Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Issues in Cloud Computing Services

G.Harish Reddy*
Asst. Prof, Dept of Computer Application,
SNIST, Hyderabad
A.P., India

K. Venkat Reddy, S.Uttam Raj., **K.Jeevana Jyothi**
Dept of Computer Application,
SNIST, Hyderabad
A.P., India

Abstract: - Cloud computing is an increasingly popular paradigm for accessing computing resources. Cloud Computing holds the potential to eliminate the requirements for setting up of high cost computing infrastructure for the IT-based solutions and services that the industry uses. It promises to provide a flexible IT architecture, accessible through internet for lightweight portable devices. Cloud service providers tend to offer services that can be grouped into three categories: software as a service, platform as a service, and infrastructure as a service. This paper aims to provide a means of understanding and investigating IaaS, PaaS, SaaS. Internet has been a driving force towards the various technologies that have been developed. Arguably, one of the most discussed among all of these is Cloud Computing. Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it. The advantages of using cloud computing are: i) reduced hardware and maintenance cost, ii)accessibility around the globe, and iii) flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter.

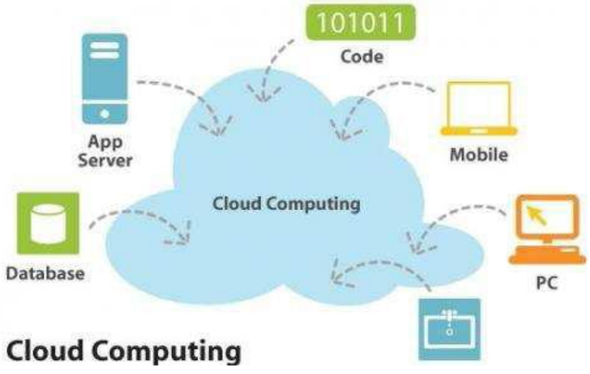
Keywords – Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS).

I. INTODUCTION

Cloud computing can be considered a new computing paradigm with implications for greater flexibility and availability at lower cost. Because of this, cloud computing has been receiving a good deal of attention lately. Cloud computing services benefit from economies of scale achieved through versatile use of resources, specialization, and other efficiencies. However, it is an emerging form of distributed computing still in its infancy. The term itself is often used today with a range of meanings and interpretations. According to the different types of services offered, cloud computing can be considered to consist of three layers. IaaS or Infrastructure as a Service is the lowest layer that provides basic infrastructure support service. PaaS or Platform as a Service layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications. SaaS or Software as a Service is the topmost layer which features a complete application offered as service on demand SaaS ensures that the complete applications are hosted on the internet and users use them. In the Platform as a service approach, the offering also includes a software execution environment. Infrastructure as a service refers to the sharing of hardware resources for executing services, typically using Virtualization technology.

II. WHAT IS CLOUD COMPUTING?

Cloud computing is Internet("CLOUD") based development and use of computer technology ("COMPUTING").Cloud computing is a general term for anything that involves delivering hosted services over the Internet. It is used to describe both a platform and type of application. These cloud applications use large data centers and powerful servers that host Web applications and Web services. Anyone with a suitable Internet connection and a standard browser can access a cloud application.[1]



In this paper we discuss about
i)Cloud computing services
ii)Cloud computing security issues
iii)Cloud computing deployment models

III. CLOUD COMPUTING SERVICES

A .Infrastructure as a service (IaaS)

Infrastructure as a service is taking the physical hardware and going completely virtual (e.g. all servers, networks, storage, and system management all existing in the cloud). This is the equivalent to infrastructure and hardware in the traditional (non-cloud computing) method running in the cloud. In other words, businesses pay a fee (monthly or annually) to run virtual servers, networks, storage from the cloud. This will mitigate the need for a data center, heating, cooling, and maintaining hardware at the local level. Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities.

