Research Journal of Recent Sciences _____ ISSN 2277-2502
Vol. **3(6),** 116-123, June **(2014)** *Res.J.Recent Sci.*

Review Paper

Cloud Computing Safety Concerns in Infrastructure as a Service

Shakir Khan[1] and Mohamed F. AlAjmi[2]
[1]King Saud University, Saudi Arabia, Nationality INDIA
[2]College of Pharmacy, King Saud University, SAUDI ARABIA

Available online at: www.isca.in, www.isca.me
Received 4th December 2013, revised 3rd April 2013, accepted 27th May 2014

Abstract

Cloud computing is current exhortation in the market. It is pattern in which the assets can be leveraged on user basis and by this way reducing the cost and complication of service providers. Cloud computing guarantee to slice operational and capital costs and more prominently let IT departments focus on planned projects instead of maintenance datacenters running. Cloud computing is much more than easy internet. It is a build that permits user to access applications that in reality exist at location rather than user's own computer or other Internet-connected devices. There are many benefits of this build. For example other corporation hosts user application, this means that they need to bear the cost of servers, deal with software updates and depending on the contract and by this way user need to pay less i.e. for the service only. Secrecy, Integrity, Availability, Authenticity, and Privacy are important concerns for both Cloud providers and customers as well. Infrastructure as a Service (IAAS) gives out as the groundwork layer for the other delivery models, and a lack of safety in this layer will definitely change the other delivery models, i.e., PAAS, and SAAS *that are built upon IAAS layer. This paper gives a detailed study of IAAS components' security and finds out vulnerabilities and countermeasures. Service Level Agreement should be considered with very much importance.*

Keywords: Computing, cloud computing security, service level agreement (SLA), infrastructure as a service (SAAS).

Introduction

Mists are extraordinary accumulations of basically practical and accessible virtualized capitals. These capitals might be animatedly improving the settings to rectify a variable weight (equalization), allowing best conceivable asset utilization. It's an installment for genuine assets multiplication in which the Infrastructure Provider is dependable of altered Service Level Agreements (SlAs) infers affirmation regularly upward an accumulation of assets. Business and people can take the profit from aggregation registering and information gathered apparatus focuses, given by enormous organizations with unfaltering and well-constructed cloud presentation transcript. Distributed computing incorporates virtual adaptation of it, at whatever point obliged misuse, Internet arrival of repair and open source programming (OSS). From one perception, distributed computing is not anything novel in light of the fact that it uses advance to thought and best catch up that has as of recently been distinguished. From an alternate viewpoint, the entire thing is new since distributed computing adjusts how we find, grow, compose, offset, reestablish, save, and give for requirements and the foundation under which they administrations run. Distributed computing is information that uses the web and concentrates remote servers to protect information and applications[1]. Distributed computing grants clients and commercial enterprises to use the requisitions with no setting-up on their own PCs and right of passage there any individual document at whatever available PC through the association of web. These provisions of science grant for considerably more capable utilization of workstations by concentrate (control of a movement or association) under a solitary power stockpiling, memory, preparing the information exchange rate.

Distributed computing Services and inspection

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. Open Stack has awesome potential but the pressure is on to attract more partners and further grow the community. It is in the best interest of the cloud community to see this succeed. We need true, open platforms. It's not enough to solely support open APIs. 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. Success Factors uses activity streams as a universal notifier and contact environment for employee productivity. It's a different strategy than Chatter, which uses activity streams to enhance its customer relationship platform. Instead, it's more about establishing a presence for every employee in the enterprise by offering a dashboard view. At the heart of cloud infrastructure is this idea of multi-tenancy and decoupling

between specific hardware resources and applications," explains Data monitor senior analyst Vuk Trifkovic[2]. "In the jungle of multi-tenant data, you need to trust the cloud provider that your information will not be exposed." 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 common place for many business tasks, including computerized billing, invoicing, human resource management, financials, content management, collaboration, document management, and service desk management. Google is achieving something significant with its Google Apps Marketplace. It is serving as an ecosystem for third party SAAS providers. Its success shows in its numbers. It has more than 200 apps and about four million users with access to the service. Salesforce.com is now a platform company. This past week is testament to the role Chatter has played in the development of its strategy. Salesforce.com opened itself to a larger developer community by offering Chatter. It's just a year old but its significance cannot be questioned.

