Security Control of Service Models in Cloud Computing: A General Scope

Sandeep Kaur[1]Satveer Kaur[2]Hardeep Singh[3]
[1,2,3]Department of Computer Science & Engineering
[1,2,3]GNDU RC, Sathiala-143205, Amritsar, Punjab, India

Abstract—*Security in cloud computing is, for the most part, no different than security controls at any IT sector. The cloud service models employed the operational model and technology used to enable cloud services, cloud computing service model may present diverse risks to an organization than traditional IT solutions. This paper describes in a more general way about the security boundaries of service models. Security boundaries help us to control losing of data and maintain accurate accountability. The security tasks of both the provider and the consumer greatly differ between cloud service models. Purveyor tasks for security up to the hypervisor, means they can only address security controls such as physical security, environmental security, and virtualization security. The consumer, in turn, is responsible for security controls that relate to the IT system (instance) including the operating system, applications, and data.*

Keywords—Security control model, compliance model, Cloud computing

I. Introduction

Cloud computing is a subscribed based service where a user can get a networked storage space and various other tools to enjoy. With all these achievements in hand, cloud computing fights against some challenges also. Security is the basic challenge in cloud computing world.[2] Clouds have their different category for which they are subscribed like public cloud, private cloud, hybrid cloud and community cloud. Cloud computing also supports the service models like Infrastructure as a service, Platform as a service, Network as a servicesecurity control in more general scopeand Storage as a service and Software as a service. They help to provide the services to the end user with full security. Security issues are also their like Misuse and reprehensible Use of Cloud Computing. • Insecure API. • Wicked Insiders. • Shared Technology issues/multi-tenancy nature. • Data Crash. • Account, Service & Traffic Hijacking. • Unidentified Risk report.In Section 2. Cloud computing types will be discussed and in section 3. Service models will be discussed section 4. Includes the compliance model.Section 5. Deals with the security control model. In last section 6. Conclusion is made on the basis of these models with the services provided by the administrator to the users.

II. Cloud types

Clouds have their different categories for which they are widely subscribed to.Fig. [1] Defines share of each cloud type over ally.

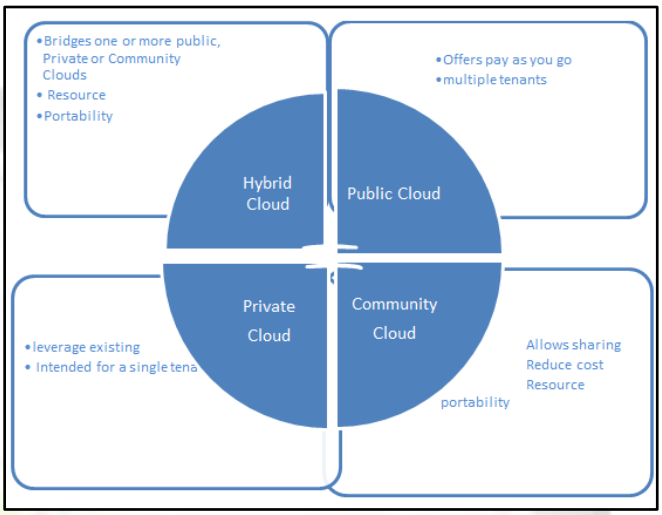

Fig. 1: Cloud types in computing

A. *Public Cloud:*

Public cloud, as per its name, is accessed publicly over the network. Any subscriber to a cloud can access the space and resources of cloud using an internet connection. This also refers to the fact that a subscriber using public cloud is relying on third parties which are presenting IT services efficiently on the internet. Example of public cloud includes Amazon AWS, Google apps, salesforce.com, Microsoft BPOs [2]

– Data security issue

B. *Private Cloud:*

According to the National institute of standards and technology (NIST), a private cloud is a cloud structure that is made isolated for just one particular organization or a specific group of departments.[3] This means that private cloud is confined to certain circle. Private clouds are mostly used to secure the confidential data. Its security architecture is made like so. It works same like cloud but on small scale.

