ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

A brief Survey on Security Issues in Cloud and its service models

G.Kalpana[1], P.V. Kumar[2], R.V.Krishnaiah[3]

Research Scholar, Dept of C.S.E, DRK Institute of Science &Technology, Hyderabad, India [1]

Professor, Dept of C.S.E, Osmania College of Engineering. O.U, Hyderabad, India[2]

Dean, Dept of C.S.E, Institute of Aeronautical Engineering, Hyderabad, India [3]

Abstract: With the progress of cloud computing there is significant transformation in IT organisations. The immense thrust for cloud computing by numerous large companies has been at the forefront of the cloud computing movement. It will be easily reached worldwide via internet, an advantage for large, intermediate and small enterprises. Storage of data in cloud is fast moving and moreover the security breach is a worry and we can expect to see many maturities in the coming years. The diverse concerns that arise have to be magnified with respect to safety and confidentiality of the data in cloud. There are many pros in using the cloud besides many cons, which should be taken into observation from which most of them being specific in cloud. This paper presents a glimpse of survey on cloud computing along with its safety.

Keywords: Cloud computing, confidentiality, Data storage, issue, analysis.

I. INTRODUCTION

As the technology advances, computing has become the fifth most utility besides the water, electricity, gas and telephony [1].The triumph of internet has led the computing ability budge from an individual desktop to service providers' computer over the internet. The technology of the Cloud computing is based on the technique that all the data storage and processing will be done away from the end user, which leads to the security threats(Secrecy, Integrity, Availability) in cloud computing. Cloud computing proffers various advantages for service providers, end users and business organizations but have drawbacks as well. The major advantage is that user need not handle the infrastructure, development environment and applications, the complications taken care by third parties.

In this paper, we analyse the security issues involving in Cloud service models such as security issues in Platform as a Service, Software as a Service and Infrastructure as a Service.The rest of this paper is structured as follows: Section II introduces the cloud definition, different types of Cloud models also known as deployment models, cloud structure, advantages of cloud computing and survey report by IDC of cloud challenges. Section III explains Cloud computing service models with a security insight. Finally, section IV gives the conclusion.

II. OVERVIEW OF CLOUD COMPUTING

As defined by Buyya[1],"A Cloud is a type of parallel and distributed system consisting of a collection of inter connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service level agreements established through negotiation between the service provider and user."

The Cloud computing uses the internet as the media, data storage, processing and maintenance is provided by the cloud vendor which leaves the user/client/customer unaware of where the data is stored and processed. So, the client never be having the control over the data in cloud. The Service Level Agreement (SLA) is only the legal agreement between user and service provider.

A. TYPES OF CLOUDS

Model	Description
Public cloud	The service provider makes resources (applications, storage, and so on) available to the general public over the Internet.
Private cloud	The infrastructure is dedicated to one organization.
Community cloud	Several organizations share resources.
Hybrid cloud	This model combines two or more of the other deployment models.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

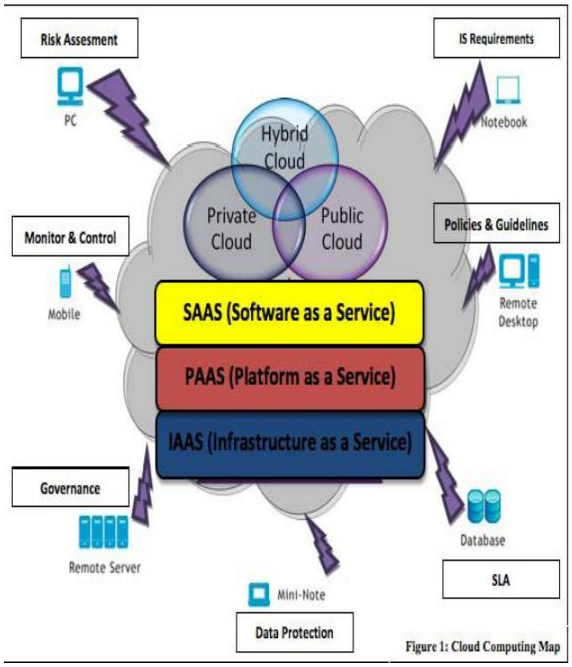

Figure. 1Structure of Cloud computing

B. Advantages of Cloud Computing

1) Cost Saving: With cloud computing, we can save extensive capital costs with zero in-house server storage, development environment and application requirements. The lack of on-p remises infrastructure also removes their associated operational costs in the form of power, air conditioning and administration costs. We pay for what is used and free whenever we like. Apart from storage and infrastructure costs, all the other costs can be reduced with cloud services like updating and managing software or applications, employing and training new staff.

