compatibility is eliminated.

- SaaS has the capacity to support multiple users.

In spite of the above benefits, there are some drawbacks of SaaS. For example, SaaS is not suited for applications that need real - time response where there is a requirement for data to be hosted externally.

3.5 Architectural Design Challenges

The cloud architecture design plays an important role in making cloud services successful in all aspects, but still it has some challenges. The major challenges involved in architectural design of cloud computing are shown in Fig. 3.5.1 and explained as follows.

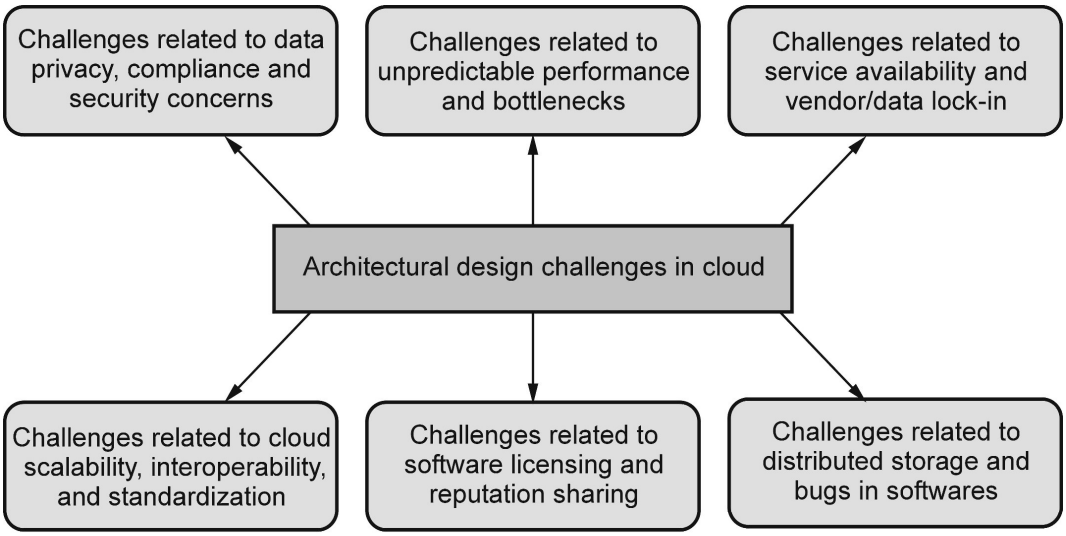

Fig. 3.5.1 : Architectural design challenges in cloud

3.5.1 Challenges related to Data Privacy, Compliance and Security Concerns

Presently, most of the cloud offerings are basically runs on public networks which renders the infrastructure more susceptible to attack. The most common attacks on the network include buffer overflows, DoS attacks, spyware, malware, root kits, trojan horses and worms. With well-known technologies such as encrypted data, virtual LANs and network middleboxes such as firewalls, packet filters etc., many challenges can be solved immediately. Newer attacks may result from hypervisor malware, guest hopping and hijacking or VM rootkits in a cloud environment. Another form of attack on VM migrations is the man-in-the-middle attack. The passive attacks typically steal personal data or passwords while active attacks can exploit data structures in the kernel that will cause significant damage to cloud servers.

To protect from cloud attacks, one could encrypt their data before placing it in a cloud. In many countries, there are laws that allow SaaS providers to keep consumer data and copyrighted material within national boundaries that also called as compliance or regulatory standards. Many countries still do not have laws for compliance; therefore, it is indeed required to check the cloud service providers SLA for executing compliance for services.

3.5.2 Challenges related to Unpredictable Performance and Bottlenecks

In cloud computing, the cloud platform is responsible for deploying and running services on the top of resource pool which has shared hardware from different physical servers. In a production environment, multiple Virtual Machines (VMs) shares the resources with each other like CPU, memory, I/O and network. Whenever I/O devices are shared between VMs, it may generate a big challenge during provisioning due to I/O interfaced between them. It may generate an unpredicted performance and may result into system bottlenecks. The problem becomes wider when such I/O resources are pulled across boundaries of cloud. In such scenarios, the accessibility may become complicated for data placement and transport. To overcome that, data transfer bottlenecks must be removed, bottleneck links must be widened and weak servers in cloud infrastructure should be removed. One solution for this challenge is to improve I / O architectures and operating systems used in physical servers, so that interrupts and I / O channels can be easily virtualized.

