RESEARCH ARTICLE OPEN ACCESS

Security in Cloud Computing For Service Delivery Models: Challenges and Solutions

Preeti Barrow[#1], Runni Kumari[#2], Prof. Manjula R[#3]
Scope, VIT University, Vellore, India-63201

ABSTRACT
Cloud computing, undoubtedly, is a path to expand the limits or add powerful capabilities on-demand with almost no investment in new framework, training new staff, or authorizing new software. Though today everyone is talking about cloud but, organizations are still in dilemma whether it's safe to deploy their business on cloud. The reason behind it; is nothing but Security. No cloud service provider provides 100% security assurance to its customers and therefore, businesses are hesitant to accept cloud and the vast benefits that come along with it. The absence of proper security controls delimits the benefits of cloud. In this paper, a review on different cloud service models and a survey of the different security challenges and issues while providing services in cloud is presented .The paper focuses on the security issues specific to service delivery model (SaaS, IaaS and PaaS) of cloud environment. This paper also explores the various security solutions currently being applied to protect cloud from various kinds of intruders.

***Keywords*-** Cloud computing, security, Service delivery models, Security solutions.

I. INTRODUCTION

Cloud Computing has replaced the traditional client-server hierarchical driven model with more scalable, on demand, well-organized and flexible data driven model. NIST provides a comprehensive definition of cloud computing as, "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. Today, almost all companies whether big or small are realizing that by using cloud services they can quickly access business applications or immensely increase their computing resources, all at imperceptible cost. Although, the technology supporting cloud computing is evolutionary, it is revolutionary by providing long –standing features like pay as-you-go, resource pooling, and provincially available system. Deployment of cloud computing extended the issues of transaction control, latency and in particular security over the traditional model.

Successful implementation of cloud computing include improving profitability and taking right security measures. Several pricing models are available which needs to be defined under two different classes of cloud computing as deployment model and service model. When an enterprise deploys a cloud based on the location, purpose, trait, applications and business demands of an organization, it is deployment model. Community, hybrid, public and private are the principal cloud deployment models. Whereas, if it seems to service providers subscribing Service as software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS) is called service model (also called SPI model).

Cloud as a service is been populated by many of the costumers and enterprises as it decreases its cost and increase the service provider's revenue. It is always a good option to choose cloud as service rather than the deployment model. Service model is more compatible with user's behavior and static pricing approach than dynamic one because a static approach would charge less. However, this model triggers the provocations for the service provider and security risks. In this survey, key concept has been reviewed of service model which include concerns in security risk, vulnerabilities, threats and possible curative measures for an enterprise. Also, the guidance for the user end has been instigated which can be verified and analyzed taking security as a parameter.

In this paper we shall be discussing about various securities challenges that come when a user moves to cloud environment. Understanding the security dangers and counter measures will help associations to complete the cost saving analysis and will encourage them to move to cloud. This paper gives security models and essential policies for securing cloud computing environment. The paper is divided into four sections: first section describes the three cloud service models, SaaS,

IaaS, PaaS and how the interdependency of the models affect the movement of risks from one service layer to the other. Second section deals with deep analysis of the various security challenges and concerns associated with each of these layers. Problems in maintaining data integrity, information confidentiality and availability due to multi-tenant and resource sharing feature of cloud makes it difficult for cloud users to impose their full trust on cloud resulting in many organizations still pondering over whether they should move their business to cloud or not. In section three, we explore various security mechanisms available for each service model, supported by a comparative table distinguishing some cloud providers on the basis of utilization of security measures. The last section presents some conclusions of our survey research.

II. RELATED WORK

Security issues in the region of cloud computing is dynamic area of examination. Merino, Luis noted the various risks associated with PaaS service model due to the multitenancy in software platforms. He provides a survey on the security risks, security mechanisms and limitations of two platforms: Java and .NET. They have also briefly describe about Operating Systems classical security capacities and why OSs are not likely to be picked as the premise of PaaS offers [5].Karadsheh, Louay explores the role of security policies and service level agreement (SLA) to increase the security in IaaS service model [9]. Sengupta, Nandita has given a new approach to handle the security issues in cloud-hybrid DESCAST algorithm. The proposed algorithm is a combination of DES and CAST algorithm to encrypt the data while sending through network and also the data shall remain in encrypted form while it is at rest at the cloud server. By combining 128 bit and 64 bit key algorithms it has been proved that DESCAST algorithm can provide security from brute-force attack and attacks via birthday problems. Also the algorithm is more robust compared to other encryption algorithms [16]. The author in [3] has given a survey on security issues that comes due to very nature of cloud computing. The paper also talks about issues in MCC and provides a literature review of the existing solutions for the same.

