Challenges in Cloud Security

Reena Somani
Assistant Professor,
Information Technology
Atharva College of Engineering,
India

Gayatri Sawale
Assistant Professor,
Information Technology
Atharva College of Engineering,
India

Poonam Joshi
Assistant Professor,
Information Technology
Atharva College of Engineering,
India

***Abstract*—Cloud computing is a technology that gives a on-demand access and convenient to the eclectic and various services through a shared pool of configurable computing resources. Recent advances have given rise to the popularity and success of cloud computing. Cloud computing provides many benefits in terms of low cost and accessibility of data. Anyhow, when the business application to a third party and outsourcing the data causes the security and privacy issues to become a critic concern. Cloud Computing also attracts the attentions of attackers and raises many security concerns. One main concern of using the cloud is data privacy and security especially for users with sensitive data that would be detrimental to the client if it were stolen. cloud security is an emerging sub-domain of network security, computer security and more vastly information security. It points to a broad set of technologies, policies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. This paper we discussed deployment and service model, various security challenges in cloud and security issues and control mechanism in cloud security and also focused on cloud security technologies. Hence In this paper cloud security concerns and security requirements are addressed.**

Keywords— Cloud Computing, Cloud Security, Security Challenges and issues, Control Mechanism

I. INTRODUCTION

Now a days increasingly prevalent cloud computing, datacenters play a fundamental role as the major cloud infrastructure providers, such as Google, Amazon, and Microsoft Azure. Datacenters gives the utility computing services to the software service providers who further provide the application service to end users through Internet. The later service has long been called "Software as a Service (SaaS)", and the former service has recently been called "Infrastructure as a Service (IaaS)", where the software service provider is also referred to as cloud service provider. To take the advantage of computing and storage resources provided by cloud infrastructure providers, data owners outsource more and more data to the datacenters through cloud service providers, eg.- the online storage service provider, which are not fully trusted by data owners.

As a general data structure to describe the relation between the graph ,entities has been increasingly used to model schema less data and complicated structures, such as the personal social network (the social graph), the relational data base, For the protection of users privacy, the sensitive data have to be encrypted before outsourcing to the cloud. Moreover, some data are supposed to be shared among trusted partners to all organizations.

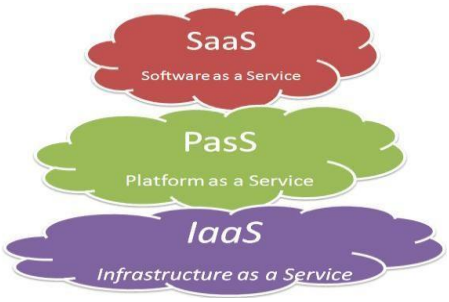
II. CLOUD COMPUTING ARCHITECTURE

There are several major cloud computing providers including Google, Amazon, Salesforce, Yahoo, Microsoft and others that are providing cloud computing services (Figure1. shows current cloud providers).Cloud computing providers provide a variety of services to the customers and these services include software-as-a-services,e-mails, storage, infrastructure-as-a-services etc.

The main attractiveness of cloud computing is not only to large enterprises but also startups,entrepreneurs, medium companies and small companies would benefit greatly and they will have a new alternative and opportunities that is not available to them in the past that would save them millions of dollars because with cloud computing they will have the choice to only rent the necessary computing power, storage space and communication capacity from a large cloud computing provider that has all of these assets connected to the Internet**.** In practice, cloud service providers tend to offer services that can be grouped into three categories: platform as a service, software as a service, and infrastructure as a service. The all three categories group together the various layers illustrated in Figure1, with some overlap.

A. Software as a Service (SaaS)

The use of single instance of the application runs on the multiple end users or client organizations and cloud services. The widely known example of SaaS is salesforce.com, though many other examples have come to market, including email and word processing, including the Google Apps offering of basic business services..



B. Platform as a service (PaaS)

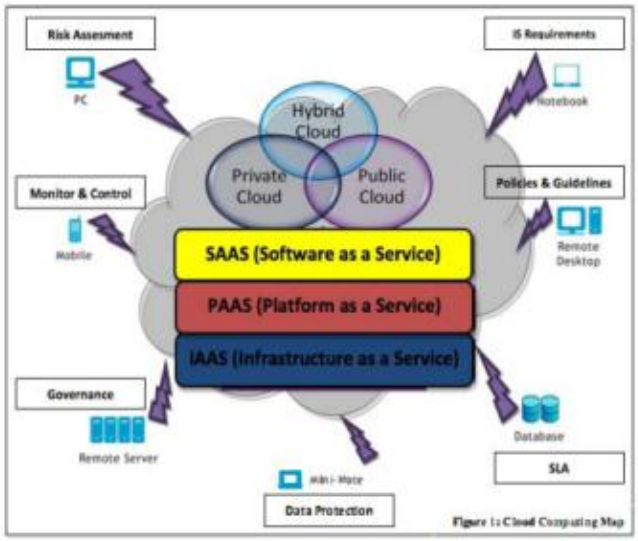
Platform as a service enclosed a layer of software and provides it as a service that is used to build higher- level services. There are at least two perspectives on PaaS depending on the perspective of the producer or consumer of the services:

