Indian J.Sci.Res. 17(2): 559-568, 2018

ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

DATA PROTECTION AND SECURITY ISSUES IN CLOUD PLATFORM

[1]N.Phani Lalithendra, [2]S Shalini
[1,2] Department of Computer Science and Engineering, Aurora's Scientific, Technological and Research Academy, Hyderabad.

Abstract - In Cloud computing is Platform for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.

Keywords- Security Issues, Cloud Security, Cloud Architecture, Data Protection, Cloud Platform, Grid Computing

I. Introduction

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) both offer services. Cloud computing is a model that enables convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications that can be rapidly provisioned and released with minimal management effort or service provider's interaction. In general cloud providers offer three types of services i.e. Software as a Service (SaaS),

Clouds are the new trend in the evolution of the distributed systems, the predecessor of cloud being the grid. The user does not require knowledge or expertise to control the infrastructure of clouds; it provides only abstraction. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing power. Cloud computing providers deliver common online business applications which are accessed from servers through web browser [2].

II. Cloud Computing Blocks

A. Different models of cloud computing

Generally cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Software-as-a-Service (SaaS): SaaS can be described as a process by which Application Service Provider (ASP) provides:

The developers to concentrate on the business value rather on the starting budget. The clients of commercial clouds rent computing power (virtual machines) or storage space (virtual space) dynamically, according to the needs of their business. With the exploit of this technology, users can access heavy applications via lightweight portable devices such as mobile phones, PCs and PDAs. Amazon, Google, Yahoo! and Salesforce.com. This makes it possible for new startups to enter the market easier, since the cost of the infrastructure is greatly diminished.

Figure 1. High Level View of Cloud Computing Architecture

[1]Corresponding Author

Platform as a Service (PaaS): "PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure.

Infrastructure as a Service (IaaS): Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Examples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid.

There are also four different cloud deployment models namely Private cloud, Public cloud, Hybrid cloud and Community cloud. Details about the models are given below.

Private cloud: Private cloud can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems [4].

Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party and exist beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud includes Microsoft Azure, Google App Engine.

B. Cloud computing entities

Cloud providers and consumers are the two main entities in the business market. But, service brokers and resellers are the two more emerging service level entities in the Cloud world. These are discussed as follows

Cloud Providers: Includes Internet service providers, telecommunications companies, and large business process outsourcers that provide either the media (Internet connections) or infrastructure (hosted data centers) that enable consumers to access cloud services. Service providers may also include systems integrators that build and support data centers hosting private clouds and they offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to the consumers, the service brokers or resellers [6].

Cloud Service Brokers: Includes technology consultants, business professional service organizations, registered brokers and agents, and influencers that help guide consumers in the selection of cloud computing solutions. Service brokers concentrate on the negotiation of the relationships between consumers and providers without owning or managing the whole Cloud infrastructure. Moreover, they add extra services on top of a Cloud provider's infrastructure to make up the user's Cloud environment.

III. Cloud Computing Security Architecture

Security within cloud computing is an especially worrisome issue because of the fact that the devices used to provide services do not belong to the users themselves. The users have no control of, nor any knowledge of, what could happen to their data. This is a great concern in cases when users have valuable and personal information stored in a cloud computing service. Users will not compromise their privacy so cloud computing service providers must ensure that the customers' information is safe. This, however, is becoming increasingly challenging because as security developments are made, there always seems to be someone to figure out a way to disable the security and take advantage of user information. Some of the important components of Service Provider Layer are SLA Monitor, Metering, Accounting, Resource Provisioning, Scheduler& Dispatcher, Load Balancer, Advance Resource Reservation Monitor, and Policy Management. Some of the security issues related to Service Provider Layer are Identity, Infrastructure, Privacy, Data transmission, People and Identity, Audit and Compliance, Cloud integrity and

Binding Issues. Some of the important components of Virtual Machine Layer creates number of virtual machines and number of operating systems and its monitoring. Some of the security issues related to Virtual Machine Layer are VM Sprawl, VM Escape, Infrastructure, Separation between Customers, Cloud legal and Regularity issues, Identity and Access management Some of the important components of Data Center (Infrastructure) Layer contains the Servers, CPU's, memory, and storage, and is henceforth typically denoted as Infrastructure-as-a-Service (IaaS).

