Article can be accessed online at http://www.publishingindia.com

A Survey on Cloud Computing and Cloud Security

Rohit Handa*

Abstract

Cloud computing involves the delivery of computing as a service instead of a product. In cloud computing environment the resources are provided as a utility to the end users. End user's access the shared resources through internet. The two advantages of cloud are ease-of-use and cost-effectiveness. Despite of the advantages offered by cloud to the organizations there are still factors which inhibit the use of cloud. This paper explores the basics of cloud computing with introduction to security risks involved in it.

Index Terms-Cloud, Cloud Security, Cloud Deployment Models, Cloud Delivery Models, Cloud Security Boundaries, Cloud Computing Advantages, Cloud Computing Challenges

Keywords: Cloud, Cloud Security, Cloud Deployment Models, Cloud Delivery Models, Cloud Security Boundaries, Cloud Computing Advantages, Cloud Computing Challenges

Introduction

The word computing implies to the use of computer as a technology to complete a task. It may involve computer as hardware and/or software. Cloud computing is defined as a computing paradigm shift where computing is moved away from personal computers or an individual application server to a "cloud" of computers [1]. Cloud gives user the facility to pay-per-use, i.e., the services are charged based on the resources used. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. The idea of cloud computing is based on fundamental principal of reusability of IT capabilities.

So, in this paper, the aim is to study cloud computing along with the various challenges related to cloud computing and investigate the security issues related to cloud computing.

Rest of this paper is organized as follows. In Section II, we discuss the fundamental concepts of cloud. The security aspect of cloud is discussed in Section III. Finally, Section IV gives the concluding remarks of the paper.

Cloud Computing

Introduction to Cloud Computing

The US National Institute of Standards and Technology (NIST) [2] has developed a working definition that covers the commonly agreed aspects of cloud computing. The NIST working definition summarizes cloud computing as: *'A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'.*

Cloud provides an illusion of infinite storage to the users at limited setup and usage cost. It permits the user to perform computation intensive operations on the cloud and that too at multiple disparate locations [1]. The prime requirement for cloud usage is the availability of internet. As fast speed internet is available at lower costs the organizations are motivated to outsource their data on the

* *Lecturer, CSE Department, Baddi University of Emerging Sciences & Technology, Baddi, Himachal Pradesh, India.
E-mail: handarohit140@gmail.com

cloud. There are large number of cloud service providers namely VM ware, Microsoft, Google, Salesforce.com, Rackspace and Amazon [3]. The organizations can deploy a private cloud or may use a public cloud to store their data based on the sensitivity of the data, time to deploy cloud and the budget available [4]. As deploying public cloud involves less cost and time, many organizations prefer using a public cloud than setting up a private cloud.

Related Work

Jeffery Voas and Jia Zhang [5] presented the historical evolution of cloud computing. Initially mainframe technology existed where the users connected to a single powerful system to perform the desired task. Soon the power of personal computers increased so as to perform the routine jobs and the requirement of sharing a single mainframe system was no longer required. From single computer system a shift was made to multiple computer system where multiple computing resources were connected with each other to provide resource sharing. In single computing environment, the network was local which gradually expanded to global network via internet. Finally grids evolved which paved way for cloud computing which is an upcoming trend with significant impact on IT sector.

Luis M. Vaquero et al. [6] introduced the concept of cloud computing as a paradigm for provision of computing infrastructure. Cloud involves the migration of hardware and software infrastructure to the network so that the overall cost is reduced. According to the authors, SLA (Service Level Agreement) is very important as it is in the light of it that the desired QoS (Quality of Service) is provided to the consumers. The existing definitions in literature are analyzed and cloud according to the authors is defined as: "Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs". They have listed ten characteristics of cloud computing in their sum-up which are user friendliness, virtualization, internet centric, variety of resources, automatic adaptation, scalability, resource optimization, pay-per-use, service SLAs and infrastructure SLAs.

Lizhe Wang et al. [7] introduced various aspects of cloud computing, i.e., definitions, features and enabling technologies behind it. They presented the reasons due to which a single definition of cloud is not provided. The reasons for this are: (i) the technologies used to provide cloud services are evolving and are new technologies; (ii) the researchers work on cloud with different view points than the entrepreneurs; and (iii) cloud is still evolving and is not extensively used.

R. Buyya et al. [8] presented around nineteen characteristics of cloud along with the differences between cluster, grid and cloud computing. The characteristics listed are complex as compared to the other available in literature. In cluster computing, the resources are present under a single administrative domain whereas in cloud and grid the resources are located under multiple administrative domains. It can be concluded that cloud computing possesses characteristics of both cluster and grid and provides services to the consumers without knowing about the underlying infrastructure.

Chunye Gong et al. [9] compared cloud computing with grid computing and provided the characteristics of cloud which make it different from other computing techniques. Grid computing is based on High Performance Computing services whereas cloud is based on reliability of services. The characteristics of cloud are categorized into different domains as conceptional, technical, economical and user experience. The concepts of service oriented fall under conceptional domain. This concept is applied relatively more to cloud as compared to other computing techniques and is based on the idea of providing abstraction and accessibility through virtualization. Technical characteristics include loose coupling and strong fault tolerance. Virtualization is used to provide loose coupling as it isolates the virtual machines. Fault tolerance is provided at lower layers using specific hardware, at upper layer using specific software and at the middle layer using check points. In cloud computing, a fault may occur at the provider's end or at the user's end. Few methods to provide fault tolerance include redundancy of data, using the services of other providers by redirecting the request for resources or services and protecting the resources which are critical at different levels such as hardware, software and operating system. Economic characteristics under cloud computing is oriented towards profit as compared to grid which is oriented towards research. The entire user experience depends on the ease of use of

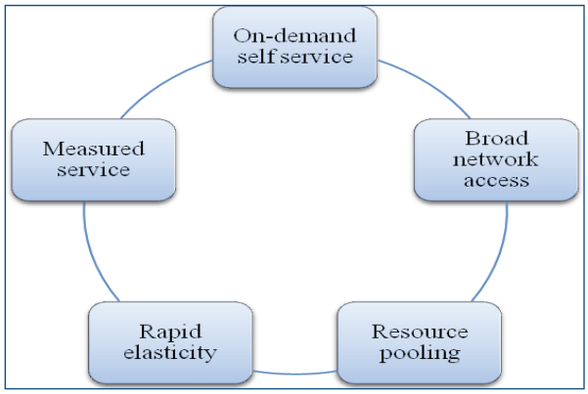
cloud. Cloud improves user experience as compared to other computing techniques.

