ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

A Survey on Cloud Computing Levels and Their Security Models

Ashwini R. Dhange, Rashmi K. Dixit

Department of Computer Science and Engineering, Walchand Institute of Technology, Solapur, Maharashtra, India

ABSTRACT: Currently cloud computing is being the organizations and industrial need. It is delivery of computing services like storage, servers, software, databases, analytics, networking and more over the Internet or the cloud. And these services provided by Companies are called cloud providers and depending on usage it charge for cloud computing services. Cloud computing has different levels such as Iaas, Paas and Saas. Each level has security paradigm or models. Security is the main aspect of the cloud computing like data loss, data leakage and disclosing of personal data or secret data. This paper presents a survey of existing cloud computing levels and their security models.

KEYWORDS: Cloud computing, Cloud Computing levels, Cloud Computing Security and models, Cloud Deployment Model.

I. INTRODUCTION

Cloud computing is one of the most essential core technology in the modern era. It has most effective across IT, software engineering, businesses and data storage. The main effects are the increase of their capability and availability. The National Institute of Standards and Technology (NIST) definition, the cloud computing is important for enabling convenient, resource pooling, on-usage based access which can be easily delivered with different types of service provider interaction.

The cloud computing follows pay as you go (PAYG) structure where you pay whichever services you have used. One of the major benefits of PAYG structure is that it can reduce expenditure by provisioning a certain amount of resources. The client can request processor, memory, hard disk, operating system, net- working, access control and any additional new software as required to their environment. The resources provided on-demand to the customer or end users. It provides benefits to industry and home users and attracts the attention of the research community.

Cloud computing provides distributed computing services, utility computing, fast deployment, pay for use, lower cost, elasticity, greater network access, disaster recovery, on demand security control and other more benefits. It provides greater flexibility and cost effective services. Cloud computing has greater scalability and availability characteristics. Industries, organizations and individuals have benefits of cloud in term of economic savings, resource sharing and outsourcing mechanism. Cloud provides these services at any-time and any-where on demand based and flexible services.

Cloud computing has four deployments model that are Private Cloud, Public Cloud, Community Cloud and Hybrid Cloud. Deployment model controls the operating cost and reduces the power of servers.

DOI: 10.15680/IJIRCCE.2018. 0611059

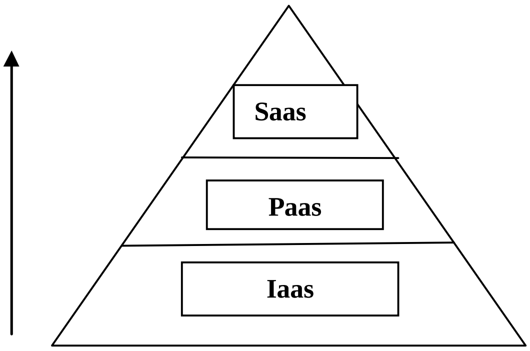

Figure 1: Cloud Computing Levels

The cloud computing works within the data center of an organization is called Private Cloud. The cloud computing works in open environment is called public cloud. Cloud computing infrastructure operates and managed by any organization in community is called Community Cloud. Hybrid cloud is the combination of all deployment clouds models.

The cloud computing provides three computing levels such as infrastructure as a service (Iaas), Platform as a service (Paas) and Software as a service. Figure1 shows the layered view of the cloud computing levels such as upper level is software as service level middle level is Platform as service level and lower level is Infrastructure as service level.

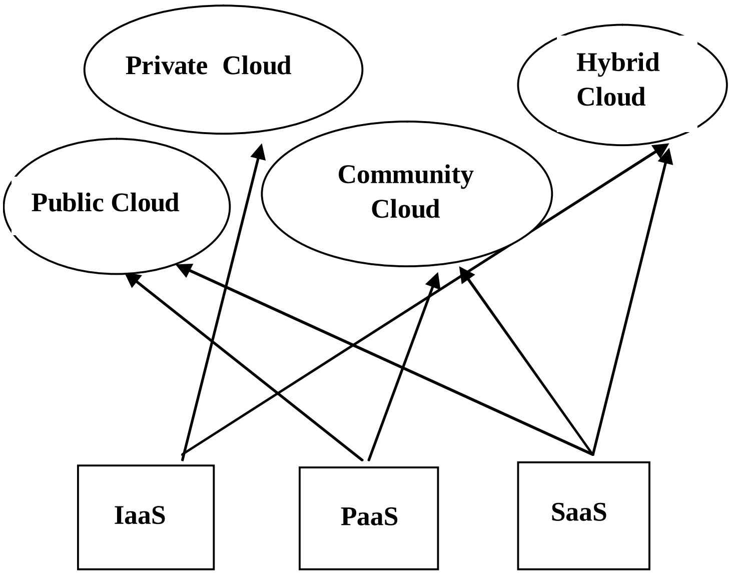

Figure 2: Cloud levels and Cloud deployment Model

Software application comes into the Saas level this is the highest level. The example of the software application is email system, Salesforce.com, WebFilings, NetSuite, Lotus etc. Middle level is Paas level it defines platform for which to develop and host the applications.