III. MOTIVATION

Cloud brings engaging benefits including alleviation of the load for capacity administration, all-inclusive information access with different geographical areas, evasion of capital consumption on programming, equipment, and work force systems for up keeps, and so forth. In any case, there are obstructions that impede relocation to the cloud. One of the primary boundaries is that, due to absence of substantial control over the deployed information, a cloud client might stress over whether her information are kept safe and the integrity of the data is maintained. Furthermore, in the event that the cloud client is an organization, aside from the danger of remote noxious assaults on the cloud, the customary concerns postured by pernicious organization insiders are presently supplemented by the significantly more risky danger of malignant outcasts who are given the force of insiders. Therefore, persuading cloud clients that their information are in place is particularly crucial when clients are organizations. Cloud computing security is not anymore paper-based analysis of its vulnerabilities. The deployed technology has some limitations which needs to be filled in a customized manner. Here customized means, the ideal cloud computing security environment for usage as per the customer or enterprise. Hence, it becomes very essential for the clients to be aware of the various security issues associated with cloud and at the same time the cloud providers must know the best security control measures that they can provide to their customers. The authors in the current study represent the problems and solution according to the particular destitute cloud computing security environment for SPI model.

IV. CLOUD COMPUTING SERVICE MODELS

Cloud Computing Service models can be categorized into three major types, namely Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

4.1. Saas

Software as a Service model focuses on providing business operations over a network as a service. It helps in reducing the effort of installation and maintenance of complex software, as one can essentially get it from the Internet. Furthermore, it liberates the user from intricate programming and equipment management. SaaS applications can be termed as web-based or hosted-software. No matter what the name of the service is, they require Cloud Service Provider's (CSP) servers to be executed. The wholesome responsibility for software that is availability, security, execution lies on the CSP.A very basic example of SaaS can be Google Apps, Salesforce, and Citrix GoToMeeting etc. Currently the organizations are creating SaaS integration platforms (SIPs) for making more applications of SaaS. The counseling firm Saugatuck Technology calls this the "third wave" in programming

adoption: when SaaS moves past standalone programming usefulness to end up a stage for mission-critical applications.

4.2. Paas

Platform as a Service model focuses on providing platform and environment to the customers for creating services and applications using Internet. In the hierarchy architecture of service delivery model PaaS takes the middle layer, with SaaS layer above and IaaS layer below. The customers can ask for customized platform from the providers according to their requirements and pay-as-per the usage. Google App Engine is a well renowned working example for PaaS. The security issues due to multi-tenancy and data sharing has to be taken care by both the provider as well as the cloud user.

4.3. Iaas

Infrastructure as a Service model aims at providing virtual infrastructure for instance servers, network, RAM etc. as a service to the cloud buyers. The buyers pay only for the resources they utilize to the cloud service providers. The provider is responsible only for the hardware maintenance to ensure that the servers run correctly while the responsibility of security lies in hands of the customer. Some of the real time providers are Amazon Web Services, Qwest, and Cisco Metapod etc.

The above mentioned three categories: SaaS, PaaS and IaaS form the basis of service model in cloud computing. These service models provide an immense number of facilities to the cloud users but at the same time there are risks and security concerns associated with each of them. In this paper we shall be focusing on the security issues and solutions pertaining to each model. Also, the analysis showed that the security issues of one model can cause problem to the other model due to inter-dependency of the models.

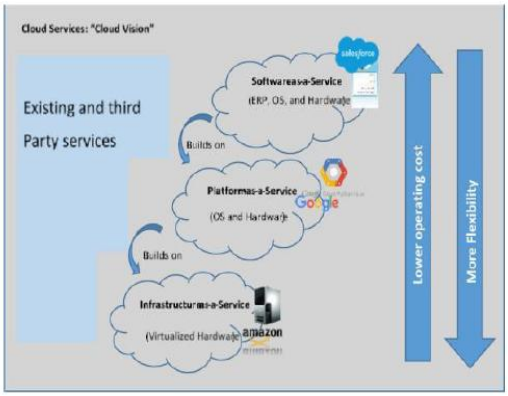


Fig.1. Inter-dependency of cloud service models

Figure.1 illustrates the dependency of the three service models. The SaaS applications are built and deployed over the PaaS and the PaaS is dependent on the underlying IaaS [2].This functional dependency of the service models on each other adds the dependency in security too. For instance, if an intruder succeeds to get hold of IaaS, the result will be a security breach prone PaaS that is making use of IaaS. A compromised PaaS can lead to unsafe SaaS. In all, if an attacker succeeds in gaining access to any service model then getting access to other layers of the service model is child's play for him.