E.B. Dudin and Yu. G. Smetanin [10] presented a review of cloud computing and stated that the success of cloud computing is based on three factors: (i) the ability to fulfill the needs of the potential users; (ii) the economic stability provided as the resources and services are available at reduced cost and (iii) the technological support provided to the customers by the cloud service provider (CSP). In comparison to relational databases, cloud is used for relatively simple queries. Cloud computing takes the benefit of open source technology as compared to closed source technology. It is also stated that the initial benefits of cloud can be realized for small and medium scale organizations.

Essential Characteristics

The essential characteristics of cloud computing as shown in Figure 1 are as under [3]:

Figure 1: Essential Characteristics Of Cloud



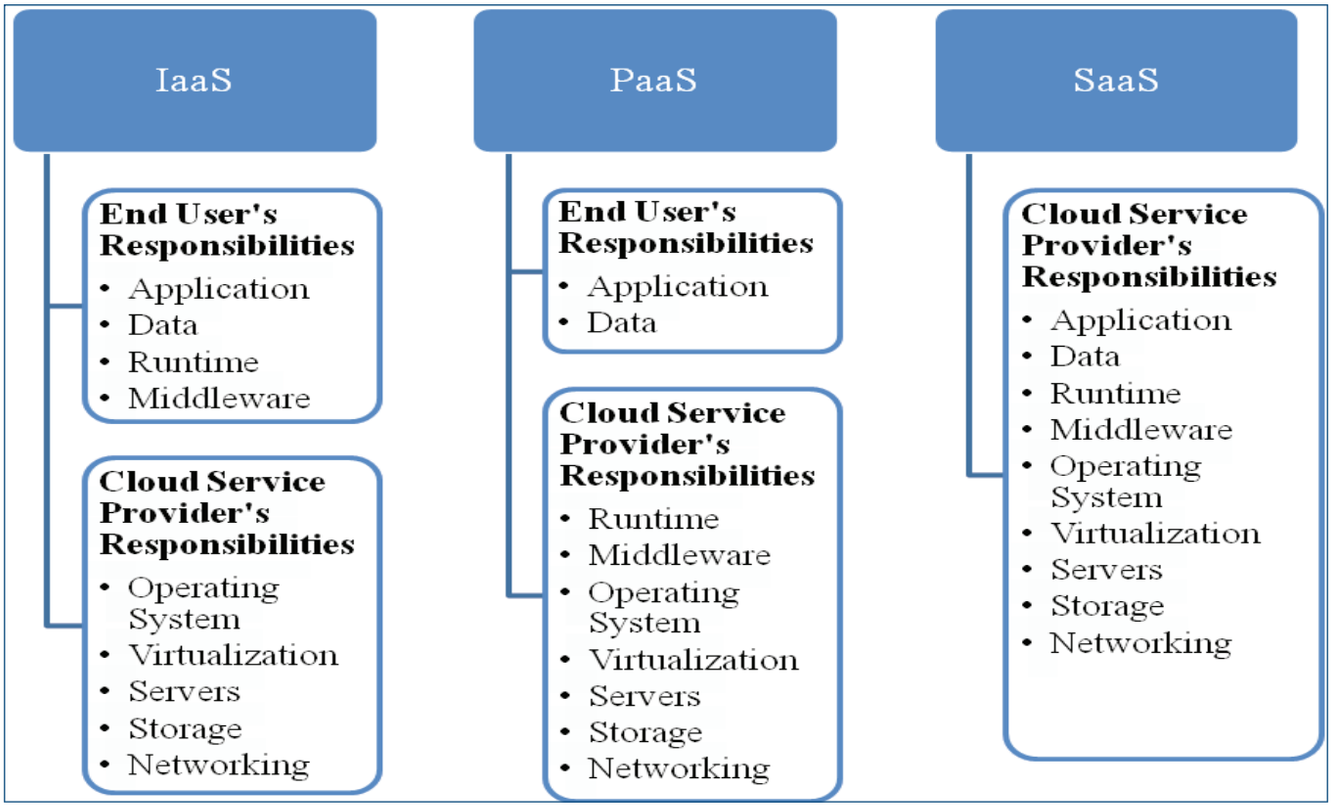
1. **On-demand Self-Service:** There is no need of human interaction from the cloud service provider side to make the computing resources available. Computing resources can be acquired and used at anytime. The computing services can be easily provisioned based on the requirements.
2. **Broad Network Access:** The computing resources can be accessed using a large number of heterogeneous devices including thin clients, thick clients and mobile devices. It provisions the end users to connect to the service provider through geographically disparate locations. Thus, providing mobility to the end users.
3. **Resource Pooling:** There is a vast pool of shared resources provided by the cloud service providers to the end users. This is called multi-tenant model. The end users have no knowledge regarding the exact location of the resources on the cloud.
4. **Rapid Elasticity:** There is a provision to automatically scale out or scale in the resources based on the requirements. The users, software features and other resources can be easily added or removed. Users can add more resources from the cloud by scaling out and can release those resources whenever they are no longer required.
5. **Measured Service:** A metering service is provided which will record the resource usage. It includes measuring the amount of storage used, the bandwidth used and the number of user accounts created. The metering service is transparent to both the cloud service provider and the end user.

