Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 3, March 2017, pg.154 – 159

An Overview of Issues and Data Security Expert Reveal for Cloud Computing

Ms. Neelkamal Chaudhary
Computer Science and Engineering Department, NIMS University, Jaipur
neelkamal.chaudhary26@gmail.com

Abstract: Cloud Computing is a promising technology to development of computing infrastructures. Cloud Computing is continuously evolving and showing consistent growth in the field of computing. It provides different computing services as Cloud storage, Cloud hosting and Cloud servers etc. In this paper, we discuss Security Issues for Cloud Computing including Security. Then we select some topics and describe them in more details. Security is still critical challenge in the Cloud Computing paradigm. Also present different opportunities in security & privacy in Cloud environment.

Keywords: Cloud Computing, Security, Privacy.

I. INTRODUCTION

The term Cloud refers to a Network or Internet. Cloud Computing provides us a means by which we can access the applications as utilities, over the Internet. We can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. It allows us to create, configure, and customize applications online. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud. Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application.

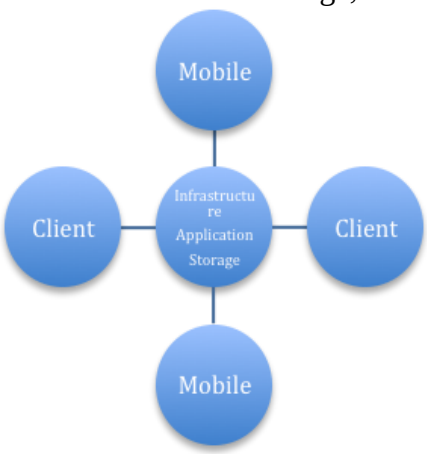


Fig 1. Infrastructure of application storage

There are certain services and models working behind the scene making the cloud computing. Following are the working models for cloud computing:

- **Deployment Models**
- **Service Models**

II. DEPLOYMENT MODELS

Deployment models define the type of access to the cloud. Cloud can have any of the four types of access: Public, Private, Hybrid and Community.

A. PUBLIC CLOUD

The Public Cloud allows systems and services to be easily accessible to the general public.
Public cloud may be less secure because of its openness, e.g., e-mail.

B. PRIVATE CLOUD

The Private Cloud allows systems and services to be accessible within an organization.
It offers increased security because of its private nature.

C. COMMUNITY CLOUD

The Community Cloud allows systems and services to be accessible by group of organizations.

D. HYBRID CLOUD

The Hybrid Cloud is mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

III. SERVICE MODELS

Service Models are the reference models on which the Cloud Computing is based. These can be categorized into three basic service models as listed below:

Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)

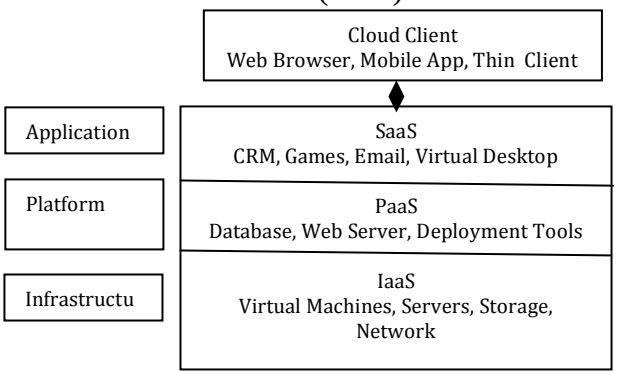


Fig 2. Service Model

IV. CLOUD COMPUTING TECHNOLOGIES

Virtualization is a technique, which allows to share single physical instance of an application or resource among multiple organizations or tenants (customers). It does so by assigning a logical name to a physical resource and providing a pointer to that physical resource when demanded.

Service-Oriented Architecture helps to use applications as a service for other applications regardless the type of vendor, product or technology. Therefore, it is possible to exchange of data between applications of different vendors without additional programming or making changes to services.

Grid Computing refers to distributed computing in which a group of computers from multiple

locations are connected with each other to achieve common objective. These computer resources are heterogeneous and geographically dispersed. **Grid Computing** breaks complex task into smaller pieces. These smaller pieces are distributed to CPUs that reside within the grid.

Utility computing is based on Pay per Use model. It offers computational resources on demand as a metered service. Cloud computing, grid computing, and managed IT services are based on the concept of Utility computing.