V. CLOUD COMPUTING CHALLENGES AND ISSUES

Cloud computing deals with open widespread systems that are connected by diverse networks and hence results in high concerns for security. Confidentiality, integrity and authentication are the major challenges of cloud computing. Organizations willing to move their data to cloud from traditional storage area have great fear about the security in cloud. Customers must have a clear understanding of all the risks and potential security challenges that may arrive while moving to cloud computing. Moving to public cloud computing involves the transfer of responsibility as well as control to the cloud service provider on data and system components. The transition from traditional to cloud environment brings with it loss of direct management of transactions and also loss of power over decisions to be made in regards of the computing environment. The CSP(s) need to maintain the protocol of confidentiality and integrity to ensure safe and secure transmission of data through Internet. The provider(s) has to provide best security measures to gain the trust of the customers. At the same time customers have equal responsibility towards security of their cloud usage. In order to do so the consumers ensure that the contract with the provider and its joined Service Level Agreement (SLA) has suitable provisions for protection and isolation of data and systems.

Cloud computing take advantage of three service models through which various kinds of services are provided to the customers. The three delivery models are namely-SaaS, PaaS and IaaS which contribute infrastructure reserves, platform to execute applications and software services to the end users. These models have different risks and security challenges associated with them. IaaS forms the base for any cloud service, with PaaS being above it and SaaS being above PaaS. Due to the hierarchical build-up, the information security challenges are inherited from the bottom layer to the top layer. Each of these layers has their own

associated security challenges and various security measures are available to cater each of those issues. With new providers and offerings available all the time, cloud computing depicts a very dynamic field at the current time. There are number of security risks associated with cloud which should be addressed on priority. Although the risks mentioned in [3] need to be mitigated, the use of cloud computing brings forth opportunities for discovering new security solutions that may result in overall security growth of many organizations. The CSP must be able to provide latest security solutions relating to privacy, integrity and confidentiality of data to the consumers. Below we put forth the key issues and the challenges to be taken care so that the cloud security system can be brought in compliance with at least the current IT systems.

5.1. Saas Security Challenges

Undoubtedly, cloud is considered as the greatest rebellion in IT industry but without security it is a disruptive trend. ShopCart is one good example of SaaS Company which has "pricing page" of two thousand four hundred and ninety nine (in rupees) per month. SaaS is an application by a provider whose responsibility is to host all the data of client at the server and make it approachable for the clients across the world via internet. All the functionality and data are not installed locally rather delivered from the server for user experience. There are times when the idea of keeping data at the server can make clients feel unwilling to use cloud computing SaaS. Therefore, CSP should propose a suit of SaaS which include various security measures. A traditional model in which core security services are already available is also a concern of CSP. Sustainable traditional security issues affecting the SaaS model too are security of virtual machine, data confidentiality, authorization and authentication, data integrity and availability. However, in SaaS model the user lack the overlook of the data in the way it is stored and accessed, it becomes easy for the intruder to trespass without acknowledgment. Addressing the kind of security measures taken into consideration by the user makes the CSP more genuine and wide – spread.

Due to the least user extensibility (openness) it offers the CSP to deliver integrated functionality makes it more responsible and customer to pay them. The following key components of SaaS in cloud security which is different from traditional security and challenges:

5.1.1. Information Security

The top priority of security in to secure the information of the costumer. The reliability on the cloud is in the form of information which is managed by the CSP that is out of the frontier of the consumer so, as the CSP has to add some additional feature to protect the information from intrusion. The data can be the type of logs of client action, openness or the information. Security vulnerabilities can lead to breaching of data. Although the treats could be internal or external. Encryption mechanism prevents information from external threat whereas, to prevent the internal threat the vendor has to provide administration which does not allow to access costumer instances. The cryptography is done to prevent threats like snooping, denial of service, modification, repudiation and masquerading majorly data at rest.

5.1.2. Network Security

Establishment of connection between the vendor and customer is equal to establishment of identity over the network. The parameter for authentication of registered customer is passed over the internet which has to be secured from various attacks such as IP spoofing, MITM (man in the middle) attacks, packet sniffing, port scanning, etc. The sensitive information over the network required to be secured. Further, tests are performed to detect any vulnerability which has to be less loaded over the network. The assessment involve configuration of insure SSL trust, management of session weaknesses, penetration of network and analysis of packet.

5.1.3. Resource Locality

Without the knowledge of the locality of data it becomes more difficult to rely on the CSP. The migration of data to different location having different law however to utilize the use of resources. If the data and the resources are not encapsulated it may face an issue of
E-discovery where the CSP's hardware is snatched for inspection. When the inspection falls there is an ambiguity that what is the jurisdiction of the data is an add-on to SaaS security challenges.

