Journal of Theoretical and Applied Information Technology
31st January 2014. Vol. 59 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FOREMOST SECURITY APPREHENSIONS IN CLOUD COMPUTING

[1]H. KAMAL IDRISSI, [2]A. KARTIT, [3]M. EL MARRAKI
[1,2,3] University Mohammed V – Agdal Rabat, Faculty of Sciences, LRIT
4 Avenue Ibn Battouta. BP 1014 RP 10006 Rabat, Morocco
E-mail: [1]h.kamalidrissi@gmail.com, [2]alikartit@gmail.com, [3]elmarrakimohamed@gmail.com

ABSTRACT

In the recent years, a term keeps coming in the sphere of IT. This new concept called cloud computing is probably the most noteworthy evolution since the arrival of the web. Many business leaders have decided to invest in this architecture in order to gain in terms of saving on material and human resources. Cloud computing can outsource the IT hub of a company, therefore it can focus on its own business. Cloud computing is not only full of benefits. Indeed, it is still subject to several threats related to security which is now must be implemented at a large scale so the transition to the cloud should be attended by some adaptations to export all the known security arsenal. Besides, billing within cloud services does not obey until now to precise and deterministic rules and many companies are crying foul when they are charged with an extortionate price. Cloud computing has certainly turned upside down the practices of business and IT professionals need to review their careers. However, some still do not dare to step into this architecture and they claim that more research effort must be done in order to fill the gaps in the cloud. This paper targets to afford a best description of cloud computing features and explore guidelines for research and high-tech tendencies in order to use and implement cloud infrastructure networks. The chief concepts of cloud computer billing and security threats will be also exposed.

Keywords: *Cloud Computing, Large Scale, Focus, Billing, Threat, Security.*

1. INTRODUCTION

The remarkable development of cloud computing in recent years, attracting more and more the interests of different users of the internet and computing professionals looking to enjoy the best services and applications available online through the web which are moreover on-demand usage billing services. This new economic and promising model represents a tremendous and revolutionary approach of investment and operating the IT resources. With cloud computing, organizations, institutions and companies no longer need to invest heavily in resources, inevitably limited, requiring a heavy and expensive internal management. Today they have the choice to migrate to a cloud computing model where they can buy or rent online resources [1]. This architecture allow them to save costs on internal management since resources are administered at the cloud computing provider.

The availability of online services also gives the opportunity to not acquire specific equipment but the companies cloud pay based on the use of resources. This model already fascinate many enterprises, especially small and medium ones. Cloud computing also offers the scalability of hardware and software computing resources in terms of volume and time, according to customer requirements.

Cloud computing fits naturally in the evolution of IT services supply and relies on a series of innovations that preceded it: Grid computing (computer delivered as a service) and Utility Computing (on-demand computing). Big companies has long recognized the cloud computing enormous potential to improve the delivery of IT services to its customers, and to also rationalize and optimize the coverage of its own needs for IT resources. This has led to a very active deployment of cloud computing within leading IT enterprises so they can today react quickly in an economic environment where companies seek to maximize the return on investment and reduce operating costs.

Cloud computing providers can offer an extremely flexible and scalable solutions in order to help enterprises to cope with peak periods requiring to handle an invasion of requests that exceeds their internal IT capabilities. This on demand

Journal of Theoretical and Applied Information Technology
31st January 2014. Vol. 59 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

architecture provide resources (servers, storage and network) needed for business in just a few hours. So thanks to cloud computing, companies could meet the needs of a number of clients without a problem. In parallel, enterprises could significantly improve their productivity and performance [2].With cloud computing, the period of resource provision has been reduced to one day, instead a minimum of a week before. As a result, the ability of the industry has increased dramatically, with a shorter business cycle which is directly reflected in a higher profitability for companies.

Despite these multiple benefits of Cloud Computing, its successful adoption in business requires a prior understanding of this new dynamic IT services. Often, it is necessary to develop a specific expertise in the areas of administration data centers and trade relations before the implementation of the cloud computing concept. There are also number of security encounters that needs to be cautiously addressed. Even though and due to its architectural schema and features, Cloud Computing carry out a number of security aids, which embrace centralization of security, data and process dissection, redundancy and high availability. While many customary risks are handled efficiently, due to the infrastructures remarkable characteristics, a number of distinctive security challenges are introduced.