Characteristics[2] and components of IAAS include:

- Utility computing service and billing model
- Automation of administrative tasks
- Dynamic scaling
- Desktop virtualization
- Policy-based services
- Service level agreement (SLA)
- Cloud software
- Platform virtualization

B. Platform as a service (PaaS)

Platform as a service is a category of cloud computing services that provides a computing platform and a solution stack as a service. Along with software as a service (SaaS) and infrastructure as a service (IaaS), it is a service model of cloud computing. In this model, the consumer creates the software using tools and/or libraries from the provider. The consumer also controls software deployment and configuration settings. The provider provides the networks, servers, storage and other services. [3] PaaS offerings facilitate the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities. [4] There are various types of PaaS vendor; however, all offer application hosting and a deployment environment, along with various integrated services. Services offer varying levels of scalability and maintenance. PaaS offerings may also include facilities for application design, application development, testing and deployment as well as services such as team collaboration, web service integration and marshalling, database integration, security, scalability, storage, persistence, state management, application versioning, application instrumentation and developer community facilitation.

i.Types

Add-on development facilities:

These facilities allow customization of existing software-as-a-service (SaaS) applications, and in some ways are the equivalent of macro language customization facilities provided with packaged software applications such as Lotus Notes, or Microsoft Word. Often these require PaaS developers and their users to purchase subscriptions to the co-resident SaaS application.

Stand alone development environments :

Stand-alone PaaS environments do not include technical, licensing or financial dependencies on specific SaaS applications or web services, and are intended to provide a generalized development environment.

Application delivery-only environments:

Delivery-only PaaS offerings do not include development, debugging and test capabilities as part of the service, though they may be supplied offline (via an Eclipse plug-in for example [5]). The services provided generally focus on security and on-demand scalability.

Open platform as a service:

This type of PaaS does not include hosting as such, rather it provides open source software to allow a PaaS provider to run applications. For example, AppScale allows a user to deploy some applications written for Google App Engine to their own servers, providing datastore access from a standard SQL or NoSQL database. Some open platforms let the developer use any programming language, any database, any operating system, any server, etc. to deploy their applications.

ii. Key characteristics

Ease of use:

PaaS platforms are commonly designed around developer ergonomics to maximise developer productivity.

Simplicity:

PaaS allows resources to be focused on value add development effort by removing the need for most non-differentiating project tasks associated such as provisioning and managing environments.

Automation:

PaaS platforms make aggressive use of automation to eliminate repetitive tasks that add no value, instead allowing developers to focus on high-value differentiating features.

Multi-tenant architecture:

PaaS offerings typically attempt to support use of the application by many concurrent users, by providing concurrency management, scalability, fail-over and security. The architecture enables defining the "trust relationship" between users in security, access, distribution of source code, navigation history, user (people and device) profiles, interaction history, and application usage.

iii. Full development PaaS characteristics

Services to develop, test, deploy, host and maintain applications in the same integrated development environment:

Different PaaS offerings provide different combinations of services to support the application development life-cycle. A comprehensive development PaaS might provide service options in an integrated development environment within the actual target delivery platform. It could include source code control, version control, user testing, roll out and roll back with the ability to audit and track who made what changes when and which task they were accomplishing.

Web-based user-interface creation tools:

Some PaaS offerings provide a level of support to ease the creation of user interfaces, either based on standards such as HTML and JavaScript or other Rich Internet Application technologies like Adobe Flex, Flash and AIR. This might allow rich, interactive, multi-user environments and scenarios can be defined, tried out by real people (non-programmers), with tools that make it easy to log/single out features that annoy or frustrate either novices or experts. Creation tools might allow interfaces to be defined for different user profiles by function or expertise.

Support for development team collaboration:

The ability to form and share code with ad-hoc or pre-defined or distributed teams could potentially enhance the productivity of PaaS offerings. In some cases, schedules, objectives, teams, action items, owners of different areas of responsibilities, roles (designers, developers, tester, QC) can be defined, updated and tracked based on access rights.

Utility-grade instrumentation:

PaaS offerings provide developers some insight into the inner workings of their applications, and the behavior of their users. Some PaaS offerings use information about user behaviour to enable pay-per-use billing. Historical usage and logs may help:

- determine whether services are of value to users/customers
- compare the value of different services
- track activity based costs and revenues

Visualization tools could show usage patterns, exposing functional or correlational relationships between:

- services and/or user interactions
- the value to the user or users
- the cost of alternative service paths such as web, mobile browser or mobile applications

Business benefits of PaaS

Cost savings:

PaaS platforms help improve the efficiency of core IT processes that form part of application delivery in an organization. They facilitate creation of applications and services without the cost and complexity of provisioning and managing a traditional application platform stack.