5.1.4. Cloud Standards

Efforts are afoot to develop an interoperability standards that post with any cloud type. It may happen that the standards may be adopted by some of the CSP and but some are restricted to its own standards called "sticky services", this does not imply that the some other standard is superior nor, it is worse than another. If a particular standard is not followed then it becomes inconvenient for the users to migrate from one cloud provider to another. To increase the usage of cloud computing an "Intra-cloud standard" needs to be implied which will be the result of discussion among all cloud service

provider. The following are discipline which are required to increase free data movements and cloud interoperability among cloud:

- Quality of service
- Provisioning of resources
- Formatting old data
- Architecture of network
- Billing
- Privacy, security and authentication

5.1.5. Data Segregation

Data segregation is the challenge which comes under tenancy and storage location. Each CSP has to negotiate with the customer on how the data will be stored. Data stored in cloud is for multi-tenant user, thus the challenge is that each customer data is segregated in a unique routine as per the service provider. Two aspects for data segregation in cloud: tenancy and geolocation. The customer should have the full acknowledgment of the routine and make it as a predefined parameter in SLA. The segregation of data is unsuccessful when the application executes the masked code injected by the trespasser in it. Affirmation of application code is required before executing to prevent high probability of intruder to access other's data. The service should facilitate to identify malicious user and the vulnerability to bypass fragile data of other tenant and cybersecurity checks.

5.1.6. Data Access

Suppose a small cloud service provider merge with another service provider (B2B) for providing service. While accessing data from one provider to another the security mechanism has to be applied from both sides to maintain the integrity of data. There are number of challenges as follows:

- Audit data
- Maintain integrity
- Detect unauthorized access

Sort out data of particular provider

5.1.7. Security of Web Application

Web application is among the top five application used in the area of cloud computing. The edge that the web application provides to cloud service is: Price, Reliability, Simplicity, Flexibility and Reliability. These features are difficult to deploy and may demand for initial investment. Moreover, in traditional security system Intruder prevention and intruder detection system (IPS and IDS) uses the firewall which does not appropriately detect the problem may be because it does not create much loop holes in the security mechanism. SQL injection make the web application prone to attack. To stretch the security of the web service application the CSP has to include security mechanism in which it can satisfy all the advantages.

- Injection
- Session management and broken authentication
- Scripting of cross-sit (XSS)
- Leak fragile data
- Misconfiguration of security
- Missing of access control at function level
- Auditing of user's account
- Usage of known vulnerabilities components
- Void forwards and redirects

Verizon Business in their "Verizon Business 2015 Data Breach Investigation report" shows nearly two-thirds of Web App Attacks. Almost all attacks in this data set (98%) was opportunistic in nature, all aimed at easy impressions. Public entities, Information and Financial Services, dominate the victim demographics, but only a few industries fully escaped the attention ofthese criminal empires [4]

.

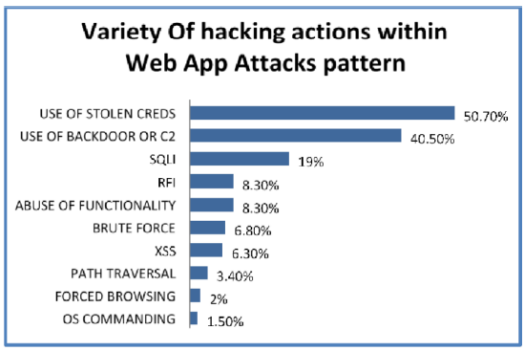


Fig. 2. Frequency of various Web Attacks

5.1.8. Back-up Security

Backup is the most important area of cloud computing whose role is realized during loss of data. "Backing up" implies duplicating of the essential data. Provoking the backup of data is infrequent thus, if any of the backup is violated due to lack in security mechanism it would be difficult to be acknowledged. The service provider may also behave deceitfully by not informing the users of the corrupted or injected backup. In a long run there is no security mechanism introduced so as to encrypt backup and provide authentication to access backup from the vendor side.

5.1.9. Sign-on Process and Identity Management

ID management (IdM) deals with the identification of the user to control the access on the resources by limiting the privileges. SaaS service is still raw in terms of identity management. It has some standards for identity management as:

- Extensible Resources Descriptor Sequence (XRDS)

- Services proving attribute
- Extensible Resource Descriptor Sequence (XRDS)

The challenge is to manage under the standard. The sing-on process which let users to choose the level of their authenticity. For example, the CSP may have many application available and to serve the application and access the provider has to identify the eligibility of the user and up to which level. If the user is exhausted which the service then he/she may not be able to access until and unless it is renewed.