The specifications and test beds. Some of the existing standards and test bed groups are Cloud Security Alliance (CSA), Internet Engineering Task Force (IETF), Storage Networking Industry Association (SNIA) etc. On the other side, a cloud API provides either a functional interface or a management interface (or both). Cloud management has multiple aspects that can be standardized for interoperability. Some possible standards are Federated security (e.g., identity) across clouds, Metadata and data exchanges among clouds, Standardized outputs for monitoring, auditing, billing, reports and notification for cloud applications and services, Cloud-independent representation for policies and governance etc., Figure 2 showing the high level view of the cloud computing security architecture.

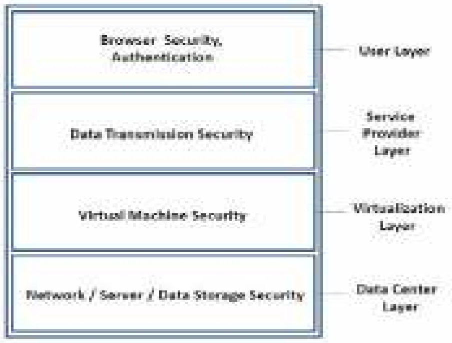
Browser Security, Authentication
User Layer
Data Transmission Security
Service Provider Layer
Virtual Machine Security
Virtualization Layer
Network / Server / Data Storage Security
Data Center Layer

Figure 2. High Level Security Architecture of Cloud Computing

IV. Security Issues In Cloud Computing

Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs different operations and offers different products for businesses and individuals around the world. The business application includes Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Integration. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

Access to Servers & Applications: In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections which is not the case of cloud data centers. In cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data. In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. Some organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users [9].

Data Transmission: Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here. In Cloud environment most of the data is not encrypted in the processing time. But to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

Virtual Machine Security: Virtualization is one of the main components of a cloud. Virtual machines are dynamic i.e it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. They can also be readily cloned and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. Full Virtualization and Para Virtualization are two kinds of virtualization in a cloud computing paradigm. In full virtualization, entire hardware architecture is replicated virtually. However, in para-virtualization, an operating system is modified so that it can be run concurrently with other operating systems. VMM (Virtual Machine Monitor), is a software layer that abstracts the physical resources used by the multiple virtual machines. The VMM provides a virtual processor and other virtualized versions of system devices such as I/O devices, storage, memory, etc. Many bugs have been found in all popular VMMs that allow escaping from Virtual machine. Vulnerability in Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system. Vulnerability was found in VMware's shared folders mechanism that grants users of a guest system read and write access to any portion of the host's file system including the system folder and other security-sensitive files. Vulnerability in Xen can be exploited by "root" users of a guest domain to execute arbitrary commands. The other issue is the control of administrator on host and guest operating systems. Current VMMs (Virtual Machine Monitor) do not offer perfect isolation. Virtual machine monitor should be 'root secure', meaning that no privilege within the virtualized guest environment permits interference with the host system.

Network Security: Networks are classified into many types like shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of DNS attacks, Sniffer attacks, issue of reused IP address, etc which are explained in details as follows.

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems.

Data security: For general user, it is quite easy to find the possible storage on the side that offers the service of cloud computing. To achieve the service of cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). In order to assure the information security and data integrity, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are the most common adoption. In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in cloud computing, the enterprise data is stored outside the enterprise boundary, at the Service provider end. Consequently, the service provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. Cloud service providers such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host. All such accesses are logged and routinely audited. While the data at rest in Simple Storage Service (S3) is not encrypted by default, users can encrypt their data before it is uploaded to Amazon S3, so that it is not accessed or tampered with by any unauthorized party [13].

Data Privacy: The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. Requirement: This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks [14].

Data Integrity: Data corruption can happen at any level of storage and with any type of media, So Integrity monitoring is essential in cloud storage which is critical for any data center. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control.

Data Location: In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. Next in the complexity chain are distributed systems. In a distributed system, there are multiple databases and multiple applications [15].

Data Availability: Data Availability is one of the prime concerns of mission and safety critical organizations. When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider. If the Cloud goes out of operation, data will become unavailable as the data depends on a single service provider. The Cloud application needs to ensure that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan for business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies.