Infrastructure-as-a-Service like Amazon Web Services provides virtual server instances with unique IP addresses and blocks of storage on demand. Services like Sherpa Tools strengthen the platform, Twilio[3] is intriguing. It's an energetic group of people who have embraced telephony in the cloud with more youthful energy compared to most companies we follow. This is a company that has a bounty of case studies for how the platform is applied. We think of it as an idea engine that demonstrates how messaging is becoming a new communications system for people. Messaging can be done through SMS or through apps that trigger information that needs to be presented in a specific context. Twilio[3] also makes money. Its API provides ways for developers to create services that can be charged to the end user. That's a huge market opportunity. Twilio[3] is right there to take advantage of it. SAAS layer is mainly concerned with end users because end users can access and use these applications which were made by cloud providers. Thanks to everyone for their support in the development of Read Write Cloud. Our community has grown quite a bit in the past year. We value your continued interest. We look forward to a new year with more coverage and insights to help you get a picture of the market, its technologies and the trends that are fueling significant innovation. 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. 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. London-based financial transaction specialists Smart Stream Technologies made its foray into the cloud services space last month with a new SAAS product aimed at providing smaller banks and other financial institutions with a cheap means of reconciling transactions. Product manager Darryl Twiggs[4] says that the service has attracted a good deal of interest amongst small to mid-tier banks, but that some top tier players are also being attracted by the potential cost savings.

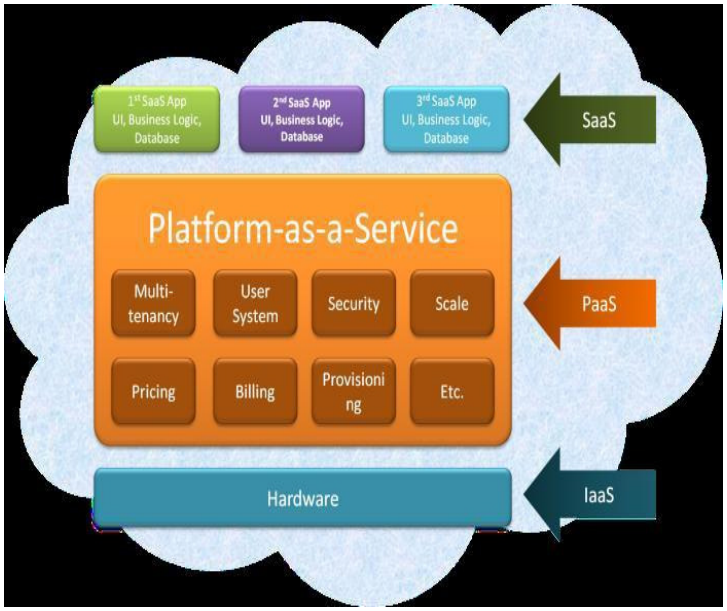

Figure-1
Distributed Computing Services

Distributed computing security concerns

Cloud figuring does not allow shoppers to physically own the stockpiling of the information, leave-taking the information stockpiling and sort out in the hands of cloud suppliers. Because of virtualization, customers of public clouds have growing concerns regarding the clouds security primarily because virtualization has changed the relationship between the hardware and the operating system. Additional concern about the virtualization software, with a tendency to be compromised, makes users wary about the capability of cloud computing to be secured. Furthermore to the prerequisites to which buyers are subject, the server farms saved by cloud suppliers might likewise be liable to satisfaction necessities. Many regulations influence to the stockpiling and utilization of information requirement typical reporting and review trails, cloud suppliers must encourage their customers to watch suitably with these regulations. Overseeing Compliance and Security for Cloud Computing gives close on how a top-down perspective of all IT assets inside a cloud-based area can carry a stronger administration and authorization of satisfaction arrangements. Where the information is more secure i.e. on your nearby hard driver or on high wellbeing servers in the cloud? Some contend that customer information is more secure when managed inside, while others contend that cloud suppliers have a solid inspiration to administer trust and as being what is indicated utilize a larger amount of security.