5.2. PaaS Security Challenges

Platform as a Service or PaaS is the one of the service delivery model that provides a complete development environment to the consumer to build and run their applications. Thus, with the help of cloud the customer can start developing applications that can be set out worldwide without any obstructions instead of building a server setting to execute an application and installing a development environment for creating applications on that server. A PaaS cloud allows different users to execute their components on the same platform. This multi-tenancy feature of cloud gives open ways to malicious users to interfere with the other user's components and harm the integrity of the system. The authors of [5] stressed that the cloud service providers are responsible for providing isolation to components so that no user gains the right of tampering the other user's software. Unique security difficulties of the focused architecture are produced primarily by the distribution of the consumer objects over the proprietor of the cloud. Allowing strict access of objects to the shared resources and protecting the objects from malicious or fraudulent providers significantly reduce the likely risks. Shared network access and utility validation raise concerns for secure access control and communications. Besides, the above mentioned issues, user privacy need to secured in a shared cloud. Therefore, the solutions discussed later in the paper must talk about privacy preserving issues. Another major concern for various organizations that uses cloud for their business is of service continuity. For continuous service of business there is need of fault-tolerant well-built systems.

Some of the major problems caused by the resource pooling and fast adaptability characteristics of cloud in PaaS service model are discussed below:

5.2.1. Interoperability of Heterogeneous Resources

In cloud different types of hardware and software resources are clubbed together to provide better cloud services. Varying reckoning resources may result to security breaches if users' access to the resources cannot be taken care properly. This may result a bunch of resources to stop or a certain setting that was confirmed to be secure for a particular resource may turn out to be a reason for security violation for another. An example of it can be a scenario where an individual who is authorized to edit a file named "capture" can acquire access to a confidential file named "CAPTURE" by mistake.

To handle the issues of interoperability objects' must be provided with common interfaces to access resources. The designing of resource interfaces is a complex and tedious task as these interfaces should be able to provide support for various kinds of sequence of events.

5.2.2. Compromised Host

Ever since the discovery of multi-user operating systems, multi-tenancy has been the part of the study [5]. Different type of resources have different security issues related with them, however to achieve a safe resource distribution surroundings in a multitenant OS five major security dimensions can be taken into consideration. Firstly, access control, an access method must be provided to validate requests of users or processes to carry out OS operations like read, write on files, sockets etc. Secondly, use of Integrated Firewall. Thirdly, encryption techniques for data at rest and in transit. Fourthly, restraining execution of memory dedicated areas. Lastly, OS should provide isolation of resources.In case of security breach at host side, an intruder can easily gain access not only to all host's resources but also to resources of its tenants. Henceforth, the provider must ensure protection from third parties and should take necessary security measures to prevent such kind of security breaches.

5.2.3. Compromised Objects

In the PaaS service model the security of the user objects can be harmed in a number of factors. Firstly, the cloud service provider may misuse the user objects as the provider can access any data that resides on the cloud. Secondly, an inside attacker can gain access to and exploit a user's object through sniffing or spoofing because of multitenant nature of cloud. Thirdly, third parties may attack user object and gain access to the user confidential data.

5.3. Iaas Security Challenges

Iaas service model is the capacity conveyed to the consumers to procurement preparing, capacity, networks and other assets where the purchaser can deploy and execute

arbitrary software for example, OS and applications that best fit to their prerequisites. The cloud customer has control over operating systems, repositories, middleware etc. On the contrary to the aforementioned controls of the consumer, the consumer does not have administrative control over the cloud infrastructure. IaaS model basically involves creation of several VMs from the physical calculating resources to be shared among several users may be situated at various locations. The reliability and the predictability in relation to the availability of the cloud services is not certain [6] .But before all the above mentioned features can be used there are numerous security issues associated with IaaS service model that must be taken into account. The security issues vary with varying implementation of IaaS like the issues associated with private cloud implementation of IaaS are distinct from those of public cloud implementation. The below mentioned security challenges can be considered for both the aforementioned scenarios.

5.3.1. Data leakage

The private or public cloud both store data and that data must be supervised diligently. The monitoring of data becomes essentially important when IaaS service is deployed in pubic cloud. It is difficult to maintain information about who, how, where and what happens to data that is being accessed. These concerns can be solved by applying certain restrictions to mission critical data.

5.3.2. End-to-End Log in and Reporting

For successful implementation of IaaS service model extensive logging and reporting is essential. With proper reporting and logging mechanisms, the information about who is accessing the data, from where the data is being accessed and which data stores are responsible for providing the data, can easily be determined.

5.3.3. Lock-in or Interoperability risks

These risks arise when the cloud service provider platform does not support interoperability [7] expressed that there are no commonly acknowledged systems to encourage the amalgamation of service provider's administrations into undertaking models and to bolster the exchange of data between various suppliers. Thus, it sometimes makes it impossible for the users to transfer their data from one cloud service provider to the other, resulting in lock-in.