V. CLOUD COMPUTING SECURITY

Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from direct accessing the shared data, proxy and brokerage services should be employed. Before deploying a particular resource to cloud, one should need to analyze several attributes about the resource such as:

1. Select which resources he is going to move to cloud and analyze its sensitivity to risk.
2. Consider cloud service models such as IaaS, PaaS, and SaaS. These models require consumer to be responsible for security at different levels of service.
3. Consider which cloud type such as public, private, community or hybrid.
4. Understand the cloud service provider's system that how data is transferred, where it is stored and how to move data into and out of cloud. Mainly the risk in cloud deployment depends upon the service models and cloud types.

VI. ISSUES TO CLARIFY BEFORE ADOPTING CLOUD COMPUTING

The world's leading information technology research and advisory company, has identified seven security concerns that an enterprise cloud computing user should address with cloud computing providers (Edwards, 2009) before adopting:

- **Long-term Viability**: Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application.
- **Regulatory Compliance:** Make sure your provider is willing to submit to external Audits and security certifications.
- **User Access:** Ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information. Major Companies should demand and enforce their own hiring criteria for personnel that will Operate heir cloud computing environments.
- **Data Segregation**: Find out what is done to segregate your data, and ask for proof that encryption schemes are deployed and are effective.
- **Data location**: Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the privacy rules of those Jurisdictions.
- **Disaster Recovery**: Ask the provider for a contractual commitment to support specific types of investigations, such as the research involved in the discovery phase of a lawsuit, and verify that the provider has successfully supported such activities in the past. Without evidence, don't assume that it can do so.

VII. SOLUTION OF SECURITY ISSUES

- **Find Key Cloud Provider:** First solution is of finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.
- **Clear Contract:** Contract with cloud vendor should be clear. So if cloud vendor closes before contract, enterprise can claim.

- **Recovery Facilities:** Cloud vendors should provide very good recovery facilities. So, if data are fragmented or lost due to certain issues, they can be recovered and continuity of data can be managed.
- **Better Enterprise Infrastructure:** Enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber attacks.

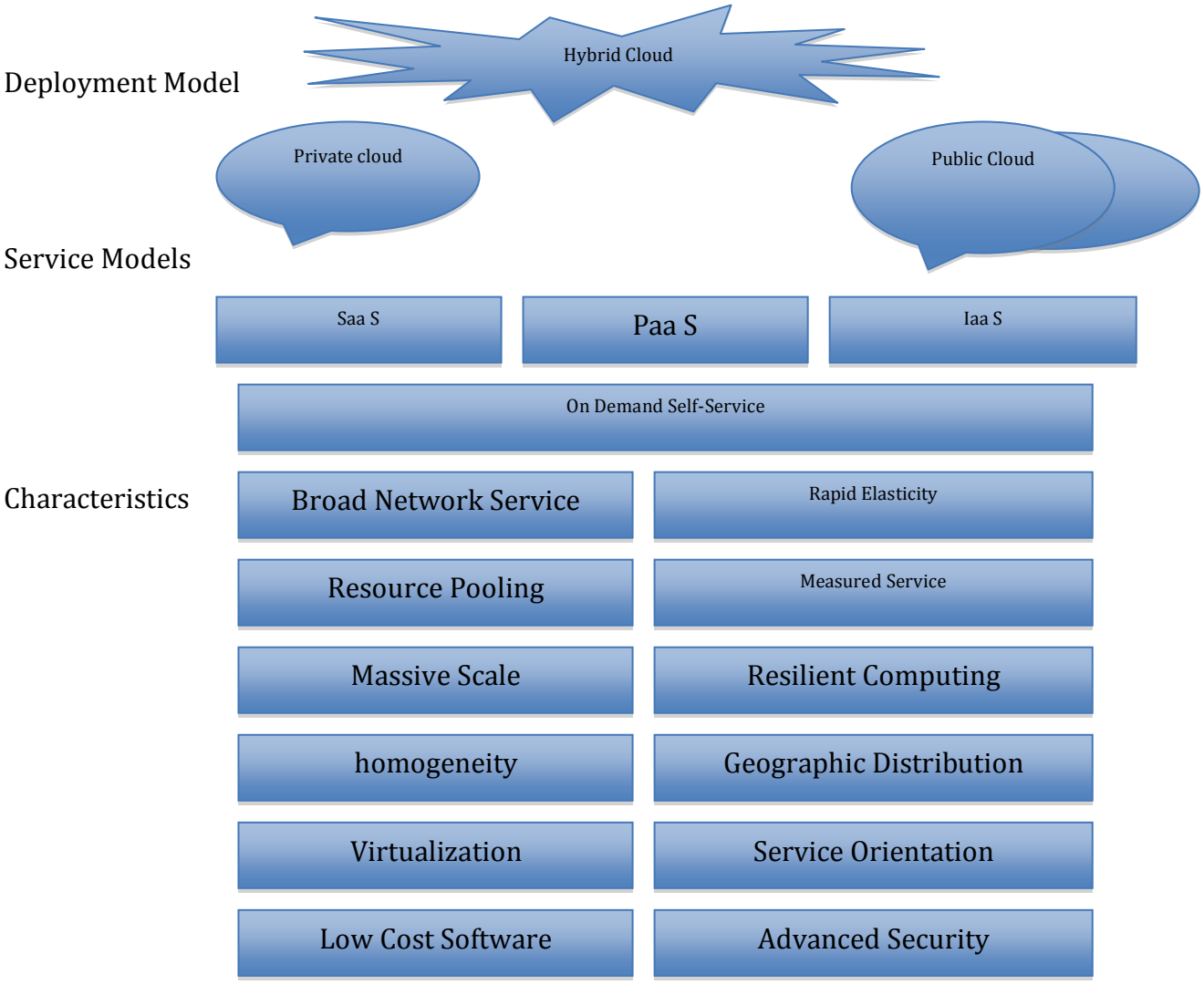
VIII. USE OF DATA ENCRYPTION FOR SECURITY PURPOSE

Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor.

- **Investigation Support:** Audit tools provided to the users to determine how their data is stored, protected, used, and verify policy enforcement. But investigation of illegal activity is quite difficult because data for multiple customers may be collocated and may also be geographically spread across set of hosts and datacenters. To solve this audit tools must be contractually committed along with the evidence.
- **Network Security**: A user can deny the access of any Internet based service by using IP Spoofing which can be a cause of security harm. To solve this we can use Digital Signature technique. SSL (Secure Socket Layer) Protocol is used for managing security of message transmission on The Internet. Which also avoid resource hacking.
- **Encryption Algorithm**: Obviously cloud service providers encrypt the user's information using strong encryption algorithm. But problem is that encryption accident can make data totally unusable and encryption also complicates the availability. To solve this problem the cloud provider must provide evidence that encryption scheme were designed and tested by experienced specialists.
- **Backup**: Natural disaster may damage the physical devices that may cause of data loss. To avoid this problem backup of information is the key of assurance of service provided by vendor.
- **Customer satisfaction**: Very hard for the customer to actually verify the currently implemented security practices and initiatives of a cloud computing provided by the service provider because the customer generally has no access to the provider's facility which can be comprised of multiple facilities spread around the globe [8]. Solution for this Provider should get some standard certificate from some governing or standardized institution that ensures users that provider has established adequate internal control and these control are operating efficiently.

IX. CHARACTERISTICS

There are four key characteristics of cloud computing. They are shown in the following diagram: It is possible that the data requested for deletion may not get deleted. It happens either because extra copies of data are stored but are not available or disk destroyed also stores data from other tenants.



X. CONCLUSION

Cloud computing is the future of IT industries It helps the industries to get efficient use of their IT Hardware and Software resources at low cost. Cloud computing is a combination of several key technologies that have evolved and matured over the years. Enterprise looking into cloud computing technology as a way to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing. Cloud computing has a potential for cost savings to the enterprises but the security risk are also enormous. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. We tried to solve many issues. In our future work, we will include the developing of testing of data flow and security in cloud computing.

There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted.

XI. FUTURE WORK

Our objective is to block the hole arise in the security management processes of the cloud consumers and the cloud providers from adopting the cloud model. The cloud architecture, security patterns and security enforcement mechanisms and Deliver feedback about the current security status to the cloud providers and consumers.

REFERENCES

[1] Chandra Prakash Verma, Neelkamal Chaudhary, Noopur Rastoagi"Analyzing Cloud Storage Database Management "International Journal of Innovative Computer Science &Engineering (IJICSE),ISSN:2393-8528.
[2] Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems; 2009; 25(6):599–616.
[3] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A View of Cloud Computing. Communications of the ACM ; 2010; 53(4):50–58.
[4] Subashini S, Kavitha V. A survey on security i ssues in service delivery models of cloud computing. Journal of Network and mputer Applications; 2011; 4(1):1–11.
[5] Takabi H, Joshi J B D, Ahn G. Security a nd privacy challenges in cloud computing environments. IEEE Security & Privacy;2010;8(6) :24–31.
[6] Sangroya A, Kumar S, Dhok J, Varma V. Towards analyz ing data security risks in cloud computing environments. Communications in Computer and Information Science; 2010; 54 :255–265.
[7] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 8, August 2012).