In our paper, we recall with a concise manner the basics of cloud computing. We aimed to clarify its description through a study that we conducted on various clouds products. The objective at the end of this comparison of cloud solutions is to afford a better understanding of this immensely prosperous pitch of computer science and deduce the main drawbacks and threats affecting its security and billing facets.

This paper is ordered as follows: The first section provides an inclusive definition of cloud computing compared to earlier computing models, the second enumerates the diverse layers and technologies associated with this concept. The third describes the different kinds of cloud computing and reviews the multiple existing solutions. The fourth explain security facets and concerns. The fifth chapter talks about billing problematic and the last one conclude this whole paper.

2. WHAT IS CLOUD COMPUTING?

2.1 Definition

Cloud computing is a recent paradigm. The first Formulation of this concept was in 1960 (John McCarthy), but its implementation never took place until the early 2000 and the upcoming of Web 2.0.Indeed, Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to traditional utilities [3] such as water. As for Utility Computing, it is not a new paradigm of computing infrastructure; fairly, it is a business model in which computing resources, such as computation and storage, are wrapped as metered services similar to a physical public utility, such as electricity and public switched telephone network. Utility computing is typically implemented using other computing infrastructure. In a cloud business model, a customer will pay the provider on a consumption basis, very much like the utility companies charge for basic utilities such as electricity, gas, and water, and the model relies on economies of scale in order to drive prices down for users and profits up for providers. Whether they are software, hardware, platform, or storage providers, they deliver their offerings over the Internet. There are no wrapped boxes containing discs or hardware for you to buy and set up yourself. Thus, the computing world is rapidly transforming towards developing software for millions to consume as a service, rather than to run on their individual computer.

Cloud computing is therefore a new approach based on leveraging the Internet to consume software or other IT services on demand. End users share processing power, storage space, bandwidth, memory and software. With cloud computing, the resources are shared and so are the costs. Users can pay as they consume and only use what they need at any given time, keeping charges to the user cheap. The location of physical resources and devices being accessed are typically not known to the end user. It also provides facilities for users to develop, deploy and manage their applications on the cloud, which entails virtualization of resources that maintains and manages itself.

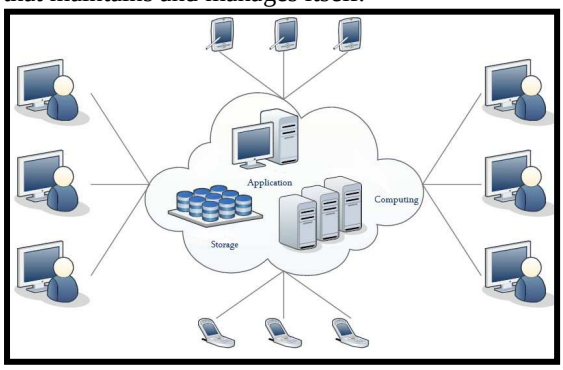

Figure 1: Cloud Components

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The cloud model is composed of five essential characteristics [4]:

1) On-demand self-service. A consumer can separately consume computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2) Access through internet. Capabilities are available over the network and accessed through standard protocols that support use by heterogeneous thin or thick client platforms.

3) Resource sharing. The provider's computing resources are pooled to serve multiple consumers using a multi-pooling model, with different physical and virtual resources dynamically allocated according to consumer demand.

4) Elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale promptly proportionate with demand. To the consumer, the capabilities available for provisioning often appear as nested bricks capable to produce a solution ready for consumption.

5) Monitored. Resource usage can be measured, controlled, and reported, offering transparency for both the provider and consumer of the utilized service.

2.2 The Cloud as an extension of other computing models

There is often some confusion about the difference between Grid vs. Cloud computing. Grid computing is a paradigm that enables the sharing, selection, and aggregation of a wide variety of geographically distributed resources including supercomputers, storage systems, data sources, and specialized devices owned by different organizations for solving large-scale resource-intensive problems in science. The computers that are part of a grid are heterogonous and can run different operating systems belonging to different hardware. Grid is inherently distributed by its nature over a LAN, metropolitan or WAN. The vision [5] of the two paradigms is the same, they aim to reduce the cost of computing, increase reliability, and increase flexibility by transforming computers from something that we buy and operate ourselves to something that is operated by a third party. Nevertheless, Cloud computing is considered as an extension of this paradigm wherein the capabilities of business applications are exposed as sophisticated services that can be accessed over a **network**. Cloud computing moreover use specific next-generation data centers with **virtualized** nodes dynamically provisioned on demand as a personalized resource collection to meet a specific service-level agreement, which is established through a negotiation and accessible as a compostable service via **Web Service** technologies such as SOAP and REST.