1) *Drawbacks of Private Cloud:*

In comparison to Public cloud, it involves more cost.

C. *Community Cloud:*

Community Cloud is set to operate on two or more groups of organizations that have same requirements, security, and privacy considerations instead of single organization. [4] It is exclusively accessed by more than one organization. Community cloud lies between private and public cloud, also cost of setting up a community cloud is cheaper because of division among the organization.

However, limitation of community cloud can be if compared with the public cloud, is it is more costly. Organizations share fixed bandwidth and storage space.

D. *Hybrid Cloud:*

Hybrid, as the name suggests, is a combination of two or more cloud types. Hybrid clouds are considered to be more

complex than the other deployment models, since they involve a composition of two or more clouds (private, community or public). Each member remains a unique entity, but is bound to others through standardized or proprietary technology that enables application and data portability among them [3]. A hybrid cloud is typically offered in one of two ways: a vendor has private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms [4].

In hybrid cloud, an organization provides and manages some resources in-house and some out-house. For example, organizations that have their human resource (HR) and customer relationship management (CRM) data in public cloud like salesforce.com but have confidential data in their own private cloud [5].

Hybrid clouds [6] offer the cost and scale benefits of public clouds, while also offering the security and control of private clouds.

III. SERVICE MODELS

A. Software as a Service (SaaS):

A software as a service is one to many software delivery service. It gives its subscribers wide range of activities, resources, its different applications, software and its functions over the internet. With the software as a service, user needs not to worry about the installation, daily work and maintenance. Software as a service or simply hosted applications is hosted remotely. SaaS allows the same software to be accessed on all devices over the cloud. Example Facebook, sales force, Google apps, workday are some of the providers that use SaaS applications.

B. Platform as a Service (PaaS):

PaaS, as the name says, it provides computing platform for the development and up gradation of software, delivered over the web. It provides various interrelated activities for the software like testing, deploying hosting and maintaining different UI scenarios. Platform as a service also provides tools that can be used to handle billing and subscription management like operating system handles and manages all the work and acts as a platform in which all software applications run, same as that is Hadoop, Amazon web services (AWS), Mendix, Appear IQ.

C. Infrastructure as a Service (IaaS):

The services infrastructure as a service deals with operating systems, network connectivity and storage. The user needs not to operate the internal infrastructure. Infrastructure services provided by cloud vendors, allow any user to provision a large number of compute instances fairly easily [9].

D. Data as a Service (DaaS):

Like all the services, data is integrated in a form that is understandable to users and are accessible to it regardless of any geographical or network organization. This provides cloud users with protected, well updated and affordable data. Also, data which is accessed has a single update point which facilitates its accessibility to be in more controlled way which ultimately leads to good quality of data. However, security issues on one single voluminous data are applied which make it easier to encrypt in case of any sensitivity.

Example oracle data as a service helps customers deal with their data to access and personalize their experience

E. Network as a Service (NaaS):

Network as a service often called as Communication as a service, delivers its cloud subscribers with the network related services. NaaS provides flexible and extended virtual private network (VPN), bandwidth on demand, custom routing, protocols, firewalls, wide area networks, data maintenance, security methods and antivirus. With the use of appropriate network, subscriber can access to cloud data. So NaaS makes sure the availability of communication lines for better uptime.

F. Storage as a Service (SaaS):

Storage as a service compensates for the data that is, it keeps the data to some other party. That is why it is also considered as a kind of model which is deployed in such a way that keeps the storage space in other third company. However this kind of approach is useful in small sized organizations that may not be able to build or maintain large storage structures.