2) Convenience and continuous availability: With a supervised service platform, cloud computing is much more reliable and consistent than in-house IT infrastructure. This enables easy access to information and facilitates the needs of users in different time zones and geographic locations. Most providers offer a Service Level Agreement that guarantees 24/7/365 and 99.99% availability. Organization can benefit from a immense pool of excessive IT resources, if a server fails, hosted applications and services can easily be hand over to any of the available servers.

3) Backup and Recovery: Cloud backup services can make simpler the process of saving important data, and the superlative solutions allow a business to stay up and running even in the event of a disaster Xerox's Cloud Backup offers highly developed, patented data deduplication and virtual server protection technologies from Quantum, a esteemed leader in data protection and management. This service replicates information from a locally installed Quantum product, which reduplicates compresses and encrypts data prior to transmitting it to the Xerox cloud. The complete process occurs automatically, every day.

4) Cloud is environmentally friendly: Cloud data center minimizes the energy consumed through server consolidation, where the different workloads can share the same physical host using virtualization and unused servers can be switched off.When the servers are not in use, the infrastructure usually scales down, freeing up all the resources and consuming less power.

5) Reliability, Scalability, Flexibility and Performance: Cloud computing presents the opportunity to scale their computing resources whenever they need it necessary for the organizations both in large and small. This is done automatically either increasing or decreasing the required resources, services, meaning we're not paying for which we are not utilizing.

The systems utilize distributed environment which offer excellent speed of computations, so the performance can be increased. Cloud computing allows employees to be more flexible in their work practices, even it provides on demand bandwidths. Cloud reliability offer failure-free services to the hardware, software, consumer's personnel, and connectivity to the subscribed services

6) Quick deployment and ease of integration: Through the cloud, a business is allowed to choose the services and applications that best suit their preferences, while there is minimum effort in customizing and integrating those applications. MENDIX,SAP HANA[2] Cloud Platforms are the scalable, secure, modular, and open-standard platform as a services (PaaS). These include comprehensive functionality designed to facilitate customers and partners to build cloud-based business applications quickly .The software integration occurs automatically, in nature in the cloud environment.

7) Increased Storage Capacity: The cloud can accommodate and store more data according to the user requirement. Cloud creates the extra data center space to accommodate banks of hard drives. "Virtual machines" (VMs) create store and access data across a pool of virtualized storage. That data is stored wherever the capacity exists, in a random fashion. No more infrastructure investments or time spent adding new servers, partitioning silos – none of that mess.

8) Device Diversity and Location Independence (Mobility): Cloud computing services can be accessed via any of the electronic devices (traditional PCs, Smartphone's, notebooks, tablets etc) that are able to have access to the internet. There is no limitation of location and medium. We can access our applications and data anywhere in the world. Easy learning: Due to the efficient services of the cloud, people can learn and adopt the applications very easily(For e.g.: Gmail, Box, toggl and Google Docs etc.)

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

C. Cloud Computing Challenges:

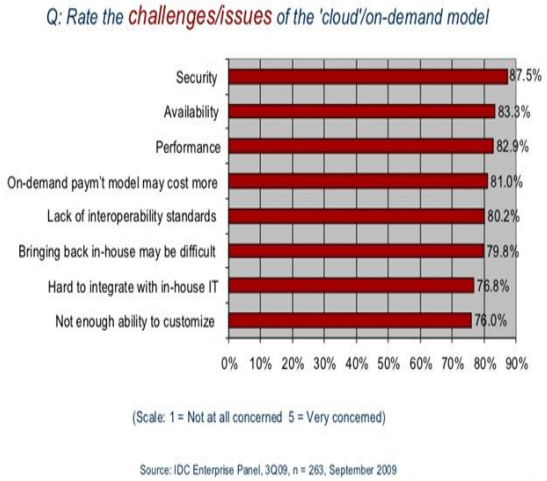

Figure 2 Cloud computing Challenges and Issues in August 2008

The figure 2 demonstrates the cloud challenges and issues survey taken by IDC in Aug 2008.Even though having the strong advantages, cloud torments with the security, privacy,availability, service delivery, billing, performance and third party dependences.