C. Infrastructure as a service (IaaS)

Infrastructure as a service gives the basic storage and compute capabilities as a standardized services over the network. Storage systems, servers, switches, routers, and other systems are pooled and made available to handle workloads that range from application components to high- performance computing applications.Examples of IaaS include Joyent, whose main product is a line of virtualized servers that provide a highly available on-demand infrastructure.

III. DEPLOYMENT AND SERVICE MODEL OF CLOUD

For deploying a cloud computing solution, the major task is to decide on the type of cloud to be implemented. Presently three types of cloud deployment takes place - ,private cloud , public cloud and hybrid cloud Figure below shows the overview of the deployment of these three clouds[9]



A. Public Cloud

Public cloud allows users' to access the cloud via interfaces using web browsers. Users need to pay only for the time duration they use the service, i.e., pay-per-use. This can be compared to the electricity system which we receive at our homes. We pay only for the amount of that we use. The same concept applies here. This helps in reducing the operation costs on IT expenditure. However public clouds are less secure compared to other cloud models as all the applications and data on the public cloud are more prone to malicious attacks. The solution to this can be that security checks be implemented through validation on both sides, by the cloud vendor as well as the client. Also both the parties need to identify their responsibilities within their boundaries of operation.

B. Private Cloud

A private clouds operation is within an organization's internal enterprise data center. The main advantage here is that it is easier to manage security, maintenance and upgrades and also provides more control over the deployment and use. Private cloud can be compared to intranet. Compared to public cloud where all the resources and applications were managed by the service provider, in private cloud these services are pooled together and made available for the users at the organizational level. The resources and applications are managed by the organization itself. Security is enhanced here as only theorganizations' users' have access to the private cloud.

C. Hybrid Cloud

It is a combination of public cloud and private cloud. In this model a private cloud is linked to one or more external cloud services. It is more secure way to control data and applications and allows the party to access information over the internet. It enables the organization to serve its needs in the private cloud and if some occasional need occurs it asks the public cloud for intensive computing resources.

D. Community Cloud

When many organization jointly construct and share a cloud infrastructure, their requirements and policies then such a cloud model is called as a community cloud. The cloud infrastructure could be hosted by a third-party provider or within one of the organizations in the community.

IV SECURITY ISSUES AND CONTROL MECHANISMS IN CLOUD

A. CLOUD SECURITY ISSUES

Cloud security differs from the conventional security requirements in many ways. Threats such as Insecure Application Programming Interface, Data Loss, hijacking etc. [3] have to be overcome. Hence, a Cloud environment requires various levels of security to be in place. Figure I shows the various levels of security required. The levels consist of Network level security, System level security,Virtual Machine security and Application level security. Network level security ensures that no data could be snooped from the network, System level security ensures that no unauthorized, unauthenticated access could takes place and application level security ensures that no illegitimate application could be run on the virtual machine that could compromise the safety of any data or no application could access anylhing past system limits. For this it must be ensured that only clean images are deployed and constant monitoring of running applications is required. Such security measures could be ensured by following the traditional security approaches such as encryption techniques, secure logins etc. The cloud environment requires an additional virtual machine level security when compared to the conventional security features. While network, system and application level security measures have evolved over the years, security at the virtual machine level is to be supported by cloud. This involves tracking of data due to migration techniques in cloud and isolation of data belonging to various organizations sharing the same system. Existences of such features in a cloud environment pose a major challenge to the cloud service provider. When these issues have been tackled, the cloud technology would be adopted on a large

scale by the industry.
While the CSP must ensure that a basic security mechanism is in place, any additional security measures could be implemented and customized according to the needs of the customers' organizational policies and needs. Such an approach has been proposed in [2]