At the same time as growingly in place of people and organizations are found in the cloud, anxieties are beginning to raise about the wellbeing of the earth implies how protected will it be[5]. Cloud computing securities fall into three general categories: Contractual or Legal Issues, Compliance, and Privacy and Security. For the contractual and legal issues, end users and cloud vendors have to negotiate about liability, end-of-service, and intellectual property. They must agree about the degree of liability of each party when data has been compromised or lost. They must also agree on how the applications and data can be returned to the client when the contract isn't renewed. Cloud providers must also take into consideration how the records are kept because there certain statutes which require electronic records to be kept in a certain way. Public institutions which are utilizing the cloud and storage must consider the laws regarding record keeping. Customers will contend that this is engaging crucial and figure out how to pay for them the office to safeguard their singular reproduction of facts in a manifestation that jam their sway of decision and shield them contrary to certain concerns somewhere else of their sort out in the meantime as liking the radiant paybacks distributed computing can convey. There is a tremendous distinction in the CSP's administration model, once you pick a specific CSP; you may be bolted in, in this way carry a potential business secure danger. Enduring attainability: You ought to be certain that the detail putting into the cloud will no more end up being invalid even your distributed computing supplier broke or get acquired and swallowed up by a greater organization. "Ask potential suppliers how you might acquire your information back and in the event that it might be in an arrangement that you could import into a substitute provision.

Security issues related to cloud computing can either be security issues experienced by end users or security issues experienced by cloud suppliers. In general, cloud providers must make sure that what they're offering is secure and their customers' applications and data are also protected. The client, on the other hand, must ensure that the cloud supplier has the appropriate security implemented in order to protect his data and applications. Right away, organizations hit in terms of professional career and modern action are decreased are more getting cognizant that simply by whipping into the cloud they can build speedy right of section to the most ideal financing decision for a particular part or industry or exchange provisions or fundamentally enhance their foundation i.e. physical assets at the negligible expense. Different from the accepted registering model, distributed computing works the virtual processing innovation, clients' close to home information may be scattered in an assortment of virtual server farm as opposed to stay in the indistinguishable physical area, even over the national outskirts, at this point, information isolation assurance will confront the contention of distinctive legitimate frameworks. Then again, stresses attach with efforts to establish safety and privacy from singular the distance through authoritative levels. Then again, clients may spill out hid data when they entering distributed computing administrations. Ambushers can look at the discriminating assignment relying upon the figuring undertaking introduced by the clients.

Distributed Computing Models

An open cloud is dependent upon the standard distributed computing model in which an administration supplier makes assets, for instance requisitions and capacity, accessible to the regular group over the Internet. Open cloud administrations may be given free or exhibited on a pay-for every utilization model. |Conceivably, the half and half approach permits a business to exploit the versatility and expense viability that an open distributed computing environment offers without uncovering mission-discriminating provisions and information to outsider vulnerabilities. No squandered assets as paid by means of utilization base.

A private cloud is prohibited by the group it serves. A third model, the hybrid cloud is preserved by both internal and external providers. Amazon Elastic Compute Cloud (EC2), Sun Cloud, IBM's Blue Cloud, Google Apps Engine and Windows Azure Services Platform are the examples of public clouds[6,7,8]. Promoting media that uses the words "private cloud" is intended to request to an association that needs or needs more control over their information than they can get by utilizing an outsider facilitated administration, for example, Amazon's Elastic Compute Cloud (EC2) or Simple Storage Service (S3). The term "open cloud" jumped out at recognizes the standard model and

the private cloud, which is an exclusive system or server farm that uses cloud computing technologies like virtualization. Easy and efficient set-up since equipment, requisition and transfer speed liabilities are secured by the administration supplier, versatility to help.