5.3.4. Risk of Business Continuity

These risks are due to of absence of control and knowledge of the consumers about the back-up policies that are currently available for cloud services. In case a consumer business requirement requires more cloud storage but is not able to pay for more cloud usage then the consumer may capacity issues and business continuity may come to risk.

5.3.5. Service Level Agreement Enforcement

Proper security constraints must be mentioned in the SLA. Monitoring and imposing of SLA is a challenging task. The SLA should focus on quality of the various services that is provided by the providers. Proper information about security measures and responsibility of each consumer as well as provider must be mentioned unambiguously.

5.3.6. Network Challenges

A large number of attacks are feasible when anything gets involved with the network. Some of them are Distributed Denial of Service attacks (DDoS), Man-In-The-Middle attack, IP spoofing, Port Scanning, DNS Security etc. A practical DoS attack was performed against Amazon EC2 by a cloud user by creating accounts and VM instances iteratively.

5.3.7. Virtualization Challenges

IaaS is mainly focused in providing infrastructure to its users by using virtualization methodology. This service model creates VMs from the physical resources and the distributed users are provided with these virtual instances. Monitoring of VMs, VMs isolation, communication between different VMs are some host originated threats. On the other hand, monitoring of VMs by other VMs, resources Denial of Service (DDoS), VMs migration is also one of the security threats due to virtual machines.

5.3.8. Hardware Challenges

The hardware devices are prone to physical attacks such as theft, damage and environment catastrophe like fire, earthquakes, and flood. The cables used for communication has to be protected from accidental or malicious harm. The service may become unavailable due to equipment failure. The backup devices must be available in case of any equipment failure and the unwanted devices have to be disposed of safely so that no confidential data may come in contact with malicious users.

VI. SECURITY SOLUTIONS AND METHODS

Security governance in cloud computing are same as those in traditional IT systems [7]. Nevertheless, due to heterogeneous systems, different technologies and different operational models involved in cloud computing, it may suffer

from risks which are absent in traditional IT environments. While moving to cloud, consumers should be aware of the maximum risks their business can withstand and should try applying security controls for the risks that the organization cannot bear to avoid.

The primary way a consumer can ensure cloud security is to validate the contract between the consumer and the service provider and also verify that the Service Level Agreement (SLA) contains all the requirements specified by the client. If the contract and SLA is not in accordance to the requirements, then it is advisable for an organization to drop the use of such cloud services. On the other hand, the cloud provider should also make sure that they are complaint with approved set of security solutions, which can be proved through certain certifications.

If a company wants to move to a cloud, it has numerous choices to do so. 34% of cloud users prefer to merge with an established CSP who will offer the resources. Second highest rank 33% of them use security software from self-governing software vendor/vendors, followed by 31% add security staff that are committed to the issues of cloud security. The most popular method to close the cloud security gap is the ability to set and enforce consistent cloud security policies (50%) [8]. Figure. 3 represents the ranking of factors that help in reducing cloud security gaps.

This section gives information about the security solutions for all three service models namely IaaS, PaaS and SaaS. A number of challenges are associated with IaaS service models like authentication, resource isolation, secure data backup, safe data destruction methods, fault-tolerance systems and a lot more. To solve all these issues security policies a major role. Louay Karadsheh (2012) in his study, describes the role of security policies, SLA and agreement for strengthening the security of the IaaS service model. The author has focused on a number of policies to enhance the level of security in cloud environment. Data removal and preservation policy, performance policy, compliance policy, secure connection policy, critical-application policy are some of the policy mentioned in [9]. The responsibility of IaaS's security lays more on cloud consumer than on provider. P.R.Jaiswal (2014) in his research has focused on how to solve the issues of data security, end-to-end logging, authentication and authorization on IaaS [6]. The author has mentioned that by using Rights Management policies one can put authorization restrictions on critical data .Also, the researcher talks about building processes that can monitor data utilization. Along with proper authentication techniques there should be an option of selecting security level so that depending upon the criticality of the data or resource appropriate logging mechanism can be built. To facilitate security from end-toend, complete disk encryption technique can be used which restricts offline attacks. Many new players have come in the IaaS market, below is the table showing comparison of the leading CSPs security offerings according to the survey done by FortyCloud. [10]

Currently organizations that need a thorough business-grade security solution need to take help of third party vendors (ISVs) to fill the security features that are missing in current CSPs. The Table.1 can be referred to identity which areas a CSP can rely for security solutions from ISVs to enhance their capability of providing secure cloud environment to the end users. One of the major issues in PaaS service model is of Interoperability. It is the ability to write code which can be executed on any platforms offered by varied CSPs.