Data Segregation: Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data. Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals [16].

Securing Data-Storage: Data protection is the most important security issue in Cloud computing. In the service provider's data center, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. Encryption keys share securely between Consumer and the cloud service provider and encryption of mobile media is an important and often overlooked need. PaaS based applications, Data-at-rest is the economics of cloud computing and a multitenancy architecture used in SaaS. In other words, data, when stored for use by a cloud-based application or, processed by a cloud -based application, is commingled with other users' data. In cloud computing, data co-location has some significant restrictions. In public and financial services areas involving users and data with different risks. The cloud-wide data classification will govern how that data is encrypted, who has access and archived, and how technologies are used to prevent data loss. At the cloud provider, the best practice for securing data at rest is cryptographic encryption and shipping self encrypting is used by hard drive manufacturers. Self-encrypting provides automated encryption with performance or minimal cost impact [17].

Patch Management: The self-service nature of cloud computing may create confusion for patch management efforts. Once an enterprises subscribes to a cloud computing resource—for example by creating a Web server from templates offered by the cloud computing service provider—the patch management for that server is no longer in the hands of the cloud computing vendor, but is now the responsibility of the subscriber. Keeping in mind that according to the previously mentioned Verizon 2008 Data Breach Investigations Report, 90% of known vulnerabilities that were exploited had patches available for at least six months prior to the breach, organizations leveraging cloud computing need to keep vigilant to maintain cloud resources with the most recent vendor supplied patches. If patching is impossible or unmanageable, compensating controls such as "virtual patching" need to be considered.

V. Challenges In Cloud Computing

Cloud Computing research addresses the challenges of meeting the requirements of next generation private, public and hybrid cloud computing architectures, also the challenges of allowing applications and development platforms to take advantage of the benefits of cloud computing. The research on cloud computing is still at an early stage. Many existing issues have not been fully addressed, while new challenges keep emerging from industry applications. Some of the challenging research issues in cloud computing are given below.

- Service Level Agreements (SLA's)
- Cloud Data Management & Security
- Data Encryption
- Migration of virtual Machines
- Interoperabilit
- Access Controls
- Energy Management
- Server Consolidation
- Reliability & Availability of Service
- Common Cloud Standards
- Platform Management

Cloud Data Management: Cloud data Can be very large (e.g. text-based or scientific applications), unstructured or semi-structured, and typically append-only with rare updates Cloud data management an important research topic in cloud computing. Since service providers typically do not have access to the physical security system of data centers, they must rely on the infrastructure provider to achieve full data security. Even for a virtual private cloud, the service provider can only specify the security setting remotely, without knowing whether it is fully implemented. The infrastructure provider, in this context, must achieve the objectives like confidentiality, audit ability. Confidentiality, for secure data access and transfer, and audit ability, for attesting whether security setting of applications has been tampered or not. Confidentiality is usually achieved using cryptographic protocols, whereas audit ability can be achieved using remote attestation techniques. However, in a virtualized environment like the clouds, VMs can dynamically migrate from one location to another; hence directly using remote attestation is not sufficient. In this case, it is critical to build trust mechanisms at every architectural layer of the cloud. Software frameworks such as Map Reduce and its various implementations such as Hadoop are designed for distributed processing of data-intensive tasks, these frameworks typically operate on Internet-scale file systems such as GFS and HDFS. These file systems are different from traditional distributed file systems in their storage structure, access pattern and application programming interface. In particular, they do not implement the standard POSIX interface, and therefore introduce compatibility issues with legacy file systems and applications. Several research efforts have studied this problem [18].

Data Encryption: Encryption is a key technology for data security. Understand data in motion and data at rest encryption. Remember, security can range from simple (easy to manage, low cost and quite frankly, not very secure) all the way to highly secure (very complex, expensive to manage, and quite limiting in terms of access). You and the provider of your Cloud computing solution have many decisions and options to consider. For example, do the Web services APIs that you use to access the cloud, either programmatically, or with clients written to those APIs, provide SSL encryption for access, this is generally considered to be a standard. Once the object arrives at the cloud, it is decrypted, and stored. Is there an option to encrypt it prior to storing? Do you want to worry about encryption before you upload the file for cloud computing or do you prefer that the cloud computing service automatically do it for you? These are options, understand your cloud computing solution and make your decisions based on desired levels of security.