Shortened application delivery:

PaaS supports and amplifies the benefits of agile software development methodologies. When used in combination with an agile development methodology PaaS can help significantly reduce the time to value of software application projects.

Increased adaptability:

PaaS reduces environmental complexity and therefore enables businesses to more rapidly adapt their applications and IT services to respond to changing market conditions and organisational needs.

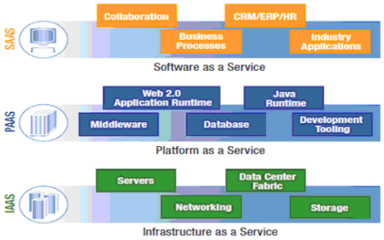


Fig: service models in cloud computing

C. Software as a Service

Software –as-a-service is the process of provisioning commercially available software but giving access over the net. oftware as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new developmental approaches, such as Ajax, become popular. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for SaaS. The *hosted application management* (*hosted AM*) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the *software on demand* model, the provider gives customers network-based access to a single copy of an application created specifically for SaaS distribution.

Characteristics of SaaS:

- configuration and customization
- accelerated feature delivery
- Open integration protocols
- Collaborative(and"social") functionality
- Adoption drivers and challenges
- Criticism

Benefits of the SaaS model include:

- easier administration
- Automatic updates and patch management.
- Compatibility: All users will have the same version of software.
- Easier collaboration, for the same reason.

IV. CLOUD COMPUTING SECURITY ISSUES

A. Issues in IaaS:

i. Security

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft

ii.Privacy

Privacy advocates have criticized the cloud model for hosting companies' greater ease can control—and thus, can monitor at will—communication between host company and end user, and access user data (with or without permission). Instances such as the secret NSA program, working with AT&T, and Verizon, which recorded over 10 million telephone calls between American citizens, causes uncertainty among privacy advocates, and the greater powers it gives to telecommunication companies to monitor user activity. A cloud service provider (CSP) can complicate data privacy because of the extent of virtualization (virtual machines) and cloud storage used to implement cloud service. CSP operations, customer or tenant data may not remain on the same system, or in the same data center or even within the same provider's cloud; this can lead to legal concerns over jurisdiction. While there have been efforts (such as US-EU Safe Harbor) to "harmonise" the legal environment, providers such as Amazon still cater to major markets (typically the United States and the European Union) by deploying local infrastructure and allowing customers to select "availability zones." Cloud computing poses privacy concerns because the service provider may access the data that is on the cloud at any point in time. They could accidentally or deliberately alter or even delete information.

iii. *Reliability*

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

iv. Sustainability

Although cloud computing is often assumed to be a form of *green computing*, no published study substantiates this assumption. Citing the servers' effects on the environmental effects of cloud computing, in areas where climate favors natural cooling and renewable electricity is readily available, the environmental effects will be more moderate. (The same holds true for "traditional" data centers.) Thus countries with favorable conditions, such as Finland, Sweden and Switzerland, are trying to attract cloud computing data centers. Energy efficiency in cloud computing can result from energy-aware scheduling and server consolidation. However, in the case of distributed clouds over data centers with different source of energies including renewable source of energies, a small compromise on energy consumption reduction could result in high carbon footprint reduction.

v. Open Standard

Open standards are critical to the growth of cloud computing. Most cloud providers expose APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs and there are a number of open standards under development, including the OGF's Open Cloud Computing Interface. The Open Cloud Consortium (OCC) is working to develop consensus on early cloud computing standards and practices.

vi. Long-term Viability

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application.

B. Issues in PaaS:

i. Vendor lock-in

Because cloud computing is still relatively new, standards are still being developed. Many cloud platforms and services are proprietary, meaning that they are built on the specific standards, tools and protocols developed by a particular vendor for its particular cloud offering. This can make migrating off a proprietary cloud platform prohibitively complicated and expensive.