3.5.3 Challenges related to Service Availability and Vendor/Data Lock-in

Due to popularity of cloud computing, many organizations run their mission critical or business critical applications on cloud with shared infrastructure provided by cloud service providers. Therefore, any compromise in service availability may result into huge financial loss. Therefore, managing a single enterprise cloud service is often leads to single failure points. The solution related to this challenge is use of multiple cloud providers. In such case, even if a company has multiple data centers located in different geographic regions, it may have common software infrastructure and accounting systems. Therefore, using multiple cloud providers may provide more protection from failures.

In such instances, even if an organization has several data centers located in various geographic regions the multiple cloud service providers can protect their cloud infrastructure and accounting systems and make them available continuously. The use of multiple cloud providers will also provide more protection against failures. Such implementation may ensure the high availability for the organizations. Distributed Denial

of Service (DDoS) attacks are another obstacle to availability. Criminals are trying to slash SaaS providers' profits by making their services out of control. Some utility computing services give SaaS providers the ability to use quick scale - ups to protect themselves against DDoS attacks.

In some cases, due the failure of a single company who was providing cloud storages the lock - in concern arises. As well as because of some vendor - lock in solutions of cloud services providers, organizations face difficulties in migrating to new cloud service provider. Therefor to mitigate those challenges related to data lock in and vendor lock in, software stacks can be used to enhance interoperability between various cloud platforms as well as standardize APIs to rescue data loss due to a single company failure. It also supports "surge computing" that has the same technological framework in both public and private clouds and is used to catch additional tasks that cannot be performed efficiently in a private cloud's data center.

3.5.4 Challenges related to Cloud Scalability, Interoperability and Standardization

In cloud computing, pay-as-you-go model refers to utility - based model where bill for storage and the bandwidth of the network are calculated according to the number of bytes used. Depending on the degree of virtualization, computation is different. Google App Engine scales and decreases automatically in response to load increases; users are paid according to the cycles used. Amazon Web Service charges the number of instances used for VM by the hour, even though the computer is idle. The potential here is to scale up and down quickly in response to load variability, to save money, but without breaching SLAs. In virtualization, the Open Virtualization Format (OVF) defines an open, secure, portable, effective and extensible format for VM packaging and delivery. It also specifies a format to be used to distribute the program in VMs. It also specifies a transportation framework for VM templates, which can refer to various virtualization platforms with different virtualization levels.

The use of a different host platform, virtualization platform or guest operating system does not depend on this VM format. The solution is to address virtual platform - agnostic packaging with bundled device certification and credibility. The package provides support for virtual appliances that span more than one VM. The ability of virtual appliances needs to be proposed to operate on any virtual platform in terms of cloud standardization to allow VMs to run hypervisors on heterogeneous hardware platforms. The cloud platform should also introduce live cross - platform migration between x86

Intel and AMD technologies and support legacy load balancing hardware to avoid the challenges related to interoperability.

3.5.5 Challenges related to Software Licensing and Reputation Sharing

Most of the cloud computing providers primarily depended on open source software, as the commercial software licensing model is not suitable for utility computing. The key opportunity is either to stay popular with open source, or simply to encourage commercial software companies to adjust their licensing structure to suit cloud computing better. One may consider using both pay-for-use and bulk licensing schemes to broaden the scope of the company. Bad conduct by one client can affect the credibility of the cloud as a whole. For example, In AWS, spam - prevention services can restrict smooth VM installation by blacklisting of EC2 IP addresses. An advantage would be to build reputation - guarding services similar to those currently provided through "trusted e-mail" providers for providers hosted on smaller ISPs. Another legal issue concerns the transfer of legal responsibility. Cloud services require consumers to remain legally accountable and vice versa. This problem needs to be solved at SLA level.

3.5.6 Challenges related to Distributed Storage and Bugs in Softwares

In cloud applications the database services continuously grow. The potential is to build a storage infrastructure that not only fulfills this growth but also blends it with the cloud benefit of scaling up and down dynamically on demand. That involves the design of efficiently distributed SANs. The data centers will meet the standards of programmers in terms of scalability, system reliability and HA. A major problem in cloud computing is data consistency testing in SAN - connected data centers. Large - scale distributed bugs cannot be replicated, so debugging must take place on a scale in the data centers for production. Hardly any data center will deliver that convenience. One solution may be to focus on using VMs in cloud computing. The virtualization level can allow valuable information to be captured in ways that are impossible without using VMs. Debugging on simulators is another way to fix the problem, if the simulator is well designed.

3.6 Cloud Storage

With the rise in the popularity of cloud computing, you may be wondering where and how the data is stored in the cloud. The model in which the digital data is stored in logical pools is a cloud storage. Your data is stored in an online repository. So, it is the responsibility of the storage service provider to take care of the data files. Take an example of the email service you are using, like Gmail, Yahoo etc. The emails you send or