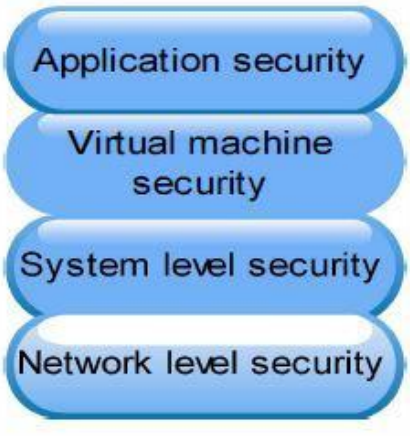


Figure 3 Security levels in cloud

The security mechanisms to be provided at each level may be described as follows:
• Network level: Firewalls, Encryption techniques and network isolation are few of the mechanisms to be provided at the network level. Threats like Man-in-the middle attacks are to be prevented.
• System level: Appropriate authentication and authorization of personnel at the CSP end and users at the client-side are necessary.
• Virtual machine level: At the Virtual machine level, proper isolation of applications and data belonging to difference clients must be implemented. All possiblesecurity holes for cross access of virtual machines must be prevented. Most importantly, the Operating system running on the Virtual machine should be secure and trustable.
• Application-level: Proper mechanisms must be in place for all the applications loaded on the Virtual machines. Security certificates could be provided for any application loaded on the cloud.By providing such levels of security, the Cloud environment could be made more trustable and safe. Security measures and mechanisms could be developed and customized according to the client's organizational needs and must be upgraded frequently to prevent occurrence of any mishaps.

B. Security Control Mechanisms
Various measures have been proposed in the literature to tackle the security issues. These have been summarized in the following sections based on the phase of cloud migration.Cloud Security Policies and Procedures - A classification
The security policies, procedures and control mechanisms to be adopted by the CSPs could be broadly classified into the following categories - pre-migration, inoperation and termination.

1) Pre-migration security procedure
When there is a migration of application and data to a cloud by an organization, their organizational Information security policies which are applicable to the new cloud setting must be extended to the cloud environment. It is the responsibility of the cloud provider to ensure that such policies have been taken care of. Prior to migration of applications and data to cloud, SLAs or contractual agreement between the vendor and the client ensures an availability of log files, compliance regulations, type of access control mechanisms, encryption standards etc. in the cloud. Along with this, additional security policies and features for managing the virtual environment must be made available. These may include - isolation of virtual networks and environment, accountability, monitoring, data location, backup plans, applicable laws and regulations and the extent of client control over the cloud infrastructure and environment. [1] An important policy to be taken care of is about the Geographical boundaries within which the data might reside. Since the Laws and Regulations vary across physical boundaries, the client might be put to risk in case of a legal situation. More complexity might arise due to the fact that Cloud vendors may have sub contracts with other CSPs. In such a scenario, it is important that security policies and procedures are understood and agreed upon at the very outset. Some of these issues that have to be address have
been specified in [6], [7] and [8]. The contractual agreement between the client and the CSP would move the onus on the CSP to provide measures against such undesirable situations. Having established the basic contractual agreement, the security features to be taken care of while in-operation have been discussed next.

2) In-Operation security mechanisms
These include tackling the security attacks while in operational, post the migration of applications and data. It involves technical measures to be adopted for a smooth operation of applications and data security in a cloud environment. Both prevention and detection measures have to be applied. The security control mechanisms provided during the Operational phase include measures against security threats like Man-in-the-middle attacks, unauthorized access etc. These types of threats could be prevented by providing the conventional security measures like provision of frrewalls, secure APIs and taking frequent backups. Moreover, authentication and authorization of both personnel and trusted nodes are required to prevent unauthorized access. During the operational phase, legal issues such as applicable laws, physical location of servers, subcontracts [5] and Compliance issues such as maintenance of log files for audit purposes are to be taken care of. In case of any security incident, measures such as in [6] would provide traceability

3) Termination phase security procedure
When vendor or client go out-of-business or there is a vendor change, security of data must be ensured. Data destruction procedures must be followed in order to prevent illegal usage of data. In case of transfer to another vendor, a new contractual agreement has to be worked out.

V- CLOUDCOMPUTING SECURITY CHALLENGES

Cloud Computing could be used almost everywhere in today's society and provides numerous benefits to companies, government and individual users. Cloud Computing also attracts the attentions of attackers and raises many security concerns. One main concern of using the cloud is data privacy and security especially for users with sensitive data that would be detrimental to the client if it were stolen. Data integrity, cost or replicating data and reliability are some points service providers would have to address in order to sway users to commit to using Storage as a Service. Access control and user authentication needs to be seamlessly supported for a large number of simultaneous users while avoiding a single point of failure is a challenge for the cloud OS.