3. CLOUD COMPUTING BASICS

3.1 Classification Based on Service Provided

Cloud computing come up with three main layers [6] ranging from infrastructure to application in conjunction with the platform:

3.1.1 IAAS: Infrastructure as a service

Infrastructure as a Service is a cloud service that enables the company to avoid the need to own, manage, maintain, and monitor its own servers and other data processing infrastructure. It is enough to have a PC or laptop connected to the Internet to ensure its business functionality. This access is a form of subscription to entities that sell hardware virtualization services. Reducing acquisition, maintenance and recycling equipment costs is important for businesses. The risk of downtime and business disruption is minimized, given the very high reliability of such online services. In the end, this is a time and money saver for clients of this form of cloud computing. The creation of these virtual and shared clusters is practicable thanks to some leading vendors such as: VMware's VSphere or Microsoft's HyperV Cloud. Some cloud solutions also rely solely on this layer like the Amazon's product EC2, Amazon S3, Rackspace Cloud Servers and Flexiscale.

3.1.2 PAAS: Platform as a service

PaaS is also called "cloudware", this other virtualization service regards provisioning the application developers with online web services development tools. Like IaaS, Paas is not interested in the inner workings of the machine but only willing to exploit a pack of apis, frameworks and databases ready to be deployed. Programmers will then concentrate on optimizing and structuring the code. Cloud computing solutions may simply provide an environment based on a virtual architecture and be limited to the first and second layer, which allows users to reduce costs and access the application and the tools they need. This layer enables the company to retract the costs of training and recruitment of qualified personnel, able to recognize and implement tools and application servers needed to run the final service we can

Journal of Theoretical and Applied Information Technology
31st January 2014. Vol. 59 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

mention in this category Microsoft Windows Azure or Google App Engine.

3.1.3 SAAS: Software as a service

The last layer in the Cloud Computing is defined as a subscription access to Internet applications. Access is online and does not require installation on the local computer. Several applications designed or offered by Google fall into this category of cloud computing. Many of us have probably used these sites where we can upload and share photos and videos with friends and family. These solutions are increasingly popular because users do not need to install and update software at home, they only need to connect and use it when they need it. The picture will probably be stored on a website that uses IaaS service virtualization for its data servers, PaaS software that lets you edit your photo, and SaaS applications that you use to access your email account, or your social networking account to publish your photo and share it with your friends. SAAS include also business services traditionally managed by companies such as customer relationship management (CRM), human resources or mail. The pioneer in this field has been Salesforce.com offering in the online CRM space. Other examples are online email providers like Google Gmail and Microsoft Hotmail, Google docs and Microsoft online version of office called Office 365.

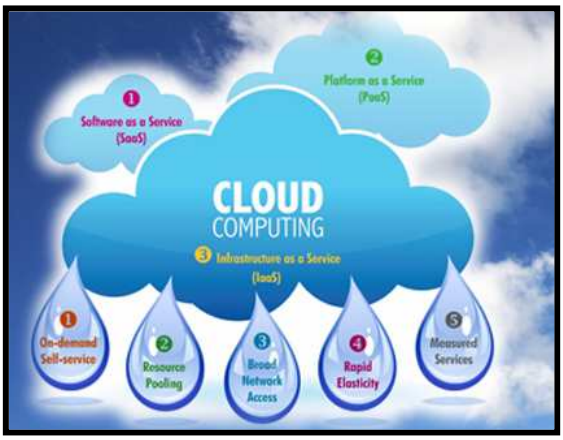

Figure 2: Cloud Computing Layers

3.2 Cloud Computing Types

The cloud has appeared as a convergence of multiple computing trends. It seeks to address certain key facets that may have been missing in each of these tendencies. The features of each of these related technologies and how they compare with cloud computing is shown below.