III.CLOUD SERVICE MODELS AND ITS SECURITY

Cloud computing uses many delivery models in which three are very important by which various types of services are delivered to the end user. The three delivery models are

- SaaS (Software as a service).
- PaaS (Platform as a Service).
- IaaS(Infrastructure as a Service).

SaaS: - is asoftware development model where applications are remotely hosted by the application or service provider and made available to customers on demand over the internet. A singleoccurrence of the software runs on the cloud and offers services to multiple end users or client organizations. The end user need not to manage or control the cloud infrastructure-operating systems,networks,storage, even the applications which are using. Example of SaaS - salesforce.com, Google Apps, email and word processing.

PaaS:-delivery model allows consumers to deploy their applications to the cloud infrastructure by means of platforms such as application servers and database services.
Consumer created applications can be produced using the programming languages, tools provided by the Cloud Service Provider. The consumer does not have the control over the cloud infrastructure but has control over deployed user applications .Example of PaaS-Microsoft Windows Azure as PaaS can be used as a development, service hosting and service management environment. SQL Azure can provide data services, including a relational database, reporting and data synchronization.

IaaS:-is the lowest level of service model in cloud delivery models. IaaS provides the consumer with theability to acquire processing, storage, networks and others fundamentals computing resources and allows consumer to deploy and run their own software, which can include operating system and applications. Instead of spending big expenses with their own data centers,softwares, etc. The consumer has the control over the storage, operating system and deployed applications. An Amazon web service is a one of the IaaS service provider –will runs a virtual server running in minutes and pay what for we use.

A. Security issues in SaaS:

Most of the Enterprises are throbbing with the SaaS model due to lack of visibility about the way their data is stored and secured. In SaaS, the client has to depend on the provider for appropriate security services. The provider must take care about multiple users' from watching each other's data. It is complex to the user to make sure that the security measures are in right way and the application be available when it necessary.
The SaaS software vendor can host the application or deploy it on a cloud computing infrastructure service provided by a third-party provider (e.g. Amazon, Google, etc.).This helps the application service provider to minimize the investment in infrastructure services and enables it to deliberate on providing better services to customers.
In SaaS model, data is stored at the SaaS provider's data center, along with the data of many enterprises and data of other unrelated SaaS applications. The cloud provider may replicate the data at numerous locations across countries for the purpose of maintaining high availability of data. As a result, there is lack of control and familiarity of how their data is stored and secured in the SaaS model. There are strong concerns about data despoliation, application vulnerabilities and availability.

The following key security essentials should be cautiously considered as an important part of the SaaS application development and deployment process:

- Security of the data
- Locality of the data
- Privacy of the data
- Integrity of the data
- Data isolation
- Accessibility to data
- Sniffing of data on the network
- Authentication, authorization and Identity management.
- Web application security
- Virtualization vulnerability
- Availability
- Backup

The different security concerns of SaaS are discussed as follows.

1) Security of the data: In traditional computing model, the sensitive data resides within in the organizational boundaries and is subject to its own

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

organizational policies. But in the SaaS the data is stored at outside the organization, at the SaaS vendor. SaaS vendor must take up additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious users. It must use strong encryption techniques for data security and fine authentication and authorization techniques to control access to data.

For eg-the cloud vendors like Amazon, the Elastic Compute Cloud (EC2) admin even restricted to access the customer objects and cannot log into the Guest OS. EC2 Administrators with a business need are necessary to use their individual cryptographically strong Secure Shell (SSH) keys to get access to a host. All these accesses are logged, audited regularly. Data resides in Simple Storage Service (S3) is not encrypted by default, users can encrypt their data before it is uploaded to Amazon S3 with the efficient encryption techniques

2) Locality of the data:In cloud environment, the consumers use the applications provided by the SaaS and process their business data. But the customer does not know where the data is located, this can be an issue. When we use a cloud computing provider, our data travels over the Internet to and from one or more superficially managed data centers. Various legal issues can arise when a customer's data resides in a cloud provider's data center in different countries. Different countries, and in some cases even different states, region or municipalities, have different laws pertaining to data.