Cloud Computing Models

A cloud computing service model defines the particular types of services that can be accessed on cloud, i.e., it describes the type of services provided by the cloud service provider (CSP). The end user can access the services based on the requirements. So, the end users don't own the resources but pay for the services used. Thus, providing control over capital expenditure on computing resources whether hardware and/or software. Cloud computing can provide three kind of service models namely, IaaS, PaaS and SaaS.

1. **Platform as a Service (PaaS):** In PaaS, the cloud service provider provides the development platform, operating system, server, storage and networking to the end user. The client is responsible for creating its own applications using the underlying infrastructure. As illustrated in Figure 2, the cloud service provider is responsible for maintaining the infrastructure whereas the maintenance of the application is the responsibility of the end user. So, the end user is relieved from the task of installing the software. Examples: Force.com and Microsoft Azure.
2. **Software as a Service (SaaS):** In the SaaS model, the cloud server provides the application to the end user. The end user can access the services using internet. The cloud service provider will provide the

Figure 2: Cloud Delivery Models



complete operating environment, applications and user interface to the end users. The end user is responsible for entering the data and to manage the interaction with the cloud. As depicted in Figure 2, the responsibility of the cloud service provider includes the application, platform and infrastructure. SaaS provides the end users with ready to use solutions. Examples: Google Docs and Salesforce CRM.

3. **Infrastructure as a Service (IaaS):** In IaaS, the cloud service provider is responsible to deliver the computer hardware and associated software as a service to the end user. The hardware includes server, storage and network whereas software includes operating systems, file systems and virtualization software. The end user will pay the cloud server based on the usage. As depicted in Figure 2, the service provider is responsible for the entire infrastructure whereas the client manages the platform, application development and deployment. So, it permits the client to use the hardware rather than purchase servers and software. Examples: Amazon Simple Storage Service and SQL Azure.

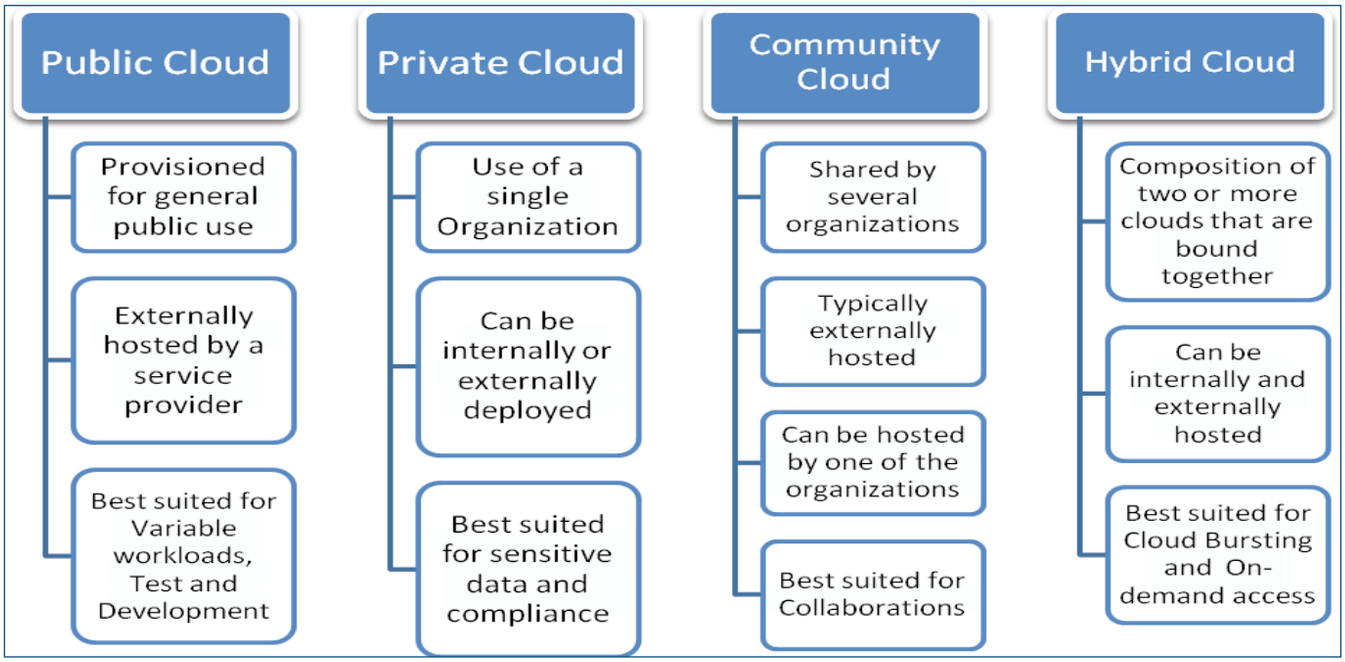
Cloud Deployment Models

A deployment model defines the purpose and the nature of how the cloud is located. The factors affecting the deployment of the cloud are:

i. Location of cloud services
ii. Security requirements
iii. Desire to share cloud services
iv. Ability to manage some or all of the services
v. Customization capabilities

1. **Public Cloud:** A public cloud as shown in Figure 3, is one which is owned by an organization providing cloud services and is available for public use. This model is used by small or medium organization as it reduces the initial capital expenditure and thus brings down the operational cost of an organization. A public cloud is used to handle sudden peaks of load through migration of workload to public cloud and pay for the duration the resources are used. It is generally used by organizations for developing

Figure 3: Cloud Deployment Models



and testing applications. Example: Amazon, Google Apps and Windows Azure. The advantages of using public cloud are [13]:

- Low upfront costs
- Simpler to manage
- Low operating expense
- High efficiency
- High availability
- Elastic scalability
- Fast deployment

2. **Private Cloud:** A private cloud infrastructure as shown in Figure 3, is owned and used by a single organization. It can be managed by the organization or by a third party. Private cloud is used when security of the data is a major concern. The initial deployment and maintenance cost of private cloud is high. Functionalities are not directly exposed to the customer and offers services with enhanced features. Example: eBay. The advantages of using private cloud are [13]:

- Greater control of security, compliance and quality of service
- Easier integration with in-house applications
- Lower long term total costs

3. **Hybrid Cloud:** A hybrid cloud provides the benefits of both public and private clouds. As shown in Figure 3, this model provides secure access to data by using private cloud whereas it provides cost effective solutions using the public cloud. Multiple clouds are tied together and a secure communication link is required between the clouds for secure communication. This secure link provides easy migration of workload between the public and private clouds.

4. **Community Cloud:** As shown in Figure 3, based on the similar requirements of several organizations, a community cloud can be deployed. This community cloud serves the common function or purpose of the organizations. These organizations share common concerns like their mission, policies and security requirements. It can be managed either by the constituent organizations or a third party can be employed for creating and managing the cloud. Community clouds reduce the cost as compared to a private cloud and are shared by a larger group.

Advantages of Cloud Computing

1. **Reduced Cost:** There are a number of reasons to attribute Cloud technology with lower costs. The billing model is pay as per usage; the infrastructure is not purchased thus lowering maintenance. Initial expense and recurring expenses are much lower than traditional computing.

2. **Increased Storage:** With the massive Infrastructure that is offered by Cloud providers today, storage & maintenance of large volumes of data is a reality. Sudden workload spikes are also managed effectively & efficiently, since the cloud can scale dynamically.
3. **Flexibility:** This is an extremely important characteristic. With enterprises having to adapt, even more rapidly, to changing business conditions, speed to deliver is critical. Cloud computing stresses on getting applications to market very quickly, by using the most appropriate building blocks necessary for deployment.

Cloud Computing Challenges

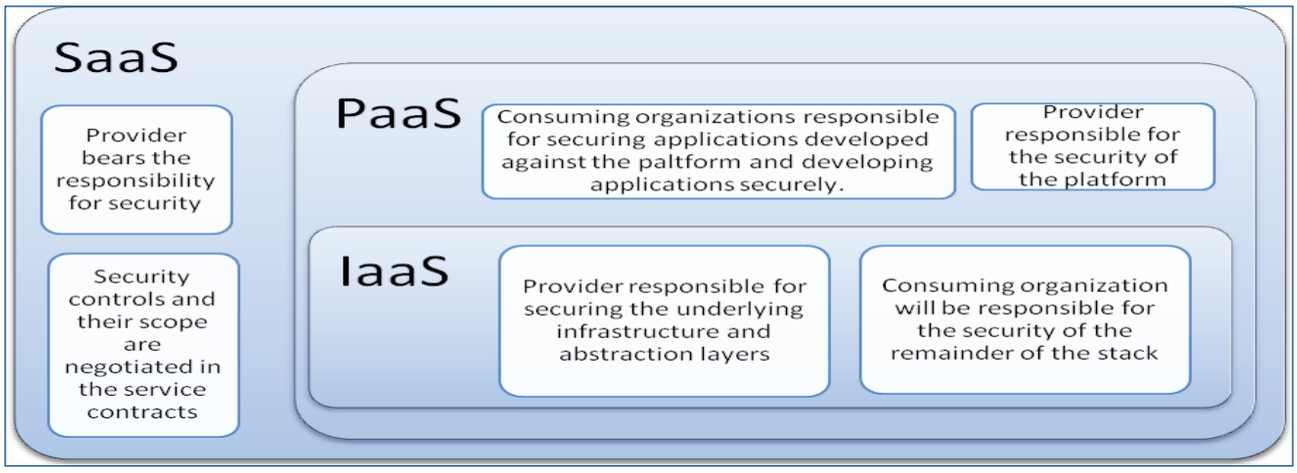
1. **Data Location:** Cloud computing permits the data to be stored at different locations. The data owner is unaware of the location of the server used to store the data. So, data location is a critical issue for data governance requirements.
2. **Performance:** Cloud computing involves the access of resource through internet. Due to delays caused by demands and traffic spikes, slowdown caused by malicious traffic the performance of the cloud services is degraded.
3. **Security:** The organizations can use cloud to store their confidential data and personal information. There may be data leakage due to replication of the data at multiple locations. Unauthorized users may gain access to the data. So, security of the data is a major challenge.
4. **Limited Features:** Certain web based applications available on cloud don't have features as are available with the desktop version. So, the consumer is bound with an application providing limited features.
5. **Cloud Data Ownership:** It may be possible that the cloud service provider assumes that it owns the data stored in the cloud computing environment and may demand for service fees for data to be returned to the enterprise when the SLA with the CSP terminates.
6. **Vendor Lock-in:** The end user uses the cloud applications to store the data. These applications provide data in a fixed format or may be developed for a fixed platform. Due to this it is difficult migrating the data or application from one cloud service provider to another. So, it is extremely complicated, time-consuming and labor-intensive task to migrate the data and hence leads to vendor lock-in.

Security on Cloud

Security

The Cloud Security Alliance (CSA) defined the hardware/software stack of cloud computing which is referred to as Cloud Reference Model. In this model, IaaS is the lowest level service, with PaaS on second level and SaaS on the top level. The cloud service models inherit the capabilities of the underlying security models. Additionally, all the security concerns and risk factors are also inherited. IaaS provides the infrastructure and has the least security integrated into it. PaaS adds application development

Figure 4: Cloud Security Boundaries



frameworks, transactions, and control structures over IaaS and has intermediate security integrated into it. SaaS provides the complete applications along with management and the user interface. So, SaaS provides the highest level of security. Each service model defines a boundary between the services provided by the cloud service provider and the end user. As shown in Figure 4, in the SaaS model, the vendor provides security as part of the Service Level Agreement. In the PaaS model, the vendor is responsible for the security of the software framework and middleware layer whereas the customer is responsible for the security of the application and user interface. In the IaaS model, the security of the infrastructure is the vendor's responsibility whereas any security measure required for the software is the customer's responsibility.