Three types of vendor lock-in can occur with cloud computing:[6]

- Platform lock-in: cloud services tend to be built on one of several possible virtualization platforms, for example VMWare or Xen. Migrating from a cloud provider using one platform to a cloud provider using a different platform could be very complicated.
- Data lock-in: since the cloud is still new, standards of ownership, i.e. who actually owns the data once it lives on a cloud platform, are not yet developed, which could make it complicated if cloud computing users ever decide to move data off of a cloud vendor's platform.
- Tools lock-in: if tools built to manage a cloud environment are not compatible with different kinds of both virtual and physical infrastructure, those tools will only be able to manage data or apps that live in the vendor's particular cloud environment.

ii. Technical Immaturity [8] Every cloud framework has its own interface methods, services and costs. The unfolding nature of the platform-as-a-service approach puts everything at risk costs could change overnight, services could be dropped, and quality of service could worsen.Standards bodies are just beginning to look at the market. Would you bet a critical business application on such a new arrival?

iii. Privacy and Control Vendors generally offer extensive protection methods, and it’s in their interests to offer high levels of security. PaaS often provides a relatively sophisticated suite of access controls. But you, not the vendor, still own the risk.

iv.Misjudging “Flexibility versus Power” Generally, you want more flexibility over design, development and deployment for a custom system such as a new profit center and PaaS doesn’t offer flexibility. Instead, it gives power and ready-made services. The trade-offs are similar to the ones for outsourcing.

C. Issues in SaaS:

i. Ad-Hoc/Custom – One Instance per customer

The first level of maturity is actually no maturity at all. Each customer has a unique, customized version of the hosted application. The application runs its own instance on the host`s servers. Migrating a traditional non-networked or client-server application to this level of SaaS maturity typically requires the least development effort and reduces operating costs by consolidating server hardware and administration.

ii. Configurable per customer

The second level of SaaS maturity provides greater program flexibility through configuration metadata. At this level,many customers can use separate instances of the same application. This allows a vendor to meet the varying needs of each customer by using detailed configuration options. It also allows the vendor to ease the maintenance burden by being able to update update a common code base.

iii.Configurable & Multi-Tenant-Efficient

The third maturity level adds multitenancy to the second level. This result in a single program instance that has the capability to serve all of the vendor`s customers. This approach enables more efficient use of server resources without any apparent difference to the end user, but ultimately this level is limited in its ability to scale massively.

iv. Scalable, Configurable & Multi-Tenant-Efficient

At the fourth SaaS maturity level, scalability is added by using a multitier architecture. This architecture is capable of supporting a load-balanced farm of identical application instances running on a variable number of servers, sometimes in the hundreds or even thousands. System capacity can be dynamically increased or decreased to match load demand by adding or removing servers, with no need for further alteration of application software architecture.

Further issues to consider:

Even having taken these precautions, CISOs should be aware that risks persist with the IaaS model. There are still issues with how much visibility the customer has into their cloud environment – access to the cloud provider's physical or admin access logs could be denied and visibility into network traffic may not be high enough for some organizations, for example. Also, the lack of role-based account access in certain IaaS packages may be problematic for some organizations.

V. Computing Deployment Models

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand as depicted in figure. The Cloud Computing model has three main deployment models which are:

1. Private cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.

2. Public cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

3. Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network It provides virtual IT solutions through a mix of both public and private clouds. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets.

For example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.

