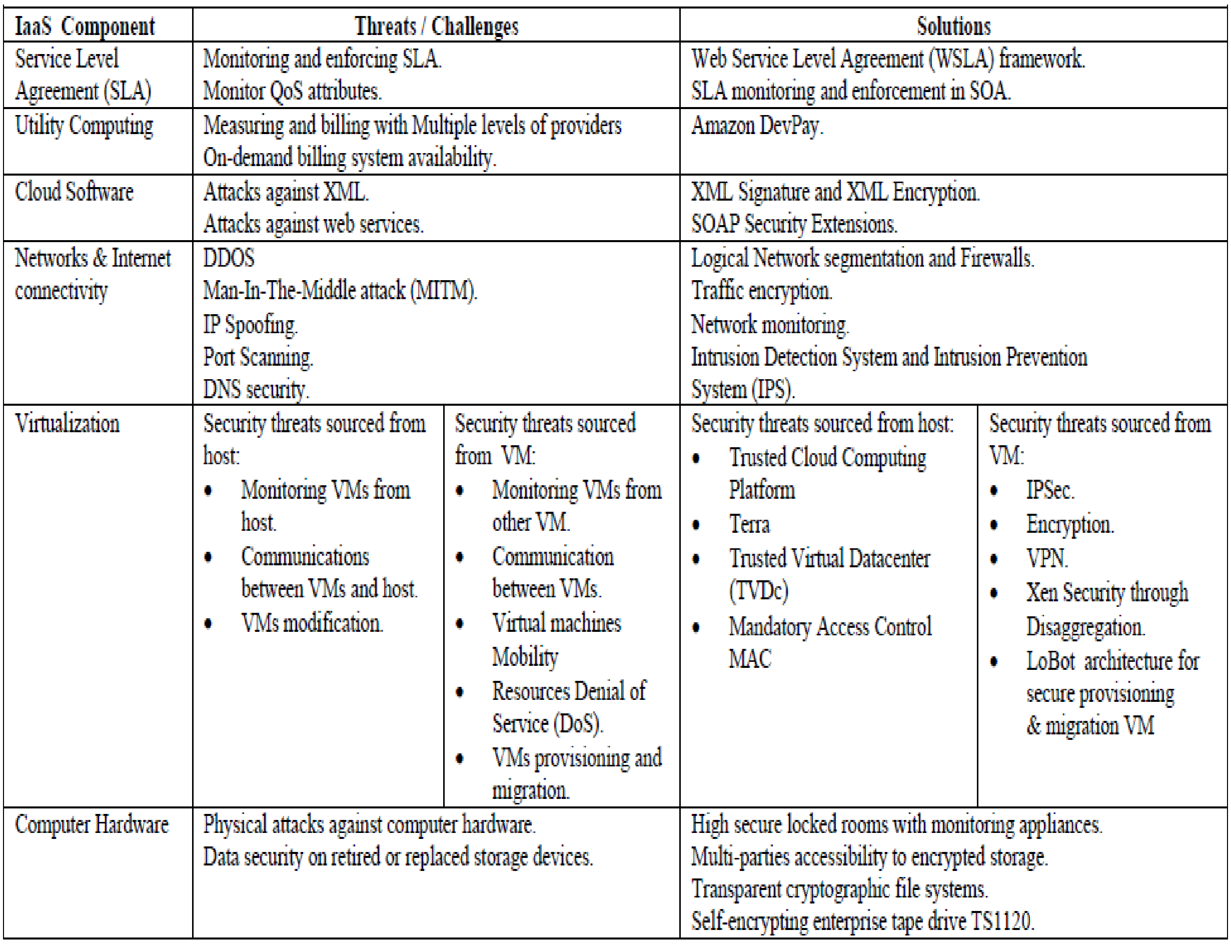


Figure 4. Security Model In IAAS

TABLE I
THREATS AND SOLUTIONS SUMMARY FOR IAAS



IaaS Component	Threats / Challenges		Solutions	
Service Level Agreement (SLA)	Monitoring and enforcing SLA. Monitor QoS attributes.		Web Service Level Agreement (WSLA) framework. SLA monitoring and enforcement in SOA.	
Utility Computing	Measuring and billing with Multiple levels of providers On-demand billing system availability.		Amazon DevPay.	
Cloud Software	Attacks against XML. Attacks against web services.		XML Signature and XML Encryption. SOAP Security Extensions.	
Networks & Internet connectivity	DDOS Man-In-The-Middle attack (MITM). IP Spoofing. Port Scanning. DNS security.		Logical Network segmentation and Firewalls. Traffic encryption. Network monitoring. Intrusion Detection System and Intrusion Prevention System (IPS).	
Virtualization	Security threats sourced from host: • Monitoring VMs from host. • Communications between VMs and host. • VMs modification.	Security threats sourced from VM: • Monitoring VMs from other VM. • Communication between VMs. • Virtual machines Mobility • Resources Denial of Service (DoS). • VMs provisioning and migration.	Security threats sourced from host: • Trusted Cloud Computing Platform • Terra • Trusted Virtual Datacenter (TVDc) • Mandatory Access Control MAC	Security threats sourced from VM: • IPSec. • Encryption. • VPN. • Xen Security through Disaggregation. • LoBot architecture for secure provisioning & migration VM
Computer Hardware	Physical attacks against computer hardware. Data security on retired or replaced storage devices.		High secure locked rooms with monitoring appliances. Multi-parties accessibility to encrypted storage. Transparent cryptographic file systems. Self-encrypting enterprise tape drive TS1120.	

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 as shown in Fig. 4. SMI model consists of three 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. 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 we discuss about Various Layers of Infrastructure as a Service. We can also Provide Security by having a public key infrastructure (PKI) 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 don't really help the customers fulfilling their losses. In this Paper we 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.