Advances in virtualization and scattered registering have allowed corporate system and datacenter directors to effectively get to be administration suppliers that meet the goals of their "clients" inside the business. A mixture cloud is a Cloud Computing environment in which an association gives and deals with a few assets in-house and has others given remotely. Case in point, an association may utilize an open cloud administration, for example, Amazon Simple Storage Service (Amazon S3) for filed information however keep on maintaining in-house stockpiling for operational client information. Private cloud (likewise called inner cloud or corporate cloud) is an advancement term for a restrictive registering structural planning that gives facilitated administrations to a predetermined number of individuals after a firewall. A group cloud may be created where numerous associations have parallel necessities and search for, to impart base in order to understand a percentage of the profits of distributed computing. With the expenses spread over fewer clients than an open cloud (yet more than a solitary occupant) this alternative is more exorbitant however may offer a special phase of isolation, wellbeing or arrangement recognition. Occurrences of gathering of individuals cloud incorporate Google's "Gov Cloud".

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[7].

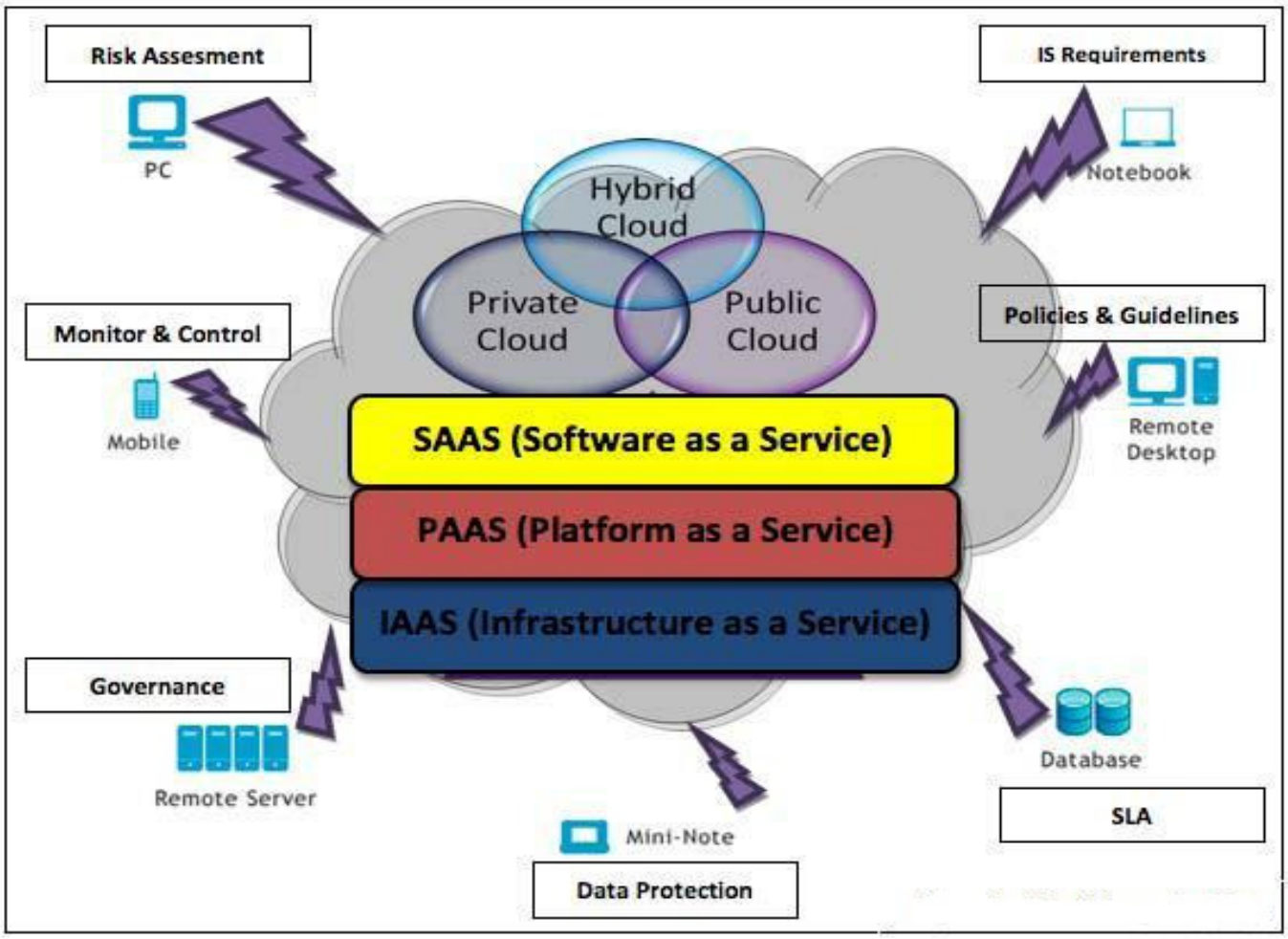

Figure-2
Cloud Computing Models

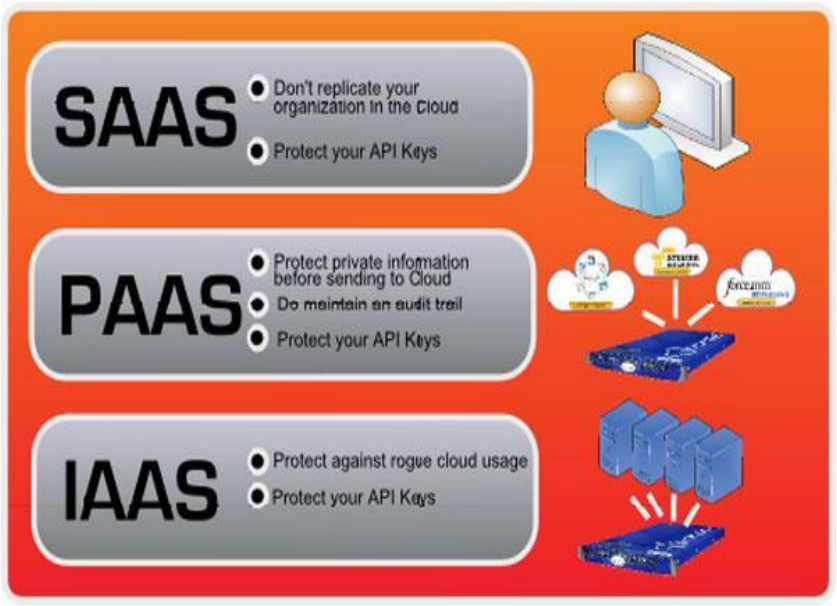

Figure-3
Cloud Computing Models

IAAS Components

Rupturing the security of any segment affect alternate parts' security, therefore, the security of the whole framework will crumple. In this segment we concentrate on the security issue of every part and examine the proposed results and suggestions. Cleanser is the most upheld convention in web benefits; numerous SOAP based security results are scrutinized, created, and executed. WS-Security, a standard enlargement for security in SOAP, addresses the security for web administrations. IAAS conveyance model comprises of some segments that have been produced through past years; in any case, utilizing those parts together in an imparted and outsourced environment conveys numerous tests. Security and Privacy are the most critical tests that may block the Cloud Computing selection. Utility Computing is not new idea; it assumed a fundamental part in Grid Computing sending. It bundles the assets (e.g., calculation, data transfer capacity, stockpiling, etc...) as metered administrations and conveys them to the customer. At last, a great situation in indicated the likelihood of breaking the security between the program and the mists, accompanied by proposal to improve the present programs security. Undoubtedly, these strike have a place more to the web administrations world, however as an innovation utilized within Cloud Computing, web administrations' security firmly impacts the Cloud administrations' security[9]