1) Data privacy and security

Confidentiality, integrity, and availability, are three key issues in Information Assurance, they are also very important in Cloud Computing because applications are deployed in a shared network environment. Confidentiality gives customers the reassurance that the information that is being stored offsite that can only be accessed by authorized persons. Integrity of the data that is transferred from one location to another is to guarantee that the data has not been corrupted or tampered with in any way, and to keep the data in its original format. Last but definitely not least, availability is the data available when it is needed. This is determined by certain policies set in place, to make sure the customer has the data when stated available. These are key factors insecurity challenges that consumers, providers, and developers have, and will continue to face when providing confidentiality, integrity, and availability within the cloud. Keeping all cryptographic algorithms up to date is another factor when the information needed to be protected is done so by encryption. In the case of a developer using cryptographic algorithms that are not up to date can result in exposing pertinent data that was encrypted but can be compromised because of a faulty algorithm. This presents a challenge in the case of information leakage for the cloud provider, and the consumer's information which has been victimized. If the developers are not aware or concerned about these changes the security risk will continue to increase, while attackers are looking for specific vulnerabilities dealing with unsuitable cryptographic algorithms.

2) External threats

An attacker that exploits vulnerabilities in services provided to a consumer, poses external threats that both the consumer and provider must be aware of. External threats can be characterized by attacks that occur outside a consumers' domain. External threats include man-in-the-middle, packet sniffing, IP spoofing, denial of service attacks, etc. Applications are a key component in Cloud Computing and a perfect opportunity for a man-in-the-middle attack. This happens when a malicious user deploys a proxy application in between a consumer and provider without them knowing and the attacker intercepts personal information such as login credentials, credit card information and more. Data within the cloud travels over a designated network to and from a specific location while a vast number of packets are sent containing sensitive data. A malicious user can capture and analyze the data in the packets sent over this network by packet sniffing. IP spoofing occurs when a malicious user impersonates a legitimate users IP address where they could access information that they would not have been able to access otherwise.

3) Guest-to-cloud threats

Guest-to-cloud threats deal with malicious behavior on the guests' side. This behavior could include the guest conducting certain attacks that affect the provided cloud infrastructure. Possible attacks that threaten the cloud provider would be SQL injection and Cross- Site scripting. Knowing data is initially collected from registration applications for cloud services and or trial registrations these attacks can be used on the guest side application where attackers and other malicious users look to attack. Because of the re-use of a lot of these applications any known or similar vulnerabilities not mitigated can be easily exploited by hackers. Sharing not only information but infrastructure within An example of a guest-to-cloud threat would be the malicious use of the command for a virtualized video device "VMware SVGA II" where SVGA stands for Super Video Graphics Array. The command allows execution of code on the host side from the guests' side. The expected use for this command is to copy a source rectangle in the frame buffer to a given destination. There are two obvious ways to abuse the command, either misplaces the source rectangle or the destination rectangle, leading to two different types of bugs.

4) Other security issues

Other security issues include insecure interfaces and APIs, malicious insiders, and an unknown risk profile. APIs are used as the bridge between a user and their services. Because a lot of activity occurs on these interfaces the possibility of vulnerabilities is high. General cloud services depend upon the security of these basic APIs in order to maintain their own security and availability [8].

A malicious insider is a major threat to consumers of cloud services. The centralized location of consumers' data poses a major issue if a person with malicious tendencies infiltrates a cloud providers system. If the providers' security procedures for physical and logical access controls do not meet those of the consumers it can allow a malicious employee on the providers' side to collect and or modify data that belongs to a consumer. This kind of situation clearly creates an attractive opportunity for an adversary ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion [8].

VI- SECURITY TECHNOLOGIES

Many security technologies have been proposed and developed to enhance Cloud Computing security. Cisco Secure Data Center Framework is one of them that provides multiple security layers and applied different existing security technologies to enhance Cloud Computing security [10]. Cisco has developed the Cisco Secure Data Center Framework with many security and trust considerations. The first consideration is security. In this framework traditional security issues of information assurance such as data access control, encryption, and incident detection are integrated. The second consideration is control that means an enterprise has capability to directly manage how and where data and applications are deployed and used. The third consideration is compliance and service-level management (SLA). It includes contracting and enforcement of service level agreements between different parties, legal issues, regulation and industry requirements, etc. Figure 5 shows the framework that consists of Threat Profile, Cloud Data Center Visibility, Cloud Data Center Protection, Cloud Data Center Building Blocks, Cloud Data Center Control, Cloud Data Center Compliance and SLA. The Threat Profile contains threat models such as Service Disruption, Intrusion and Takeover, Data Leakage, Data Disclosure, Data Modification, Identity theft and Fraud, etc. The Cloud Data Center Visibility provides various functions such as intrusion detection, anomaly detection, packet capture, network data collection and monitoring as well as event analysis and correlation. The Cloud Data Center Protection is very straightforward and provides different protection techniques and mechanisms such as stateful firewall access control, intrusion prevention, content filtering, and enforces endpoint and baseline security. Cloud Data Center Control deals many issues with how data being control. Because data are centralized in Cloud Computing it increase the possibility of insider threats, therefore a compartmentalization strategy is important. The data encryption policy must be in place for customers and providers. For an administrator, who accesses and controls virtualized operating system, must be strong authenticated. The Cloud Data Center Compliance and SLA deal with how the data being handled is controlled. So certain requirements are set in place by the consumer and provider in order to reach an agreement to make sure requirements for both are met. The service level agreement is in place to enforce these requirements and to make sure that the consumer and provider remain compliant [5]