Example of Paas is Windows Azure, GoogleApp Engine, Force.com, Amazon Elastic Beanstalk, VMware CloudFoundry etc. lowest level is Iaas level that introduce infrastructure where to put hardware. Example of Iaas is Google Cloud Storage, VMware, Amazon EC2, Rackspace etc.

Cloud provides security in different levels such as physical level, virtual level, network level, interface level, operating system level, database level and application level. For example the applications which cloud provides security in that such as Email, CRM, ERP, collaborative, application development, web, streaming, caching, legacy, and networking etc.

II. CLOUD SERVICE LEVELS

There are three service levels of the cloud computation such as Infrastructure as a Service level (IaaS), Platform as a Service level (PaaS) and Software as a Service level (SaaS).

A. Infrastructure as Service Level (IaaS):

Cloud Service Provider (CSP) is the main part of the cloud computing system. Cloud service provider provides hardware, networking components and storage to Iaas consumer. CSP is responsible for the managing and maintaining their services. IaaS creates platform for service and application test, development, integration and deployment. Iaas contains dynamic scaling, desktop virtualization, service level agreement, utility computing service and billing model and automation of administrative task.

IaaS provides virtual machines, operating system, message queue, network, storage, CPU, memory backup services. IaaS works in Private and Hybrid cloud environment. The example of IaaS application is Amazon EC2, Rackspace, VMware, Google Cloud Storage and Joyent etc.

Security model in IaaS:

IaaS provides network level security, virtual machine security, operating system level security and storage level security. There are security threats between the virtual machines like monitoring VM form other VM, communication between VMs and denial of service. Virtual machine security is VM identification, virtualization, and virtual machine management. Network security includes secure data transmission, data sharing with authorized user and transparent security protocols. IaaS provides privacy controls such as data location privacy, cryptography technique for data security and hidden and redundant backup of data.

B. Platform as a Service Level (PaaS):

Platform as a service level is the middle level of the cloud computing levels. It is placed between SaaS and IaaS service level. PaaS includes developers and deployers. It provides services and application test, development, integration and deployment. It creates or deploys application and services for users. It supports operating system such as windows/.NET, Linux/J2EE, applications of choice deployed. In this level customer crested applications deployed to the cloud. PaaS includes database, web server, and execution runtime and development tools.

It provides a service to developers a complete software development lifecycle management tool, from planning to designing to building applications to deployment to testing to maintenance. This is abstracted away from the viewpoint of the developers. This advantage of PaaS is that, it is helpful to hacker to leverage the PaaS cloud infrastructure for malware command and control and go behind IaaS applications.

The example of PaaS application is Google App Engine, Force.Com, Windows Azure, RollBase and Amazon ElasticBeanstalk etc. PaaS works in the public and community cloud environment. PaaS has some advantages to the developer such as os can be changed and upgraded as many times as needed. It allows geographically distributed team for sharing information and develop software projects.

Security Model in PaaS:

PaaS allows developers to build their own applications on top of the platform. As a result it is more extensible than SaaS, at the expense of customer-ready features. This extends to security features and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security.

The application security metrics are available that are vulnerability scores and patch coverage. These metrics provides quality of application coding. The main focus will have been given to how malicious actors react to new cloud application architectures that obscure application components from their scrutiny. Hackers are attack visible code, including but not limited to code running in user context. They attack the infrastructure and perform extensive manual testing.

The vulnerabilities of cloud are associated with the web applications and it associated with the machine-to-machine Service- Oriented Architecture (SOA) applications, which are increasingly being deployed in the cloud.

PaaS security involves the tools that PaaS provider provides is cross site scripting, SQL injection etc. Scanning the web application and sanitized test data is the steps for securing data.

The PaaS security features are:

- Host Vulnerability
- Access Control
- Object Vulnerability
- Interoperability
- Privacy Aware Authentication

C. Software as a Service Model (SaaS)

As the top most level is the SaaS service model. This is also called as software distribution model. Here cloud provider host applications and make it available to customer in the cloud. The cloud service provider provides the software and maintains software application and installs new software. SaaS allows customer to purchase software on rent and execute it online instead of purchasing it to install on in house computer. SaaS is based on a multitenant architecture. It means a single version of the application, with a single configuration is used for all customers. SaaS cloud service model has some benefits such as cost reduction, flexibility, reduce risk and reliability.

Cost Reduction: The organization does not need to make significant initial investments. It eliminates the upfront commitment of resources and nothing to buy or maintain in term of network or hardware.