The force of this model lies in two primary focuses: First, it lessens the aggregate expense, i.e., as opposed to owning the assets, customer can pay for use time (pay-as-you-go). Second, it has been created to backing the adaptable frameworks, i.e., as a manager for a quick developing framework you require not to stress over denying your administration as per a fast build of clients or arriving at top popular. Possibly Cloud programming is open source or business shut source. We can't guarantee the defenselessness and bugs in accessible programming, moreover, cloud administration suppliers outfit APIs (REST, SOAP, or HTTP with Xml/JSON) to perform most administration capacities, for example, access control from a remote area. Web Service Level Agreement (WSLA) system created for SLA checking and authorization in SOA. Utilizing WSLA for overseeing SLA within Cloud Computing environment was proposed in by designating SLA observing and authorization undertakings to an outsider to tackle the trust issue. Presently, cloud customers need to trust suppliers' SLA screening until institutionalizing Cloud Computing frameworks and appointing outsiders to intercede SLA overseeing and authorization. There are numerous open source Cloud programming executions, for example, Eucalyptus and Nimbus[6]. Cloud programming joins the cloud parts together. It characterizes a SOAP header (Security) that conveys the WS-Security amplifications and figures out how the existing XML security principles like XML Signature and XML Encryption are connected to SOAP messages. Well known strike on conventions utilizing XML Signature for validation or respectability assurance might be connected to web benefits subsequently influencing the Cloud administrations.

The second test is that Utility Computing frameworks might be magnetic focuses for assailants, so an ambusher may intend to gain access to administrations without paying, or can head off further to drive particular organization bill to unmanageable levels. The supplier is the primary dependable to keep the framework sound and well working, yet the customer's practice additionally influences the framework. Then again, following and authorizing SLA stage is essential to assemble the trust between the supplier and the customer. To implement SLA in a dynamic environment such Cloud, it is important to screen QOS

traits ceaselessly. Distributed computing rises a set of IT administration complexities, and utilizing SLA within cloud is the answer for insurance worthy level of QOS. SLA includes SLA contract definition, SLA arrangement, SLA screening, and SLA authorization. SLA contract definition and arrangement stage is paramount to focus the profits and obligations of each one gathering; any false impression will influence the frameworks security and leave the customer presentation to vulnerabilities. Clearly, Utility Computing shapes two of the primary characteristics of the Cloud Computing (e.g., adaptability, and pay as- you-go). The principal test to the Utility Computing is the unpredictability of the Cloud Computing, for instance, the higher supplier as Amazon must offer its administrations as metered administrations. Those administrations could be utilized by second level suppliers who likewise give metered administrations. In such various layers of utility, the frameworks get to be more perplexing and require more administration exertion from both the higher and the second level suppliers. Amazon Devpay[5], a sample for such frameworks, permits the second level supplier to meter the use of AWS administrations and charge the clients consistent with the costs dictated by the client. For instance, customer can utilize the Amazon EC2 tool stash, a broadly upheld interface, to expend the administrations by executing own requisitions or by basically utilizing the web interfaces offered by the supplier. In both cases, client utilization web administrations conventions.

Stage Virtualization: Virtualization, an essential apparatus stage for Cloud Computing administrations, makes conceivable with a gathering of numerous distinctive frameworks into specific equipment arrange by doing virtualization of the processing game plans of stocks (e.g., set of associations, Cpus, memory, and capacity). Equipment thought hides the inconvenience of administering the physical registering stage and streamlines the processing stocks the nature of being versatile. Subsequently, virtualization makes accessible multi lease and adaptability, and these are two paramount character of Cloud Computing as the hypervisor is responsible for Vms isolation; Vms couldn't be smart to honestly right to utilize others' virtual plates, memory, or provisions on the indistinguishable facilitating. Iaas, a nature's turf, requests an exact arrangement to hold well-fabricated isolation. Cloud administration suppliers do a noteworthy exertion to spare their frameworks keeping in mind the end goal to lessen the terrorization that outcome from message, watching, change, movement, portability, and DOS. In this fragment, we discuss virtualization dangers and vulnerabilities that concern mostly Iaas discharge fake up notwithstanding the present anticipated route outs to confirmation security, isolation, and information dependability for Iaas[10].