Cloud Security Taxonomy

In cloud, the critical security and other obstacles are introduced due to the underlying technologies behind cloud computing as well as due to the new and essential features of cloud computing. Nelson Gonzalez et al. [15] have introduced many security concerns along with possible solutions. The security concerns are identified, classified, organized and quantified. The security concerns are classified in a hierarchical manner and represented by Figure 5.

Figure 5: Cloud Computing Security Taxonomy

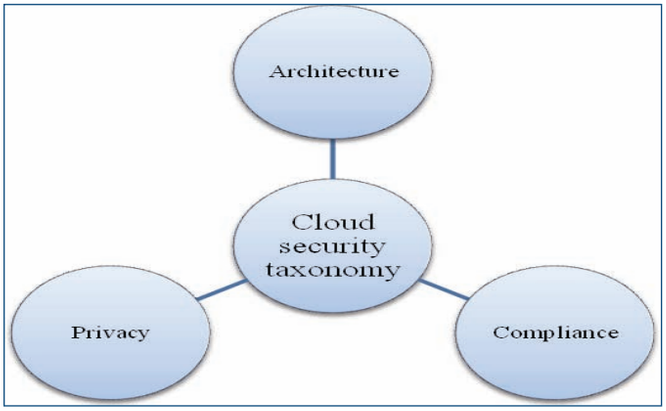


Figure 6 depicts the various security issues related to the architecture of cloud which can be classified as:

i. **Network Security:** It includes problems related to network communication and configuration pertaining to cloud infrastructure. It includes effective firewalling as a solution to provide security because it provides protection from both insiders and outsiders.

ii. **Interfaces:** It includes all the interfaces used to access and manage cloud information. These interfaces may be user interfaces, administrative interfaces and programming interfaces. For providing security, well protected APIs (Application Programming Interfaces) and proper authentication mechanisms are used.

Figure 6: Cloud Computing Security Taxonomy – Architecture

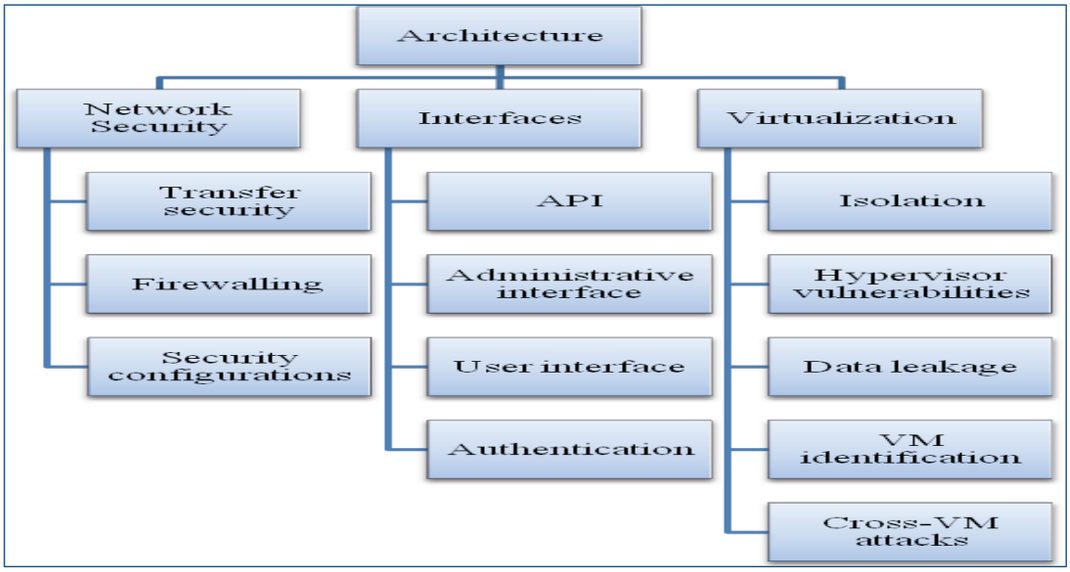
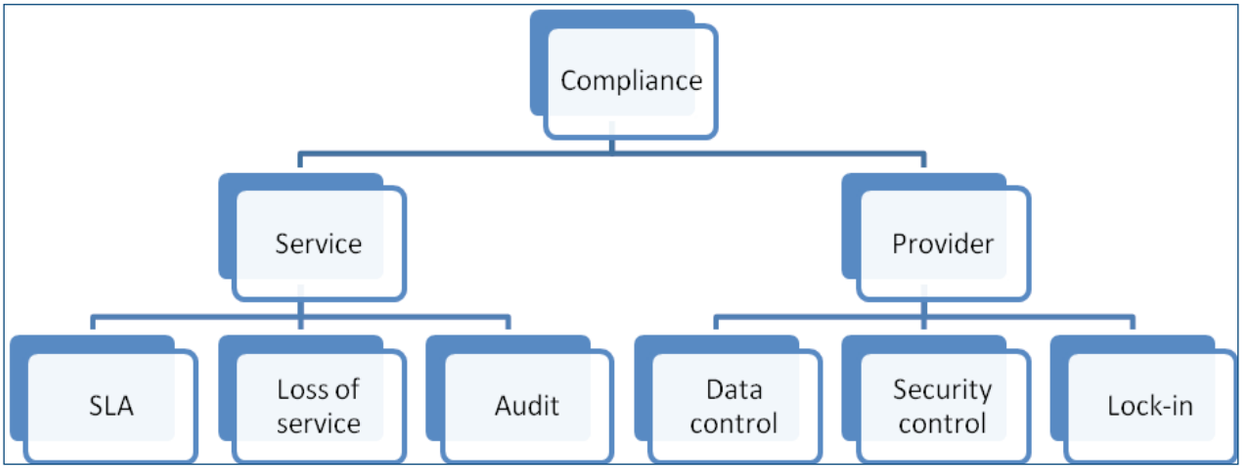