A key question raised [4], which law applies to my organization's data in the cloud: The law where I'm located, the law where my data's located, or the law where the data subject is located? , remains unsettled in cloud computing. For these reasons it's necessary for a cloud-computing provider to classify the geographic region within which the data centers locating the data.

3) Privacy of the data: Privacy refers to prevent sensitive information from reaching the unauthorized people, while making sure that the authorized people can in fact get it. Cloud allows sharing of data in different stages by various people located remotely. The cloud data includes small and big organizational data, various sites data, health records, multimedia data, many more. Customer's data resides among distrusted cloud servers with one or data centers can be owned and managed by cloud provider. The privacy question arises when data is accessed by the users because remote storage and location of information is not known for protecting the data in cloud this may lead to legal issues. Such training would typically include security risks that could threaten this information. Leaving the privacy leads to data leakage.

Privacy achieved using the data encryption. User IDs and passwords ,two-factor authentication , biometric verification , OTPs(One Time Password),security tokens, key fobs or soft tokens all will be used to get the access to authorized persons.

4) Integrity of the data: Integrity refers to maintaining the consistency, accuracy, and credibility of data over its entire life cycle. Major threats to cloud integrity are data loss and manipulation,deceitful computation in remote servers by unauthorized members. Data must not be altered at data centers or in transit, and a discipline process must be taken to ensure that data is altered by authorized people. These measures include file permissions and user access controls. Along with this, some means must be there to detect the changes in data that might arise due to non-human-caused events such as an electromagnetic pulse (EMP) or server crash. Data integrity is achieved by including check sums and meta data of the files. Backups or redundancies must be available to restore the affected data to its exact state.

5) Data isolation : In multi-tenant nature of cloud infrastructure, the resources i.e., servers, clouds, storage are shared by multiple organizations which minimizes the cost for these, but puts an organization data in risk, as it may go to other competitors or wrong hands. Each client data must be separated from others with clear boundaries. Cloud need to assure that only all data in cloud is completely secure and accessible only by authorized users.

6) Accessibility of data: When users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data protected against untrusted servers, data must be accessed by authorized users. Access control actually still remains unresolved in this distributed cloud environment because consumers are handovering their data to cloud providers for carrying their business processes. Cloud needs a user central access control where every user request to any service provider is bound with the user identity and entitlement information. The identity is tied to a domain, but is portable because employees may be changed or their positions may change. User centric approach leaves the user with the ultimate control of their digital identities. [4]

7) Sniffing of data on the Network:Sensitive information is acquire from many organizations to the cloud, processed by Saas application and stored at the Saas vendor. Every time data in transit over the network so, it needs to be protected from hackers. Malicious users may get the advantage of weakness of network security issues to sniff the data packets. Active sessions may hijack, hacker may get access to user credentials and important data. This requires strong encoding techniques such as SSL and TLS for securing the data on network.

8) Authentication, authorization and identity management: In cloud computing application software and databases are moving to the centralized large data centers, identity management and authentication are very essential in cloud computing [4].Verification of eligible users' identification and protecting such credentials are part of authentication and authorization issues in the cloud - violation of this could lead to undetected security reach todata, some extent for some period. The authentication for the cloud users can be done either by the cloud service provider or by third party specialists (Gonzalez, Miers, Redigolo, Simplicio, Carvalho, Naslund & Pourzandi, 2012; Sharma & Mittal, 2013). Account and service hijacking involves data manipulation and software vulnerabilities where attackers get credentials and gain unauthorized access to application servers, data centers.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

This unauthorized access is a danger to integrity, confidentiality and availability of data and services. Unauthorized access can be from inside or outside the organization. Harmful insiders such as dishonest administrators severely impact organizations' security, for their level of access they go beyond and gain access to corporate data and cause damage to organization. Therefore, it is critical for cloud customers to clearly determine the guarantees that the cloud providers use to detect and defend against insider threats. The current authentication mechanisms may not be applicable in cloud environments as customers no longer belong to or are able to access a single tightly controlled system [5]. Unauthorized access becomes possible through browser vulnerabilities. Therefore, Internet browser is the first stage where security measures should be considered because vulnerabilities in the browser open the door for many follow-on attacks. Identity management deals with identifying individuals uniquely and controlling their accessibilities to shared resources by referring constraints on their IDs [6].The problems may arise due to replicated IDs, this must be controlled to secure the user data.