The applications written for one provider may not run perfectly on the platform provided by the other provider due to differences in services offered by the two providers. The task of putting "all eggs in one basket" is very challenging and may cause lock-in of vendor or incompatible with other solutions available. Cloud4SOA, given by Eleni Kamateri(2013), is an extensible approach that interconnects heterogeneous PaaS offerings [11] over multiple Cloud providers that use common technology. The solution involves an arrangement of interlinked participating software models and components to

Table 1. Comparison of Cloud providers on basis of security methods

	Amazon Web Service	IBM Cloud	Rackspace	Windows Azure	Google Cloud Platform Live
Shared Cloud Network	Yes (EC2)	No	Yes	No	No
Virtual Private Cloud Network	Yes (VPC)	Yes	Yes	Yes	Yes
Firewalls	Security Groups	No	No	Firewall (endpoints only)	Firewall rules using Tags
Virtual Private Cloud Network across Data Centers	No	No	No	No	Yes
Remote Access to individual Cloud Servers	SSH/RDP	SSH/RDP	SSH/RDP	SSH/RDP	SSH/RDP
Identity-based access management	No	No	No	No	No
User-Based VPN Access	No	No	No	Yes	No
Secure extension using IPsec	Yes	No	No	Yes	In Beta

give the users and platform providers with numerous capabilities like administration, matchmaking, migration of applications and monitoring. Suggested by oracle in one of the five best practices for PaaS is to build a unified, standards-based PaaS platform to ensure portability between public or private cloud. For a successful development of hybrid cloud environment portability between all platforms is very important.

Oracle provides a common platform for all sorts of cloud integration such as data, services, events and processes

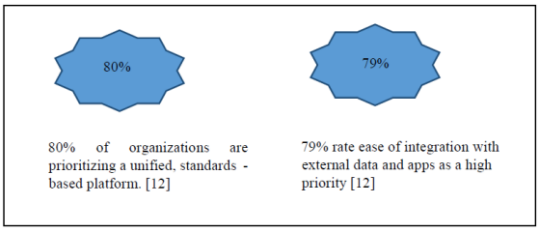
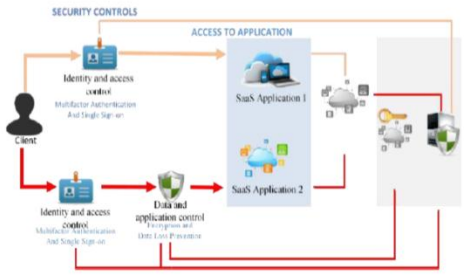


Fig. 3. Oracle's estimate of organization's demand for inter-operable cloud Platforms

Almost all leading companies are involved in building solution for SaaS. SaaS application offers agility and efficient, inexpensive, and extent partnership particularly with vendors and customers. Security challenges have always been there because the application run third-party code and host on it. To reduce risk in the cloud following best practices have been established by Intel:

1. Develop a SaaS security strategy and build a SaaS security reference architecture that reflects that strategies.
2. Balance risk and productivity.
3. Implement SaaS security controls.
4. Keep up with technology development [13].

A proposed security solution by BlueTie allows to provide safe scenario for data confidentiality. It's multi-faceted and multi-layered model for security is outlined not only to protect data in transit, but also to protect it while at rest in the cloud [14]. For the welfare of all organizations there is Security Intelligence Operation (SIO), which is based on cloud security service that can deliver warnings in global information, status-based services, and mature report to implement high level of protection plus fastest response time. Beginning with strategy development and extending to private cloud deployment, and reaching to the hybrid cloud, you can trust CIS with your most sensitive data. Defending against threats and protecting data in the cloud are complex tasks. A strong defense requires the steady observation of dangers wherever they happen and the skill to analyze their causes and the scope of outbreaks. Not every organization can support this level of threat intelligence, but the Cisco security ecosystem is unmatched. Along with our full support for international data protection regulations [15]. For information security and backup there is a demand of encryption algorithm. Although encryption is not yet meant to be for encrypting backup but an idea has been intruded in this paper. Determined to implement encryption is not the only parameter for security but the algorithm plays an important role hereby, an algorithm DECAST has been contributed in which a hybrid algorithm, that will increase the level of security of data by avoiding the disadvantage of individual algorithm [16]. For network security encryption technique such as SSL and TLS is preferred which can also be useful for key management in a network [17].
Aforesaid solution is just a glimpse of basic security measures whereas, typically issues like data segregation, sign on and accessibility need to be handled more carefully. With respect to the private cloud (preferred by most of the users) multitenancy is not a cover area of CSP as it can be categorized as authorization and authentication. Full data segregation is a myth as the users will have to share the resources so encryption is the key to protect it from unauthorized user. Recognized companies like Amazon offers AWS GovCloud which is an isolated AWS region designed to allow U.S. government agencies and clients to move sensitive data into the cloud by addressing their specific regulatory and compliance requirements [18]. Another aspect of data segregation is the physical location of enterprise's data is geographical location. It can be done in two ways either by trusting other management tool or by dealing with CSP.