Figure 7: Cloud Computing Security Taxonomy – Compliance

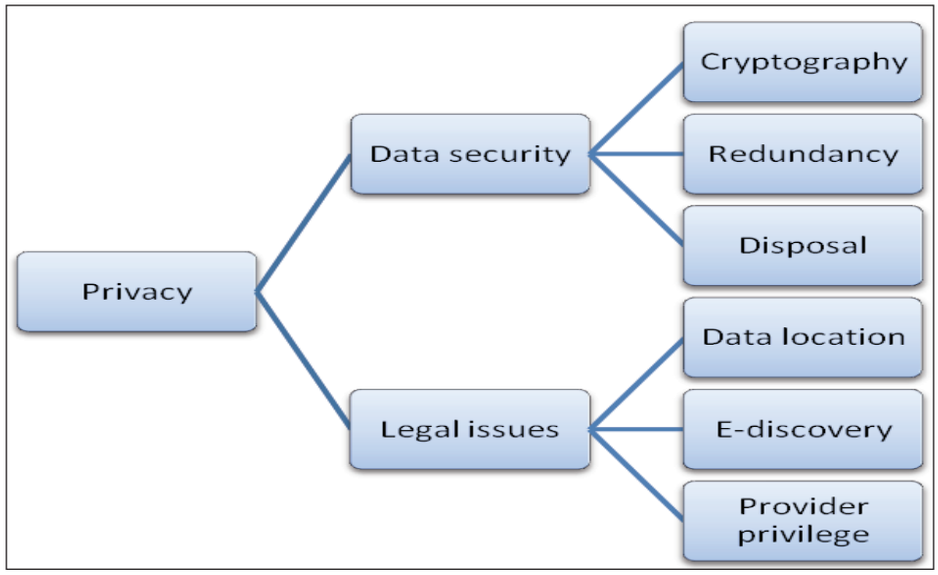


iii. **Virtualization:** It involves issues related to isolation between Virtual Machines (VMs) and other vulnerabilities related to hypervisors. To provide effective security, isolation of VMs can be extended to include isolation in computation, resources, storage and memory.

Figure 7 depicts the compliance dimension which enlists the responsibilities of the providers related to services. It involves requirements for service availability and audit.

Figure 8 depicts the privacy dimension of security which includes data security and legal issues. Data security can be achieved using cryptography (securing the confidential data by converting plaintext to human unreadable form), redundancy (creating multiple replicas of mission critical data) and disposal (effectively deleting the data from log references and hidden backup registries). Legal issues include data location (the data in cloud is located at different geographical locations which introduces multiple jurisdictions), E-discovery (involves the confiscation of hardware for investigation of an attack which affects the services offered to other customers) and provider privileges (involves restricting activities of malicious insiders in the premises of the service providers). This dimension covers the entire information lifecycle from generation, use, transfer, transformation, storage, archive and destruction.

Figure 8: Cloud Computing Security Taxonomy – Privacy



Cloud Security Threats

The most prevalent and serious security threats in cloud computing as per Cloud Security Alliance (CSA) are [16]:

1. **Data Breaches:** The most serious concern for an organization is the release of confidential data to any third party. Due to cloud usage this concern is increased by manifolds because a VM can be used to perform side channel timing exposure, i.e., a VM can be used to listen and raise a signal if an encryption key is used on other VM. If the encryption keys are lost, then the security risks are increased. If offline backup is maintained, then the exposure to data breach is further increased.
2. **Data Loss:** Data stored on the cloud can be permanently lost due to malicious attack, accidental deletion of data by the cloud service provider (CSP) and physical catastrophe. If adequate measures are not taken by the CSP, then the data may be permanently lost. In addition to this, if the encryption keys are lost by the customer then also data loss can occur.
3. **Account or Service Traffic Hijacking:** Phishing, frauds and vulnerabilities in software lead to account hijacking which is not a new issue. Cloud adds more to this by allowing the customer's account or service instances to act as base for attack and thus allowing personal credentials to be accessed and manipulated. So, it leads to loss of confidentiality, integrity and availability of services.
4. **Insecure Interfaces and APIs:** The services and resources on the cloud are accessed using interfaces and APIs. Everything from provisioning, management and monitoring is done using these interfaces. So, the security of these APIs is must for the security of cloud services. The interfaces and APIs must protect against accidental and malicious attack.
5. **Denial of Service (DoS):** A DoS attack makes a cloud user unable to use the resources of cloud. A malicious user can cause a cloud service to consume large amount of system resources which slows down the entire system. As cloud is based on pay-per-use model, the customer has to pay for the period of time when the server was busy due to DoS attack and services were partially offered to the user.
6. **Malicious Insiders:** Any malicious insider is a threat to an organization as he may use the authorized access to negatively affect the confidentiality, integrity and availability of organization's information.
7. **Abuse of Cloud Services:** An attacker may use the services of cloud to crack the security by using the large processing power available on cloud. These resources may also be used to launch a DDoS (Distributed Denial of Service) attack.
8. **Insufficient Data Diligence:** Many organizations are acting as cloud service provides but they don't understand the concept of cloud and security completely. So, the security solutions provided by these CSP are partially able to provide the desired level of security.
9. **Shared Technology Vulnerabilities:** A CSP provides services in the form of infrastructure, platform and applications. The threats of shared vulnerabilities exist in all delivery models. So, it is required that strong isolation for IaaS, proper re-deployable platforms for PaaS and proper sharing of applications in SaaS is provided.