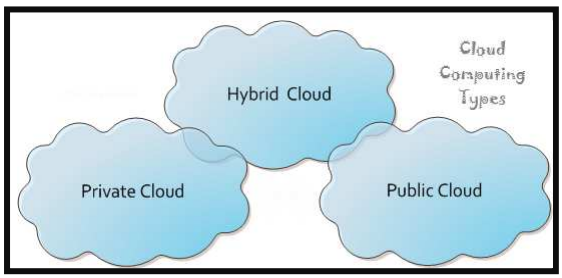

Figure 3: Cloud Computing Types

3.2.1 Public clouds

It is one in which the services and infrastructure are provided off-site over the Internet. These clouds offer the greatest level of efficiency in shared resources, there's no need to worry about security strategies. The platform is scalable and very profitable for collaboration projects. Many IT department executives are concerned about public cloud security and reliability. However, security and governance issues must be well planned, or the short-term cost savings could turn into a long-term nightmare. Typically, public clouds are ran by third parties or vendors over the Internet, and services are provided on pay-per-use basis. Public clouds are widely used in the development, deployment and management of enterprise applications, at reasonable costs.

3.2.1 Private clouds

The infrastructure is set up within the borders of a same company and is used solely for the organization's profits. They are also called internal clouds and are mainly built by IT departments within enterprises who seek to enhance exploitation of infrastructure resources inside them. A private cloud is one in which the services and infrastructure are maintained on a private network. These clouds offer the highest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduces the cost savings. The private cloud is an option for a company when its business is part of an industry that must obey to harsh security and data privacy concerns or the enterprise is huge enough to run a next generation cloud data center proficiently and commendably on its own infrastructure.

3.2.3 Hybrid clouds

A new concept combining resources from both internal and external providers will become the most popular choice for enterprises. For example, a company could select to use a public cloud service for general computing, but store its business critical data within its own data center. By spreading things

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

out over a hybrid cloud, a company keep each aspect of its business in the most efficient environment possible. The downside is to keep track of multiple different security platforms and ensure that all aspects of your business can communicate with each other. Larger organizations are likely to have already invested heavily in the infrastructure required to provide in-house resources or they may be concerned about the security of public clouds [7].

4. SURVEY OF CLOUD PRODUCTS

In this section, we present a survey of some of the leading cloud computing products. This study is a result of a previous paper exposed at last April [8].

4.1 Storage

There is nowadays an overabundance of services in the cloud, some of them are operated by giant companies like Apple, Google, Microsoft or other companies. Smaller vendors have also boarded on the adventure, like Dropbox, Canonical or OVH. Given the multitude of offers, it was time to make a point by comparing the main market players.

Of the five services listed in the table 1 shown at this end of this document, all activate the encryption of exchanges between the users and the servers of the company to prevent anyone from capturing information on the fly. However, it is important to note that all do not offer encryption of files once they arrived at the server, which is a risk to privacy.

Based on our researches and the information we could afford, Google, Microsoft and OVH let the user files as plain data. This obviously does not mean that they are accessible to anyone. Google explains that the connection between the PC and server is secure with HTTPS deployed in the Transport Layer Security.

Conversely, Dropbox and Apple offer encryption information during transfer and during storage. Is that satisfactory? Not quite. It is obviously a stronger security. However, we should underline noted that the master keys are held internally by the firm. Therefore, personnel of this company may potentially access information even encrypted. Does this mean that companies will unscrupulously access customer's data? Probably not. No One imagines a company violating its own protection mechanisms that have been designed to prevent outside intrusion (a pirate) and internal (insensitive employee) and therefore risking its reputation.

4.2 Office Suites

Microsoft aims, by launching its own cloud solution devoted for office: Office 365, to monopoly online office suite market. Neverthless, it faces established rivals in the form of Google Apps and Zoho Docs. All three platforms provide office basics such as word processing, spreadsheet, and presentation tools. All three also have an email client, online file storage, real-time sharing and collaboration, and some measure of cross-platform availability. As capable as these three offerings are, though, none of them can truly match the features and flexibility of a locally installed desktop office suite such as Microsoft Office 2010, but Office 365 still has the same look and feel overall, and the core features are present. Zoho has a comfortable to use layout as well. The various Zoho apps look and behave a lot like the pre-Ribbon Microsoft Office, particularly Office 2003. By comparison, Google Apps' menu bars and features seem austere. People who prefer the old-school text-based menu bar may appreciate the Google Apps interface, but Google Apps is more limited in what it allows you to do, both in formatting and in functionality.