9) Web application security:Attacks targeting applications, software and services were more common on the web. Webapplications and Saas are tightly coupled for providing the efficient services to the end users. Threats on web applications are easily launched through automated tools and should be a top concern for an organization that is serious about security in cloud". Mostly attackers using the web to hack user's computers and perform malicious activities such as lift sensitive data [7]. The Open Web Application Security Project (OWASP) has documented the major serious web applications security threats [9].Those threats are

- SQL injection
- Cross-Site Scripting hits
- Denial of Service
- Buffer Overflows anomalies
- Session Hijacking
- Insufficient transport layer security

10) Vulnerability in virtualization:The aim of virtualization is to utilize the IT resources such as storage, processor and network to maximum extent and to decrease the cost of IT resources, which can be accomplished by combining various idle resources into common pools and creating different virtual machines to carry out various tasks concurrently. Present Virtual Machine Monitor (VMM) do not present perfect segregation of physical machines. For example, the vulnerability in virtualization some times allows a guest operating system user to run code on host or another guest operating system. An efficient separation, inspection and interposition is yet to be accomplished in Virtual Machine Monitors (VMMs).

Security threats [9] in virtualization are classified as follows

- Virtualization Capacity Planning
- Virtual Machine Threat
- Vm Sprawl,
- Hypervisor Threat
- Virtual Infrastructure
- Virtual Network Threat.
- Virtualization Backup And Recovery
- Vm Stall

11) Availability:Saas must assure for services 24/7 around the clock. Availability can be guarantee by carefully maintaining both hardware and software, performing hardware repairs instantaneously when necessary and maintaining a appropriately functioning operating system environment that is free of software complexities. It's also important to keep current with all necessary system improvements, providing sufficient communication bandwidth and preventing the occurrence of blockage are very important. Redundancy, failover, denial-of-service (DoS) attacks,RAID, and network intrusions can lead to serious consequences when hardware issues occur. Fast disaster recovery is essential. Safeguards must include against data loss or disruption in connections, even for unpredictable actions such as natural disasters and fire. To avoid data loss from such occurrences, a backup copy must be stored in various locations, possibly fireproof, waterproof safe.

12) Backup:cloud backup provider for data protection has a number of key advantages, such as scalability; freedom from day-to-day management; and potential cost savings on bandwidth, compared with writing data between multiple sites. But using a cloud backup provider also comes with drawbacks, such as latency issues and handing data over to third parties for safekeeping.

Disadvantages: The first one is latency. There's an issue with latency into the cloud. This is less of an issue when we backup small amount of data but matters when data in large in size. Second disadvantage is that consumers handover their data to a third party for protection, but these backups may not be in encrypted form, they must encrypt the backups before submit to them. The final disadvantage is that generally consumer reliant on that cloud backup provider, what happens if that provider goes out of business, how do the data get back?

B. Security issues in PaaS:

Platform as a service' (PaaS) is the delivery the computing platform , facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and softwares [10].Deploying and delivering web applications and services completely accessible from the Internet—with no downloads or installation of software's by end-users. PaaS depends on a safe and consistent network and secure web browser. PaaS application security consists of two software layers: Security of the PaaS platform i.e., runtime engine, and Security of PaaS platform on which customer applications are deployed [11].

PaaS brings data security challenges that are described as follows:

1) Web hosted development tools and Third-party relationships: Along with the traditional programming languages, Paas also offer third-party web services Mashups (A mash-up is a Web page or application that

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

integrates complementary elements from two or more sources in to single unit)[11,12].Thus, PaaS models also become heir to security issues related to Mashups such as data and network security [13].

2) PAAS Vendor Lock In: PaaS vendors may take over the control of storage and application framework used by applications, what happens to the organizations which require the infrastructure to run their apps.

3) Rapid application change: Developers face the difficulty of building secure applications those are to be hosted in the cloud. The rapid application change in the cloud will have an effect on both the security and System Development Life Cycle (SDLC) [14]. Developers should have knowledge about upgraded applications frequently, to keep up changes with their applications [15]. Besides this, developers have to be knowledgeable about data legal issues as well, so that data stored on different places with different legal rules that can compromise its privacy and security.