VII. CONCLUSIONS

The advantages of cloud computing are being recognized and appreciated by the various organizations around the world. Since, above 85% of the organizations are exploring cloud computing in one way or another, the CSPs should take advantage of it by providing the best security solutions. By compelling the CSPs to expand cloud security solution will foster the cloud as a service. The evolution of cloud computing has gone through number of phases and each phase has provided benefits to the customers. After the benefits through evolution have been endorsed in the market, consumers are ready to migrate their data to cloud without the advice and assistance of the Cloud consultancy firm or non-negotiable agreement resulting in data insecurity and loss. Improper SLA is an outstanding issue in cloud computing. Just like before buying a car a costumer thoroughly reads the policies and blueprint for

warranty, in the same way SLA serves as the assurance of the consumer's data. As described in the paper, there are many loop-holes in terms of security with the provided solutions. For some services there may be two or more than two security mechanisms required for better performance, depends on the type of attack.

There is a big question on how the security should be provided, in an integrated manner or customized according to the user. If we provide the service in an integrated manner then the CSP should be intelligent enough to conclude what security is required at a particular service dynamically. It is possible with the help of metadata. But this proposal may require lot of memory space, bandwidth and expenses from the user end. If the bandwidth is occupied by the security mechanism it is obvious that the basic services of cloud computing will have to be compromised. Even if one security solution is affected the overall security will be hampered and the net security level shall be brought to almost zero which makes it more vulnerable for hackers and intruders. The CSP can also provide customized security services to the customers. A user should be intelligent enough to understand the security risks associated with his business and select appropriate safety measures. In customized security, it may however create a capacity bottleneck for the cloud provider as different users may require different security mechanisms and to implement all security controls may not be feasible for the provider. However, the provider may provide each of its unique customers, unique security privileges in which the customer has to be careful and aware of the functionality and the services of the security solution. Also, this kind of implementation is difficult to hack and intrude. There is still an ambiguity on how the mechanisms should be implemented and research is going in full swing to provide best security solutions for cloud services.

REFERENCES

[1]. P. Mell and T. Grance, in The NIST Definition of Cloud Computing, NIST Special Publication, 2012.
[2]. M. Ali, S. U. Khan and A. V.Vasilakos, "Security in Cloud Computing: Opportunities and challenges," Information Sciences, pp. 357-383, 2015.
[3]. D. M. Dekker and D. Liveri, "Cloud Security Guide for SMEs," European Union Agency for Network and Information Security , 2015.
[4]. verizon, "2015 Data Breach Investigations Report," verizon, 2015.
[5]. L. Rodero-Merino, L. M.Vaquero, E. Caror and A. Muresan, "Building safe PaaS clouds: Asurvey on security in multititenant software platforms," Elsevier, pp. 96-108, 2012.
[6]. R. A. Jaiswal P.R, "Infrastructure as a Service:Security Issues in Cloud Computing," vol. 3, no. 3, 2014.
[7]. "security for cloud computing 10 steps to ensure success," Cloud standards Customer Council, 2012.
[8]. H. Schulzl, "Cloud SeCuritY -Spotlight RepoRt," 2015.
[9]. L. Karadsheh, "Applying Security Policies and Servicelevel agreement to IaaS service model to enhance security and transition," Elsevier, pp. 315326, 2012.
[10]. A. Naftali, "Iaas Security State Of The Industry – Comparing Iaas Providers," Fortycloud, 2015.
[11]. E. Kamateri And N. Loutas, "Cloud4soa: A Semantic-Interoperability PaaS Solution for Multi-cloud Platform Management and Portability," Springer Berlin Heidelberg, pp. 64-78, 2013.
[12]. "Five Best Practices for Platform as a Service Success," 2015.
[13]. S. Levi, E. Brik, E. Gutierrez, K. J.Logan, J. Noel, N. Zand, C. Ashley, T. Bui and P. Mathews, "SaaS Security Best Practices: Mininmizing Risk in the Cloud," 2015.
[14]. "Advanced SaaS Security Measures ," 2010.
[15]. "Cloud Security Trust Cisco to Protect Your Data," 2015.
[16]. N. Sengupta and R. Chinnasamy, "Contriving Hybrid DESCAST Algorithm for Cloud Security," Elsevier, pp. 47-56, 2015.
[17]. P. K.V and V.Vijayakumar, "Survey on the Key Management for securing the Cloud," 2015.
[18]. Amazon, "AWS GovCloud (US) User Guide," 2016.