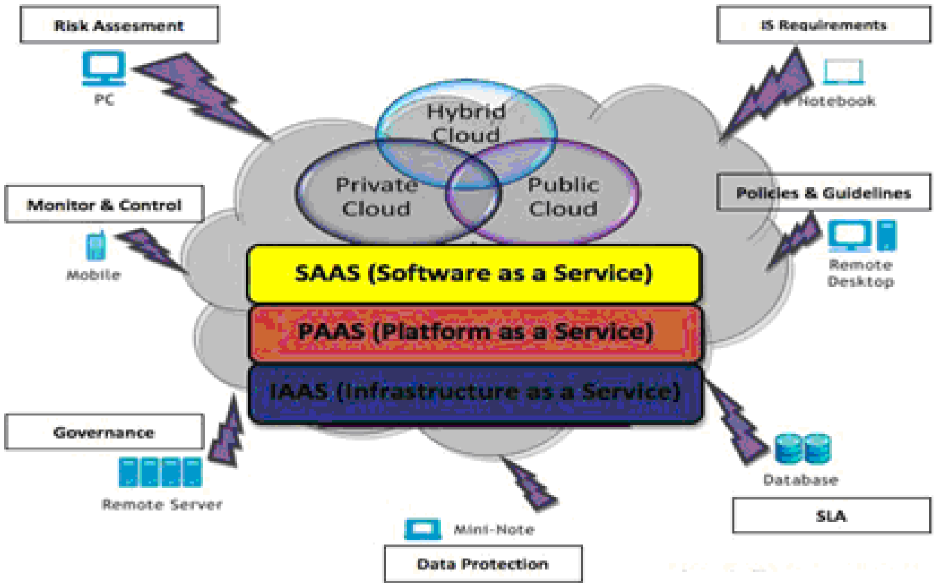


Fig: Deployment models in cloud computing

VI. ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING

- *On demand self services:* computer services such as email, applications, network or server service can be provided without requiring human interaction with each service provider. Cloud service providers providing on demand self services include Amazon Web Services (AWS), Microsoft, Google, IBM and Salesforce.com. New York Times and NASDAQ are examples of companies using AWS (NIST). Gartner describes this characteristic as service based.

- *Broad network access*: Cloud Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops and PDAs.

- *Resource pooling:* The provider's computing resources are pooled together to serve multiple consumers using multiple-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The resources include among others storage, processing, memory, network bandwidth, virtual machines and email services. The pooling together of the resource builds economies of scale (Gartner).

- *Rapid elasticity:* Cloud services can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- *Measured service:* Cloud computing resource usage can be measured, controlled, and reported providing transparency for both the provider and consumer of the utilised service. Cloud computing services use a metering capability which enables to control and optimise resource use. This implies that just like air time, electricity or municipality water IT services are charged per usage metrics.

- *Pay per use:* The more you utilise the higher the bill. Just as utility companies sell power to subscribers, and telephone companies sell voice and data services, IT services such as network security management, data center hosting or even departmental billing can now be easily delivered as a contractual service.

- *Multi Tenacity:* Is the 6th characteristics of cloud computing advocated by the Cloud Security Alliance. It refers to the need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. Consumers might utilize a public cloud provider's service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure.

VII. BENEFITS OF CLOUD COMPUTING

- Cloud technology is paid incrementally, saving organizations money.[7]
- Organizations can store more data than on private computer systems.
- No longer do IT personnel need to worry about keeping software up to date.
- Cloud computing offers much more flexibility than past computing methods.
- Employees can access information wherever they are, rather than having to remain at their desks.
- No longer having to worry about constant server updates and other computing issues, government organizations will be free to concentrate on innovation.
- Decoupling and separation of the business service from the infrastructure needed to run it
- Flexibility to choose multiple vendors that provide reliable and scalable business services, development environments, and infrastructure that can be leveraged out of the box and billed on a metered basis—with no long term contracts.

VIII. CONCLUSION

In this paper we discuss about various services in cloud computing, its characteristics, security issues and models. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing offers real benefits to companies seeking a competitive edge in today's economy. Many more providers are moving into this area, and the competition is driving prices even lower. Attractive pricing, the ability to pay for "as needed" services will continue to drive more businesses to consider cloud computing.

REFERENCES

[1] Sushil Bhardwaj, Leena Jain, Sandeep Jain, ―Cloud computing: a study of Infrastructure as a service (Iaas) IJEIT 2010, 2(1), pp 1-4.

[2] Pankaj Arora,R.C.Wadhawan,Er.Satinder pal Ahuja-Cloud computing security issues in infrastructure as a service IJARCSSE,2012.

[3] The NIST Definition of Cloud Computing". National Institute of Science and Technology. Retrieved 24 July 2011.

[4] Google angles for business users with 'platform as a service'

[5] Using the Google Plugin for Eclipse.

[6] Hinkle,Mark.(2010-6-9)"Threecloud lock-in considerations", Zenoss Blog

[7] L. Wang, G. Laszewski, M. Kunze and J. Tao, ―Cloud computing: a perspective study, *J New Generation Computing*, 2010, pp 1-11.

[8] InformationWeekanalytics.com,Dr.dobb`s Cloud computing: Platform as a service.