Safety model for IAAS

As a consequence of this explore, we also talk about a Safety Model for IAAS (SMI) as a conduct for evaluate and ornamental safety in each level of IAAS liberation representation. SMI model made up of three surfaces: IAAS components, safety model, and the control level. The front surface of the cubic representation is the mechanism of IAAS which were talked about systematically in the preceding sections. The safety model side consists of three vertical entities where each entity plasters the complete IAAS mechanism[11-12].

The first thing is Secure Configuration Policy (SCP) to assurance a secure arrangement for each coating in IaaS Hardware, Software, or SLA configurations; generally, miss-configuration occurrence could put at risk the complete safety of the system.

Secure Resources Management Policy (SRMP) that deals with the association position and rights. The closure substance is the Safety Policy Monitoring and Auditing (SPMA) which is respectable to take after the framework life cycle. The imperative arrangement side shows the phase of requirement for security model elements.

Confinement starts from detached fitting to tight relying upon the supplier, the purchaser, and the administration necessities. Yet, we need SMI model be a great quality launch for the consistency of IAAS layers. This representation brings up the following of kinfolk between IAAS parts and security necessities, and moves wellbeing improvement in character layers to achieve an aggregate safe IAAS framework.

As an outcome of this research, we recommend a Safety Model for IAAS (SMI) as a channel for assessing and fancy security in each one covering of IAAS liberation model. SMI model made up of three sides: IAAS parts, wellbeing model, and the limitation level. The face side of the cubic representation is the segments of IAAS which were discussed completely in the past areas. The wellbeing model side comprises of three perpendicular substances where each substance wraps the complete IAAS instrument. The essential element is Safe Configuration Policy (SCP) to affirmation a protected plan for all layers in IAAS Hardware, Software, or SLA designs; by and large, miss-setup event could put at hazard the complete security of the framework. The second is a protected Resources Management Policy (SRMP) that steers the organization positions and rights. The last substance is the Safety Policy Monitoring and Auditing (SPMA) which is significant to accompany the framework life cycle. The obligation strategy side shows the phase of confinement for security representation substances. The phase of imperative starts from detached fitting to extend hinging upon the supplier, the purchaser, and the administration necessities. In any case, we want SMI representation be a great quality set up for the consistency of IAAS layers. This representation calls attention to the following of family between Iaas parts and security necessities, and maneuvers wellbeing upgrade in character layers to achieve an aggregate secure IAAS system[13].

Table-1
Threat and solution review for IAAS

Iaas elements	intimidation / Challenges	Solutions
Service Level Agreement (SLA)	Checking and upholding SLA. Screen Qos traits	Web Service Level Agreement(wsla) schema SLA overseeing and implementation in SOA
Utility Computing	Measuring and charging with Multiple levels of suppliers On-interest charging System accessibility.	Amazon DevPay.
Cloud Software	Ambushes against XML Ambushes against web administrations.	XML Signature and XML Encryption Cleanser Security Extensions.
Networks and Internet Connectivity	DDOS Man-In-The-Middle attack (MIMT). IP Spoofing Port Scanning DNS security	Intelligent Network division and Firewalls. Movement encryption System following Interruption Detection System and Intrusion Prevention System(ips)
Workstation Hardware	Physical ambushes against machine equipment. Information security on resigned or supplanted stockpiling mechanisms	High secure bolted rooms with following apparatuses Multi-parties receptiveness to scramble stockpiling. Transparent cryptographic index frameworks. Self scrambling venture tape drive Ts1120
Virtualization	Security threats sourced from host: Monitoring VMs from host Communication between host and VMs VMs modification	Security threats sourced from VM: Monitoring VM from other VM. Communication between other VMs. Virtual machine 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: IP Sec Encryption VPN XEN security through disaggregation LotBot architecture for secure provisioning and migration VM