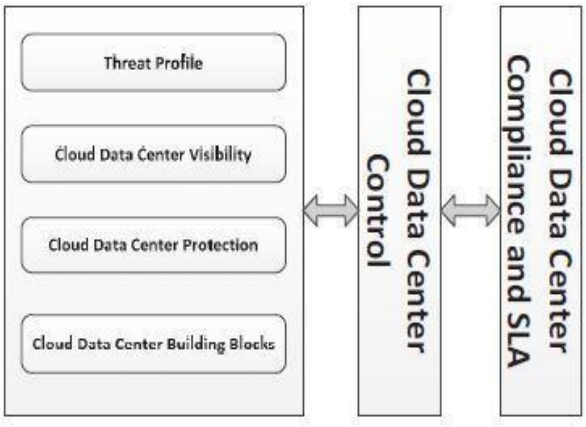


Figure 4. Secure cloud data center framework

The scalability of Cloud Computing is what makes the cloud different from the network today. Using these various services can present a more robust computing environment that can lead to smaller Internet based companies, easier user interactions and reduced cost in company infrastructure. As software engineers we still face any security problems in Cloud Computing and more research must be done.

VII- CONCLUSION

These measures would ensure a smooth operation of applications in the cloud without posing any potential risk to the client. The next section discusses the security measures to be ensured in case of contract termination or transfer to another CSP. Even though all known security mechanisms are put in place, security measures have to evolve down the line based on experimental and experience basis. Thus, different technical and legal aspects have to be taken care of by the CSP during the various phases of migration to cloud. Putting both technological and legal aspects in place would create a trust environment between the client and the CSP, thereby quickening the phase of Cloud adoption by the industry.The legal, security and regu latory issues and management techniques in Cloud have been discussed in detail. Proper policies and procedures must be in place at the provider side This would ensure a smooth migration to and adoption of cloud environment by Organizations. Any application running on the cloud environment should be supported by various levels of security. It must include network security, operating environment security and security at the Virtualization layer level. The various tasks and control measures to be taken by the CSP at various phases of migration have been discussed. Both the client as well as the CSP should agree upon these security measures. Such an understanding between these two parties would result in an increased level of trust in the cloud for the client.

REFERENCES

[1] Ramgovind, s. et ai, "The management of security in Cloud", Proceedings of lnformation Security for South Africa (lSSA), 2010
[2] Hamlen, K. et ai, "Security issues for Cloud Computing", International Journal of Information Security and Privacy, Vol 4 , Issue 2, April-June 2010
[3] Srinivasamurthy, S., David Q. Liu, "Survey on Cloud Computing Security", Proceedings of 2nd IEEE International Conference on Cloud Computing Technology and Science, 2010
[4] J. Wu, L. Ping, X. Ge, Y. Wang and J. Fu, "Cloud Storage as the Infrastructure of Cloud Computing", IEEE Int. Conf. on Intelligent Computing and Cognitive Informatics, June 2010.
[5] K. Bakshi, "Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions", DOI=http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing_WP.pdf
[6] Kuyoro S.O. et ai, "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Vol. 3, Issue 5, Page 247-253, 2011
[7] Alvi, F.A. et ai, "A review on cloud computing security issues & challenges", Proceedings of 1st International Conference on Mobility for Life, 2012
[8] Jansen, W., Grance, T., "Guidelines on Security and Privacy in Public Cloud Computing", http://www.nist.gov/itllcsd/cloud-012412.cITn, 2011
[9] Cloud Computing Architecture http://communication.howstuffworks.com/cloud-computingl.htm
[10] Peeyush Mathur, Nikhil Nishchal, "Cloud Computing: New challenge to the entire computer industry", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).
[11] Bhaskar Prasad Rimal, Eunmi Choi, "A taxonomy and survey of cloud computing systems", 2009 Fifth International Joint Conference on INC, IMS and IDC, published by IEEE Computer Society.