Securing Cloud Data

Today cloud is used by everyone to meet and exchange the information which is in the form of documents, photos, presentations and videos. So, the use of cloud has increased significantly due to which the safety of the information stored on cloud is of prime importance. Following are few of the measures which can be used for cloud data privacy [17, 18, 27]:

1. Access control lists can be used to define the permissions on each data objects stored on cloud.
2. Storage encryption can be used to protect against unauthorized access at the data center.
3. Strong passwords should be used for authentication. The passwords should be at least eight characters long and should include numbers, punctuations, symbols, uppercase and lowercase letters.
4. Transport level encryption can be used to protect data when it is transmitted.
5. Firewalls help in protecting attacks from outside.
6. The servers should be designed to protect against known and unknown vulnerabilities.
7. Physical security should be used to protect against unauthorized access to data.

8. The consumers should enquire that sufficient measure are taken by the cloud service provider to protect against threats like Distributed Denial of Service.
9. The end users should ensure that sufficient backup and recovery measures are used by the providers to deal with disaster recovery.
10. The service level agreement should be analyzed to understand the working of cloud storage.
11. Since cloud services are accessed through the use of any device whether thin client, thick client or mobile devices. There may be a possibility that key loggers or some form of malware exists in that device and the confidentiality of data may be lost. So, the device used to access cloud resources should be one that is trusted.
12. Hypertext Transfer Protocol Secure (HTTPS) is a combination of Hypertext Transfer Protocol (HTTP) with SSL/TLS protocol. It provides encrypted communication and secure identification of a network web server. So, HTTPS should be used.
13. Mobile users access cloud through mobile phones, so it is desired that their mobile phones are protected via passwords. Also, strong antivirus and malware detection software play a significant role.
14. As cloud stores data on remote servers and in case the cloud service provider is down, the access to the data is not possible. So, backup of the data should be done locally.
15. Modern web browsers provide Anti Phishing/ Malware detection extensions. So, the choice of the web browser should be made intelligently.

Related Work

William R. Claycomb and Alex Nicoll [19] presented the threats which can be possible on cloud by internal users of cloud. The internal malicious user exploits the privileges granted to affect the working of an organization. The availability of resources and services in cloud can be used by the malicious user to commit crimes and launch attacks. The insider threats in cloud scenario are classified into three categories namely, cloud administrator, employees performing unauthorized access due to vulnerabilities in the system and employees using the resources of cloud to launch attacks. Cloud administrator can be a threat to the confidential data stored on the cloud. The administrator can steal the confidential data and thus the confidentiality of the data is affected. The administrator can also affect the availability of the data. Thus affecting the services utilized by the end user. To overcome these attacks, encryption is used. But key management is an important issue related to encryption of data. The second categories of users exploit the vulnerabilities of the system to perform a fraud or theft of intellectual property. To overcome these attacks, sufficient authorization and access control policies should be enforced. For the third category of users the available tools and techniques to prevent data loss should be used.

Deyan Chen and Hong Zhao [20] presented the analysis of security of data throughout the lifecycle of data. The seven phases of data life cycle are generation, use, transfer, share, storage, archival and destruction. Data ownership is an important concern whenever data is to be migrated to cloud. As compared to traditional IT environment, the data ownership should be clearly defined. In order to handle proper transfer of data between different organizations, encryption along with secure transport protocols is required which also provide confidentiality and integrity. When the data is to be used, operations are performed on unencrypted data. So, security of data is difficult to maintain. Sufficient authorization and granularity of access should be properly defined for sharing private data. Integrity, confidentiality and availability of data should be maintained with reference to data storage. Key management is the most crucial point in data storage. The archival of data should be defined whether off-site storage is provided by the CSP or not. It is also stated that the data should be removed securely from the system using methods such that it is impossible to recover the data because if it is possible to recover the data then an adversary can easily access the sensitive data.

Abdullah Abuhussein et al. [21] identified various attributes related to various services provided on cloud with reference to security and privacy. The authors aim to provide awareness to cloud users related to security and privacy, provide skills pertaining to cloud computing technologies, provide users within the enterprise to decide the level of security desired and to clearly define the security features provided by CSP. The security concerns related to cloud computing are categorized into seven categories, namely, network security, interface security, data security, virtualization security, governance security, compliance security and legal issues. Various attributes

related to these categories are backup, encryption, authentication, access control, dedicated hardware for data isolation, monitoring, data storage location, security certificates, data sanitization, service level agreements, disaster recovery, hypervisor security and client end security vulnerabilities.

M.A. AlZain et al. [22] have identified three main factors related to cloud security in both single and multi-cloud models as: data integrity, data intrusion and service availability. Data integrity requires that the data is not modified during transmission and storage. The cloud user can use different devices to connect to cloud which can affect data integrity. An adversary can gain access to secure information and can interrupt the services offered to authorize users.

A. Patrascu et al. [23] classified cloud security into four categories, namely, (i) Traditional security which involves issues as authentication, authorization, data stealing, virtual machines vulnerabilities and cloud service provider vulnerabilities; (ii) Availability of cloud computing applications which includes vulnerabilities related to cloud applications as single point of failure and valid computations; (iii) Third party data privacy which involves efficient usage of data by third party and (iv) Third party data control which involves data stealing, data deletion or loosing access to data.

S. Subashini and V. Kavitha [24] presented the security issues present at various cloud service models, namely, SaaS, PaaS and IaaS. Security issues related to SaaS are data security, network security, data locality, data integrity, data segregation, data access, authentication, authorization, data confidentiality, web applications security, data breaches, virtualization vulnerabilities, availability, backup, identity management and sign-on process. In PaaS and IaaS the security solutions are developed and integrated by the cloud user during application development. So, only the network and host intrusion vulnerabilities are handled by the CSP.