IV. COMPLIANCE MODEL

Compliance model issues arise as soon as you make use of cloud storage or backup services. By moving data from your internal storage to someone else's you are forced to examine closely how that data will be kept so that you remain compliant with laws and industry regulations. So, when it comes to cloud compliance what data should you move to the cloud and what should be kept in-house.[14] It has a strong connection between the security control model and the cloud model. Whenever we are using the compliance model it simply means that we have to follow the rules and regulations that are provided by the services. They have firewall, code review, WAF, Encryption, Unique user IDs, Anti Virus, Monitoring, Patch, Vulnerability Management, Physical access control and two factor authentications. Compliance model is implemented on the services provided by the service model of the cloud computing. The services are Iaas (Infrastructure as a service), Paas (platform as a service), Saas (storage as a service), Saas (software as a service), Naas (Network as a service).

V. SECURITY CONTROL

Security control model is the layered model. It is similar to TCP/IP Model in Networks. It follows bottom to up approach. It starts from Physical Layer and finishes with Application Layer. Security is controlled within these layers. This model comprises of seven layers i.e. Physical, compute & Storage, trusted computing, Network, management, information and applications.

1) Physical Layer: physical layer deals with the physical plant security, CCTV and Guards.
2) Compute & Storage Layer: Host based firewalls, HIDS/HIPS, integrity & file/log management, encryption, masking.

3) Trusted Computing Layer: Hardware & Software ROT and APIs.
4) Network Layer: NIDS/NIPS, Firewalls, DPI, Anti DDOs, QOS, DNSSEs, Q Auth.
5) Management Layer: GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring.
6) Information Layer: DLP, CMF, Database Activity Monitoring, Encryption.
7) Applications Layer: SDLC, Binary analysis, Scanners, Web App Firewalls, Transactional Sec.

Security Control model helps the administrator to find the Gap between the Cloud Model and Compliance Model.

VI. CONCLUSION

We analyzed that service models are fully dependent on the security control and the compliance model for the security. Security is provided by the administrator to the end users or to the clients. Users should always keep in mind that which type of data is kept on the cloud page and which is kept in house. The aim of this research is to understand the cloud types, service models, security control model and compliance model. This is basically a review paper. This paper concludes that security is very important from data saver point of view. Data is arranged in the systematic order at the server side or at the different clouds like public cloud, private cloud, hybrid cloud and community cloud.

REFERENCES

[1] CSA Guidance version 3.
[2] Kaur S, Tanisha.(2016). *CLOUD COMPUTING- IN A MORE GENERAL SCOPE, gajets*,
[3] Cloud Computing works " *priyathevaishnavite.files.wordpress*",2014
[4] Search cloud computing TEC target website " *searchcloudcomputing.techtarget.com*",2013
[5] D.E.Y.Sarna," *Implementing and developing cloud computing applications*," Taylor and Francis Group, Boca Raton, FL:CRC Press,2011.
[6] Emma Trend Micro Website "emea.TrendMicro.com"Cloud Security/ hybridcloud-krish_110624 us.pdf, 2013.
[7] A.Stevens, "*When hybrid clouds are a mixed blessing*," The Register, June 29, 2011.
[8] J. Ekanayake and G. Fox, "*High performance parallel computing with clouds and cloud technologies*," In: Cloud Computing (pp. 20-38). Springer Berlin Heidelberg,2010.
[9] Aws. "*Amazon website*" aws.amazon.com, 2012.
[10] J. Hurwitz, R. Bloor, M. Kaufman and F. Halper, "*Cloud computing for dummies*," Wiley Publishing, Inc., Indianapolis, Indiana, 2010.
[11] O. Hamren "*Mobile phones and cloud computing*" M.S. Thesis,2012.
[12] RydhmBeri and VeerawaliBehal,"*Cloud Computing: A Survey on Cloud Computing*", IJCA, Feb, 2015.
[13] http://www.ibm.com/developerworks/websphere/techjournal/1206_dejesus/1206_dejesus.html
[14] http://www.computerweekly.com/podcast/Cloud-compliance.