Migration of virtual Machines: applications are not hardware specific; various programs may run on one machine using virtualization or many machines may run one program. Virtualization can provide significant benefits in cloud computing by enabling virtual machine migration to balance load across the data center. In addition, virtual machine migration enables robust and highly responsive provisioning in data centers. Virtual machine migration has evolved from process migration techniques. More recently, Xen and VMware have implemented "live" migration of VMs that involves extremely short downtimes ranging from tens of milliseconds to a second. The major benefits of VM migration are to avoid hotspots; however, this is not straightforward. Currently, detecting workload hotspots and initiating a migration lacks the ability to respond to sudden workload changes. Moreover, the in memory state should be transferred consistently and efficiently, with integrated consideration of resources for applications and physical servers [19].

Access Controls: Authentication and identity management is more important than ever. And, it is not really all that different. What level of enforcement of password strength and change frequency does the service provider invoke? What is the recovery methodology for password and account name? How are passwords delivered to users upon a change? What about logs and the ability to audit access? This is not all that different from how you secure your internal systems and data, and it works the same way, if you use strong passwords, changed frequently, with typical IT security processes, you will protect that element of access.

Energy Resource Management: Significant saving in the energy of a cloud data center without sacrificing SLA are an excellent economic incentive for data center operators and would also make a significant contribution to greater environmental sustainability. It has been estimated that the cost of powering and cooling accounts for 53% of the total operational expenditure of data centers. The goal is not only to cut down energy cost in data centers, but also to meet government regulations and environmental standards. Designing energy-efficient data centers has recently received considerable attention. This problem can be approached from several directions. For example, energy efficient hardware architecture that enables slowing down CPU speeds and turning off partial hardware components has become commonplace. Energy-aware job scheduling and server consolidation are two other ways to reduce power consumption by turning off unused machines. Recent research has also begun to study energy-efficient network protocols and infrastructures. A key challenge in all the above methods is to achieve a good trade-off between energy savings and application performance. In this respect, few researchers have recently started to investigate coordinated solutions for performance and power management in a dynamic cloud environment. The Global Energy Management Center (GEMC) can help companies monitor energy consumption patterns from multiple sources. These patterns can be further analyzed for usage, cost, and carbon footprint in a number of ways that help in optimizing energy. The center is uniquely positioned to service the clients across the globe by deploying a Remote Control Unit that has the capabilities to communicate to a cloud-based architecture [20].

Multi-tenancy: There are multiple types of cloud applications that users can access through the Internet, from small Internet-based widgets to large enterprise software applications that have increased security requirements based on the type of data being stored on the software vendor's infrastructure. These application requests require multi-tenancy for many reasons, the most important is cost. Multiple customers accessing the same hardware, application servers, and databases may affect response times and performance for other customers. For application-layer multi-tenancy specifically, resources are shared at each infrastructure layer and have valid security and performance concerns. For example, multiple service requests accessing resources at the same time increase wait times but not necessarily CPU time, or the number of connections to an HTTP server has been exhausted, and the service must wait until it can use an available connection or—in a worst-case scenario—drops the service request [21].

Server consolidation: The increased resource utilization and reduction in power and cooling requirements achieved by server consolidation are now being expanded into the cloud. Server consolidation is an effective approach to maximize resource utilization while minimizing energy consumption in a cloud computing environment. Live VM migration technology is often used to consolidate VMs residing on multiple under-utilized servers onto a single server, so that the remaining servers can be set to an energy- saving state. The problem of optimally consolidating servers in a data center is often formulated as a variant of the vector bin -packing problem, which is an NP-hard optimization problem. Various heuristics have been proposed for this problem. Additionally, dependencies among VMs, such as communication requirements, have also been considered recently. However, server consolidation activities should not hurt application performance. It is known that the resource usage (also known as the footprint) of individual VMs may vary over time. For server resources that are shared among VMs, such as bandwidth, memory cache and disk I/O, maximally consolidating a server may result in resource congestion when a VM changes its footprint on the server. Hence, it is sometimes important to observe the fluctuations of VM footprints and use this information for effective server consolidation. Finally, the system must quickly react to resource congestions when they occur.