Seny Kamara and Kristin Lauter [25] presented cryptographic storage service which provides confidentiality, integrity and non-repudiation and still provides benefits as availability, reliability, efficient retrieval and data sharing. The proposed architecture includes three components data processor, data verifier and token generator. Data processor processes the data before outsourcing it to the cloud. Data verifier verifies that the data stored on cloud is tampered or not. Token generator helps in retrieval of cloud data. The user retrieves the data by decrypting the received encrypted documents from the cloud server using the decryption keys. In order to share data, tokens are shared.

C. Gentry [26] presented fully homomorphic encryption. A fully homomorphic encryption scheme allows the users to perform algebraic operations on encrypted data in the same way as it is performed on encrypted data. It also provides the user with the capability to perform search operation on encrypted data in the same way as it is performed on plaintext. The proposed method requires high computational resources.

Conclusions

Cloud provides with enormous amount of resources at low initial set up and maintenance cost. There are various advantages of cloud along with the challenges involved with the use of cloud for sensitive data. Maintaining the confidentiality of the data is very important when outsourcing data on cloud. In this study rigorous analysis is made on the fundamental concepts of cloud along with the advantages and challenges involved. The security aspect of cloud along with the protection measure has been presented. The study reveals that cloud can be used for confidential data if the security aspects are also considered before migrating to cloud.

References

Cloud Computing. (2011). Retrieved from *http://en.wikipedia.org/wiki/ Cloud_computing.*

The NIST Definition of Cloud Computing. (2011). Retrieved from *http://csrc.nist.gov/publications/nistpubs/800-145/ SP800-145.pdf.*

Top-10 Cloud Service Providers. (2012). Retrieved from *http://searchcloudcomputing.techtarget.com/photostory/2240149038/Top-10-cloud-providers-of-2012/1/ Introduction*.

Morgan. (2009). Factors affecting the adoption of cloud computing: an exploratory study. Retrieved from *http://www.staff.science.uu.nl/~vlaan107/ecis/files/ECIS2013-0710-paper.pdf*.

Voas, J., & Zhang, J. (2009). Cloud computing: New wine or just a new bottle? *IT Professional*, 11(2), 15-17.

Vaquero, L. M. (2009). A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Computer Communication Review Archive*, 39(1), 0-55.

Wang, L. (2010). Cloud computing: A perspective study. *New Generation Computing,* April, 28(2), 137-146.

Buyya, R. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6), 599-616.

Gong, G. (2010). *The Characteristics of Cloud Computing.* In Proceedings of 39th International Conference on Parallel Processing Workshops, (pp. 275-279).

Dudin, E. B., & Smetanin, Y. G. (2011). A review of cloud computing. *Scientific and Technical Information Processing*, 38(4), 280-284.

Cloud Service Models. (2011). Retrieved from *http://blogs.msdn.com/b/dachou/archive/2011/03/16/rise-of-the-cloud-ecosystems.aspx.*

Cloud Deployment Models. (2011). Retrieved from *http://www.elementsolutions.com/2013/08/08/part-2-cloud-computing-demystified-3s-4d-5e-is-all-you-need-to-know/*

Arutyunov, V. V. (2012). Cloud computing: Its history of development, modern state, and future considerations. *Scientific and Technical Information Processing*, 39(3), 173-178.

Understanding Cloud Security: Finding the Boundaries. (2012). Retrieved from *http://neirajones.blogspot.in/2012/02/navigating-through-cloud-finding.html.*

Gonzalez, N. (2011). *A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing*. In Proceedings IEEE 3rd International Conference on Cloud Computing Technology and Science, (pp. 231-238).

Cloud Security Alliance. (2013). The notorious nine cloud computing top threats in 2013. Retrieved from *https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.*

5 Tips to Keep Your Data Secure on the Cloud. (2012). Retrieved from *http://www.cio.com/article/2380182/cloud-security/5- tips-to-keep-your-data-secure-on-the-cloud.html.*

Securing Cloud Data. Retrieved from *http://www.applicure.com/blog/securing-cloud-data.*

Claycomb, W., & Nicoll, A. (2012). *Insider Threats to Cloud Computing: Directions for New Research Challenges*. In Proceedings of IEEE 36th Annual Computer Software and Application, Washington, DC, USA, (pp. 387-394).

Chen, D., & Zhao, H. (2012). *Data security and privacy protection issues in cloud computing*. 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), 1, pp. 647-651.

Abuhussein, A. (2012). *Evaluating Security and Privacy in Cloud Computing Services: A Stakeholder's Perspective*. In Proceedings of 2012 International Conference on Internet Technology and Secured Transactions, London, (pp. 388-395).

AlZain, M. A. (2012). *Cloud Computing Security: From Single to Multi-Clouds*. In Proceedings of 45th Hawaii International Conference on System Science, (pp. 5490-5499).

Patrascu, A. (2012). *New Directions in Cloud Computing. A Security Perspective*. In Proceedings of 9th International Conference on Communications, Bucharest, (pp. 289-292).

Subashini, S., & Kavitha, V. (2011). Review: A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11.

Kamara, S., & Lauter, K. (2010). *Cryptographic cloud storage*. In Financial Cryptography 2010 Workshops on Real-Life Cryptographic Protocols and Standardization, Tenerife, Canary Islands, Spain, (pp. 136-149) .

Gentry, C. (2009). *Fully Homomorphic Encryption using Ideal Lattices*. In Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC), (pp. 169-178).

8 Ways to Secure Your Privacy in the Cloud. Retrieved from *http://www. gilsmethod.com/8-ways-to-secure-your-privacy-online.*