Conclusion

In this paper we discuss a mixture of Layers of interchanges as an administration. We additionally offer security stages to Provide Safety by containing an open key foundation (PKI) at each covering that we discussed in this paper. The SLA's discuss just with respect to the administrations offered and the waivers given, if the given administrations couldn't meet the agreement of understanding, this waivers don't really help the customers fulfilling their misfortunes. In this Paper we additionally speak the Security breaks interfaced with IAAS acknowledgment. The security issues open here concern the wellbeing of every IAAS component notwithstanding cutting edge anticipated results.

Acknowledgment

We acknowledge the support from Research Center, College of Pharmacy, King Saud University (KSA).

References

1. Jensen M., Schwenk J., Gruschka N. and Lo Iacono L., On Technical Security Issues in Cloud Computing, *IEEE*, **(2009)**

2. http://www.computerweekly.com/news/2240089111/Top-five-cloud-computing-security-issues

3. http://www.twilio.com/ **(2013)**

4. http://www.terremark.com/services/it-infrastructure/cloud-services/enterprise-cloud/ **(2013)**

5. Berger S., Caceres R., Pendarakis D., Sailer R., Valdez E., Perez R., Schildhauer W. and Srinivasan D., Security for the cloud infrastrcture: trusted virtual data center (TVDc), **53**(4), 6 **(2009)** [Online]. Available: www.kiskeya.net/ramon/work/pubs/ibmjrd09.pdf

6. http://www.cloudsecurity.org, accessed on April 10, **(2009)**

7. Al Ajmi, Sharma and Khan S., Growing Cloud Computing Efficiency, **3**(5), **(2012)** available on http://thesai.org/Publications/ViewPaper?Volume=3&Issue=5&Code=IJACSA&SerialNo=26

8. Wesam Dawoud, Ibrahim Takouna, Christoph Meinel Infrastructure as a Service Security, **(2013)**

9. Service Level Agreement Definition and contents, http://www.service-level-agreement.net, accessed on March 10, **(2009)**

10. Sampling issues we are addressing, http://cloudsecurityalliance.org/issues.html#15, accessed on April 09, **(2009)**

11. Mike Kavis, Real time transactions in the cloud, http://www.kavistechnology.com/ blog/?p=789, accessed on April 12, **(2009)**

12. Secure group addresses cloud computing risks, http://www.secpoint.com/security-group-addresses-cloudcomputing-risks.html, April 25, **(2009)**

13. Cloud security alliance: Security guidance for critical areas of focus in cloud computing V2.1, Dec **(2009)** Available at: www.cloudsecurityalliance.org.

14. Kamran Ahsan, Nazish Nouman, Anum Kamran, Farhana Hussain, and Saboohi Naeem Ahmed Cloud-Based Shared Food Ordering System with Context Awareness: A Location Base Services Approach, **2(11),** 84-89, November **(2013)** http://www.isca.in/rjrs/archive/v2/i11/12.ISCA-RJRS-2013-046.pdf

15. Kamran Ahsan, Nazish Nouman, Anum Kamran, Farhana Hussain and Saboohi Naeem Ahmed, Cloud-Based Shared Food Ordering System with Context Awareness:A Location Base Services Approach, *Research Journal of Recent Sciences,* **2(11),** 84-89, **(2013)**

16. Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, Cloud Computing, http://www.ibm.com/ developerswork/ websphere/ zones/hip ods/library.html, 4-4 **(2007)**

17. Frankova G., Service Level Agreements: Web Services and Security, ser. Lecture Notes in Computer Science, Berlin, Heidelberg: Springer Berlin Heidelberg, **4607, (2007)**

18. Service Level Agreement and Master Service Agreement, http://www.softlayer.com/sla.html, accessed on April 05, **(2009)**