ACKNOWLEDGMENT

I am very grateful to Er. Rubal Chaudhry Wadhawan Asstt. Professor, for his support to write this paper.

I am very thankful to Er. Satinder pal Ahuja, the Head of Department of Compuer science in Indo Global College of Engineering, for his motivation and support during the paper.

REFERENCES

[1].M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, *On Technical Security Issues in Cloud Computing*. IEEE, 2009.
[2]. Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, "Cloud Computing", http://www.ibm.com/developerswork/websphere/zones/hip ods/library.html, October 2007, pp. 4-4
[3]G. Frankova, *Service Level Agreements: Web Services and Security*, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 4607.
[4]. "Service Level Agreement and Master Service Agreement", http://www.softlayer.com/sla.html, accessed on April 05, 2009.
[5]. S. Berger, R. Caceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, W. Schildhauer, and D. Srinivasan, "Security for the cloud infrastrcture: trusted virtual data center (TVDc)." [Online]. Available: www.kiskeya.net/ramon/work/pubs/ibmjrd09.pdf
[6]. http://www.cloudsecurity.org, accessed on April 10, 2009.
[7]. "Sampling issues we are addressing", http://cloudsecurityalliance.org/issues.html#15, accessed on April 09, 2009.
[8]. MikeKavis,"Real time transactions in the cloud", http://www.kavistechnology.com/ blog/?p=789, accessed on April 12, 2009.
[9]. "Secure group addresses cloud computing risks", http://www.secpoint.com/security-group-addresses-cloudcomputing-risks.html, April 25, 2009.
[10]. "Service Level Agreement Definition and contents", http://www.service-level-agreement.net, accessed on March 10, 2009.
[11]"Cloud security alliance: Security guidance for critical areas of focus in cloud computing v2.1," Dec 2009. Available at: www.cloudsecurityalliance.org.
[12]. "Wesam Dawoud, Ibrahim Takouna, Christoph Meinel Infrastructure as a Service Security,