Flexibility: Here infrastructure scales rapidly to cope with customers need. IT department can focus on high value activity truly aligned with business goals. It has global availability the functionality is available from anywhere.

Reduce Risk: SaaS application try the software before contracting the service. Data are replicated on backup server. It has shorter deployment time and avoid typical project overruns.

Reliability: SaaS provides better reliability. It upgrates on time and sites are monitored by highly qualified operators 7*24.

SaaS applications accessed using web browser. SaaS provider provides services like Email, Office Automation, CRM, Website testing, Wiki, Blog and Virtual desktop.

Security Model in SaaS: SaaS is deployed for sales force automation and Customer Relationship Management (CRM). It is the platform for many business tasks, including computerized billing, invoicing, human resource management, financials, document management, service desk management and collaboration. The applications are accessed using web browsers over the Internet. So web browser security is vitally important. Information security head will need to consider different methods of securing SaaS applications. The security provided like Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet. The service provider verify that their multiple users do not violates privacy of the other users, also it is very important for user to verify that the proper security measures are in place mean while it is difficult to get an assurance that the application will be available when needed.

The SaaS security threats are data confidentiality, availability, authentication and authorization, information security, identity management, data access and data breaches, web application security and virtualization vulnerability security.

III. CLOUD DEPLOYMENT MODEL

There are four deployment models for the cloud computation such as Private cloud, Public cloud, community cloud and hybrid cloud.

1. Private Cloud

The private cloud used in the business units that is it is for single organization comprising multiple consumers. In the private cloud security risk are easier to detect because of the infrastructure owned and operated by the same organization so they easily find out the customer and vendor relationship.
Private cloud managed by the internal resources. It is created and maintained by an individual enterprise. Private cloud suited for secured confidential information and core systems. Virtualized resources are shared privately.

2. Public Cloud

There is a third party cloud service provider which can operate and owned cloud resources and delivers it over the internet. The example of public cloud is Macrosoft Azure, Amazon Web services etc. In public cloud the service provider makes resources available to public over the internet. The public cloud resources are free of cost or may be pay per usage based. Public cloud reduces the need for organization to invest in and maintain their own on premises IT resources.
There are few wasted resources because customers only pay for the resources they use. It is virtualized environment. Public cloud architecture is the multitenant architecture that enables users or tenants to share resources.

3. Community Cloud

A community cloud provides a cloud computing solution to a limited number of individuals or organizations that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider.
Community cloud will reside to a government of a single country. Community cloud located both on and off premises. Community cloud provides an infrastructure that is shared between organizations, usually with the shared data and data management concerns.

4. Hybrid Cloud

Hybrid cloud is the combination of all deployment cloud model such as private cloud, public cloud and community cloud. Public cloud interacts with customers, while keeping their data secured through a private cloud. In the hybrid cloud model the private cloud connected with public cloud infrastructure, allowing an organization to manage workloads across the two environments. The public cloud adequately becomes an extension of the private cloud to form a single, uniform cloud. It requires a high level of compatibility between the software and services used by both the public and private clouds.

IV. REVIEW PAPER

Nowadays cloud computing is famous and important technology in the world. Cloud computing enables companies to focus on their core businesses and avoid expending resources on computer infrastructure. It allows minimizing infrastructure costs. Cloud computing enables organization to get their applications faster, with improved manageability and less maintenance.
Cloud security is the important aspect in the cloud environment. There are different security models in the cloud computing infrastructure. Cloud security includes set of policies, technologies, and controls deployed to protect data,

applications, and the associated infrastructure. It comes under computer security, network security and information security. Different cloud service levels have different security aspect.

V. CONCLUSION

This survey paper shows the various service levels and deployment models of the cloud computing and shows their security model. Cloud computing is rapidly running and effective technology in the current IT sector and the organizations. Cloud computing will have more focus on the security issues in different levels.

REFERENCES

1. A survey on cloud computing security: Issues, threats, and solutions- SaurabhSingh a, Young-SikJeong b, JongHyukPark.
2. A survey of Cloud Computing Security challenges and solutions- Ahmed Khalid Salih.
3. A survey on security issues in service delivery models of cloud computing- S. Subashini n, V. Kavitha.
4. Software as a Service (SaaS): Security issues and Solutions -International Journal of Computational.
5. Infrastructure as a Service: Security Issues in Cloud Computing- International Journal of Computer Science.- P. R. Jaiswal, A. W. Rohankar.
6. Virtualization and Cloud Computing Threat Report- Trend Micro.
7. Security Problems of Platform-as-a-Service (PaaS)Clouds and Practical Solutions to the Problems- Mehmet Tahir, Ali Emre.
8. Cloud Computing Security Considerations- Australian government department of defense.
9. An analysis on security concerns and their possible solutions in cloud computing environment- Dr. Jayant Shekhar1.
10. A Survey on Virtual Machine Security- Jenni Susan Reuben.