Reliability & Availability of Service: The challenge of reliability comes into the picture when a cloud provider delivers on-demand software as a service. The software needs to have a reliability quality factor so that users can access it under any network conditions (such as during slow network connections). There are a few cases identified due to the unreliability of on-demand software. One of the examples is Apple's MobileMe cloud service, which stores and synchronizes data across multiple devices. It began with an embarrassing start when many users were not able to access mail and synchronize data correctly. To avoid such problems, providers are turning to technologies such as Google Gears, Adobe AIR, and Curl, which allow cloud based applications to run locally, some even allow them to run in the absence of a network connection. These tools give web applications access to the storage and processing capabilities of the desktop, forming a bridge between the cloud and the user's own computer. Considering the use of software such as 3D gaming applications and video conferencing systems, reliability is still a challenge to achieve for an IT solution that is based on cloud computing [22].

Common Cloud Standards: Security based accreditation for Cloud Computing would cover three main areas which are technology, personnel and operations. Technical standards are likely to be driven by organizations, such as, Jericho Forum1 before being ratified by established bodies, e.g., ISO2 (International Standard Organization). On the personnel side, the Institute for Information Security Professionals3 (IISP) is already offering formal accreditation for the security professionals. For the operational elements, there are some workable solutions such as tweaking the ISO 27001 and using it as the default measurement standard within the framework of the SAS 704. Currently, one of the main problems is that there are many fragmented activities going in the direction of Cloud accreditation, but a common body for the coordination of those activities is missing. The creation of a unified accreditation body to certify the Cloud services would also be a big challenge [23].

VI. Conclusion

Challenges in delivering middleware capabilities for building, deploying, integrating and managing applications in a multi-tenant, elastic and scalable environments. One of the most important parts of cloud platforms provide various kind of platform for developers to write applications that run in the cloud, or use services provided from the cloud, or both. Different names are used for this kind of platform today, including on-demand platform and platform as a service (PaaS). This new way of supporting applications has great potential. When a development team creates an on-premises application (i.e., one that will run within an organization), much of what that application needs already exists. An operating system provides basic support for executing the application, interacting with storage, and more, while other computers in the environment offer services such as remote storage.

We believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture. As the development of cloud computing technology is still at an early stage, we hope our work will provide a better understanding of the design challenges of cloud computing, and pave the way for further research in this area.

References

[1] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[3] R. L Grossman, “The Case for Cloud Computing,” IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[4] B. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[5] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, “On technical Security Issues in Cloud Computing,” Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[6] Pring et al., “Forecast: Sizing the cloud; understanding the opportunities in cloud services,” Gartner Inc., Tech. Rep. G00166525, March 2009.

[7] Aman Bakshi, Yogesh B. Dujodwala, “Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine,” ICCSN ’10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[8] B. R. Kandukuri, R. V. Paturi and A. Rakshit, “Cloud Security Issues,” 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

[9] K. Hwang, S Kulkarni and Y. Hu, “Cloud security with virtualized defence and Reputation-based Trust management,” Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695-3929 -4.

[10] R. Gellman, “Privacy in the clouds: Risks to privacy and confidentiality from cloud computing,” The World Privacy Forum,2009.http://www.worldprivacyforum.org/pdf/WPF_Cloud_ Privacy_Report.pdf.

[11] Ohlman, B., Eriksson, A., Rembarz, R. (2009) What Networking of Information Can Do for Cloud Computing. The 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, Groningen, The Netherlands, June 29 - July 1, 2009

[12] L.J. Zhang and Qun Zhou, “CCOA: Cloud Computing Open Architecture,” ICWS 2009: IEEE International Conference on Web Services, pp. 607-616. July 2009.

[13] Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An

Enterprise Perspective on Risks and Compliance, O' Reilly Media, USA, 2009.

[14] Ronald L. Krutz, Russell Dean Vines "Cloud Security A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc.,2010

[15] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

[16] Marios D. Dikaiakos, Dimitrios Katsaros, Pankaj Mehra, George Pallis, Athena Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009. DOI: 10.1109/MIC.2009.103.