4) Business stability arrangement and Disaster Recovery with PAAS vendor: If cloud computing platform, suffers with an outage what happens to enterprise been using the service, how would the outage have affected the organization's ability to conduct business whose responsibility to fix it is the major question.

5) Underlying infrastructure security: In PaaS, developers do not have access to the core layers of cloud, so CSP (cloud service providers) need to secure the underlying infrastructure as well as the applications services [16]. Even though the developers have control of their applications, they are not sure about the security of the development tools which provided by a PaaS provider. PaaS offers development tools to create SaaS applications. In both SaaS and PaaS, security of the data while it is being processed, transmitted and located depends on the provider which is a major issue.

C .Infrastructure-as-a-service (IaaS) security issues:

Infrastructure as a service (IaaS) is a delivery model which rent cloud infrastructure such as servers, storage and networking on demand, in a pay-per-use model for clients. Infrastructure as a Service (IaaS) is also called as Hardware as a Service (HaaS). IaaS provides all these resources in the form of virtualized systems, which are accessed through the Internet [14]. Iaas consists of several components - Utility Computing (UC), Service Level Agreement (SLA), Platform Virtualization, Networks and Internet Connectivity, and Computer Hardware, but applying them in out-sourced and shared environment carry several threats, violating the security of any of the component will collapse the entire system. Users can run any thing with full control and management on the resources allotted to them. When compared to other models (Saas, Paas), IaaS cloud users have better control over the security unless there is a problem with the virtual machine monitor [16]. Users must have the ability to configure security policies correctly to secure their infrastructure. Only the underlying network, and storage infrastructure is managed by cloud providers. IaaS providers must have the strong secure mechanisms to decrease the threats which result from modification, communication, monitoring and mobility [17].

The following are some of the security threats associated to IaaS.

1) Attacks on Virtualization:Virtualizationpermits users to create new layer on physical resources, a virtual version of something--such as an operating system, a server, a storage device or network resources to run their applications. Thisextra layer brings the chance for attackers to attack the physical machine[17].Virtualized environments are weak to all types of attacks than normal infrastructures, security is a major challenge as virtualization allows to create more instances and more interconnection complexity[19] . Unlike physical servers, VMs have two boundaries: physical and virtual [18].A malicious virtual machine can be easily migrated to other host (with another VMM) compromising it.

2) Weak SLAs:SLA assures acceptance level of QOS from provider to customers, SLA defines contract definition, negotiation, monitoring and enhancement of resources. Contract definition and negotiation is very important to know the benefits and responsibilities for each party. The lack of standardization in cloud-based services leads to lack of clarity in the service level agreements offered by different providers, it will affect the security, leave the client exposure to vulnerabilities.

3) Vulnerabilitythrough Sharedresources: Same server can share CPU, memory, I/O, and other resources to multiple virtual machines based on it. Sharing resources between VMs may cause the breach to other VM. A malicious VM may go for cross communication with other VMs through shared memory [20]. Using covert channels, any two VMs can communicate bypassing all the laws defined by the security module of the VMM [21]. A malicious Virtual Machine can also monitor shared resources without being noticed by its VMM, with this hole attacker can get information about other virtual machines.

4) Virtualmachine life cycle:VMs can be on, off, or suspended by malicious codeit is much difficult to detect malware, even when virtual machines are offline, they can be danger because a virtual machine can be instantiated using an image that may contain malicious code. These malicious images, maliciouscode can be injected within other virtual machines in the creation process.

5) Data Loss and Leakage in IaaS infrastructure:Both private and public cloud needs strong monitoring system. This is essential because IaaS deployed in public cloud will allow the multiple users to share the data; it is not known that who is accessing the information, how it is accessed, and location from where it is accessed and what happened to accessed information later. To avoid this it needs a strong data protection, authentication and authorization techniques.

IV. CONCLUSION

Today, we have the ability to utilize scalable and reliable computing with the help of grid computing, distributed as well cloud computing environments within the confines of

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

the Internet. The initiation in cloud computing was foreseen its immense power relying on end users ranging from individuals and upcoming businesses organisations to Fortune 500 firms along with government sectors. In the progress of this computing on a large scale, the proactive measures must be taken to ensure security as it presents an extension of harms heretofore educated with the Internet.

REFERENCES

[1] Buyya R,Yeo CS,Venugopal S,Broberg J,Brandic I. Cloud computing and emerging IT platforms: vision hype and reality for delivering It services as 5thutility. future generation of computer systems 2009;25:599-616
[2] https://www.mendix.com/.
[3] U.S. Patriot Act. It was recently revealed that U.S.-based cloud providers may have to comply with Patriot Act requests for data that's located in a provider's European data centers, even though this conflicts with the European Union's 1995 Data Protection Directive.
[4] VeriSign, "Digital ID, A Brief Overview", A VeriSign White Paper, 2004 VeriSign, http://www.verisign.com/static/005326.pdf.
[5] Angin.P and Bhargav.B et.all... "An Entity-centric Approach for Privacy and Identity Management in Cloud Computing" Department of computer science Purude University West Lafayette. IN .USA.
[6] Kim & Hong, 2012; Emam, 2013; Han, Susilo & Mu, 2013; Yassin, Jin, Ibrahim, Qiang & Zou, 2012.
[7] Owens D (2010) Securing elasticity in the Cloud. Commun ACM 53(6):46–51
[8] OWASP (2010) The Ten most critical Web application Security risks.Available:https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Projects
[9] TimurMirzoev, Baijian Yang, "Securing Virtualized Datacenters", International journal of Engineering Research & Innovation, vol. 2, no. 1, spring 2010.
[10] http://www.cloudsecurityalliance.org/
[11] 10. Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA
[12] Keene C (2009) The Keene View on Cloud Computing. Online. Available:http://www.keeneview.com/2009/03/what-is-platform-as-service-paas.html.Accessed: 16-Jul-2011
[13] Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing.In: Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, pp 36–42
[14] 13. Xu K, Zhang X, Song M, Song J (2009) Mobile Mashup: Architecture,Challenges and Suggestions. In: International Conference on Management and Service Science. MASS'09. IEEE Computer Society, Washington, DC, USA,pp 1–4 Morsy MA, Grundy J, Müller I (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. APSEC,Sydney, Australia Chandramouli R, Mell P (2010) State of Security readiness. Crossroads 16(3):23–25
[15] [Sailer05] R. Sailer, E. Valdez, T. Jaeger, R. Perez, L. Doorn, J. Griffin, S. Berger, â€œsHype: Secure Hypervisor Approach to TrustedVirtualized Systems,â€• IBM, 2005. http://domino.watson.ibm.com/library/cyberdig.nsf/3addb4b88e7a231f85256b3600727773/265c8e3a6f95ca8d85256fa1005cbf0f
[16] [Garfinkel05] T. Garfinkel, M. Rosenblum, â€œWhen Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments,â€• USENIX Association, 2005. http://www.stanford.edu/~talg/papers/HOTOS05/virtual-harder-hotos05.pdf
[17] 47. Venkatesha S, Sadhu S, Kintali S (2009) Survey of virtual machine migration techniques., Technical report, Dept. of Computer Science, University of California, Santa Barbara. http://www.academia.edu/760613/Survey_of_Virtual_Machine_Migration_Techniques
[18] Hashizume K, Yoshioka N, Fernandez EB (2013) Three misuse patterns for Cloud Computing. In: Rosado DG, Mellado D, Fernandez-Medina E, Piattini M (ed) Security engineering for Cloud Computing: approaches and Tools. IGI Global, Pennsylvania, United States, pp 36–53 Ranjith P, Chandran P, Kaleeswaran S (2012) On covert channels between virtual machines. Journal in Computer Virology Springer 8:85–97
[19]
[20]

BIOGRAPHIES

G. Kalpana, Research Scholar for JNTU, Hyderabad working as a Assistant Professor. The area of research is Cloud computing.

Dr.P.V.Kumar, Professor, Dept of C.S.E, Osmania College of Engineering. O.U, Hyderabad, India. He received the Ph.D Degree. His areas of interests include Databases.

Dr.R.V.Krishniah, Dean, Dept of C.S.E, Institute of Aeronautical Engineering, Hyderabad, India. He received the Ph.D Degree. His areas of interests include Database Networks, Cloud computing.