The Office 365 apps offer a more diverse selection of fonts and formatting styles than either Google Apps or Zoho does.

When it comes to spreadsheets, unfortunately, none of the three online packages really deliver the power and flexibility that spreadsheet gurus need. The Web-based tools are sufficient for basic purposes, but lack many advanced features. Office 365 beats the other two in macros and formulas.

Office 365 provides some real-time collaboration capabilities in Excel and OneNote, but not in Word and PowerPoint. Google and Zoho each provide better collaboration from within the apps themselves. Both allow real-time editing with multiple users simultaneously.

5. SECURITY

In the last few years, cloud computing has grown from being a promising business concept to one of the wildest rising sections of the IT industry. Now, downturn crisis hit companies which are increasingly apprehending that simply by tapping into the cloud they can benefit from immediate access to best business applications and hugely enhance their infrastructure resources, all at insignificant fee. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how secure an environment it is.

Trust [9] in a cloud surroundings is profoundly governed by chosen deployment model, as

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

governance of data and software is subcontracted and delegated out of the proprietor's authoritarian management. In ancient architectures, trust was implemented by a proficient security strategy, which lectured restrictions on roles and stream among them, constraints on access by outside systems and rivals comprising programs and access to the records by general public. In a cloud organization, this insight is entirely disguised. Within the situation of public or open clouds, management is delegated to the institute holding the infrastructure. Once set out on a public cloud, management is alleviated to the infrastructure owner to apply an adequate security policy which guarantees that appropriate security actions are being achieved to make sure that danger is reduced. This announces a diversity of risks and perils, as fundamentally security is concomitant with trusting the procedures and computing base applied by the cloud possessor. It is vital to distinguish between deployment models, as an individual cloud, wherever the infrastructure is operated and managed on premise by a non-public organization, doesn't introduce extra distinctive security tasks, as trust leftovers inside the institute. In such a scenario the infrastructures owner remains the information and process owner.

The security purposes within the cloud system are principally:

- To preserve the integrity of data transferred between or kept within participating systems, for example preventing the loss or alteration of data due to illegal entree, component breakdown or other errors;
- To guarantee the availability of data transferred between or detained within partaking systems;
- To maintain the integrity of the services provided, i.e. confidentiality and correct operation;
- To deliver control over access to facilities or their components to make sure that users may only use services for which they are approved;
- To verify the identity of interconnecting partners and where necessary to guarantee non-repudiation of information source and distribution; and where suitable, to offer secure collaboration with the closed systems all around the world.
- To certify the confidentiality of data kept on involved systems.
- Distinct division of information and processes on the virtual level of the cloud, certifying no info outflow between different soft wares.
- To uphold an identical level of security when adding or eliminating resources on the physical level.

5.1 Availability

Cloud computing is web based. It allows naturally an available solution. It should serve all the users and provide them with their data at any time. This is possible through two strategies: hardening and redundancy [10]. They are mostly used to improve the availability of the Cloud applications. Almost all cloud computing system vendors offer Cloud infrastructures and platforms based on virtual machines. For example, Amazon Web Services provide EC2, S3 entirely based on the virtual machine called Xen. Obviously, virtual machines have the aptitude in providing on demand services to the final users. In certain way, users can use them as ready systems and can upgrade at any time they want to. Virtualization then enhances availability of the provided infrastructure.

5.2 Confidentiality

Confidentiality states that only approved parties or systems have the right to reach protected data. The risk of data being altered growths in the cloud, due to the amplified number of parties, devices, gadgets and tools implicated, that conducts to an upsurge in the number of points of access. Entrusting information control to the cloud, contrariwise leads to an escalation in the danger of data compromise, as the information becomes available to a bigger number of organizations. An amount of worries arise concerning the matters of multitenancy, data remanence, application privacy and security.

Multitenancy [11] mentions the cloud feature of resource sharing. Numerous sides of the information system are pooled counting, memory, softwares, networks and data. Cloud computing is established on a business model in which resources are shared at the network level, host level, and application level. Although users are isolated at a virtual level, hardware is not detached. With a multitenant architecture, a program is aimed to virtually separate its data and configuration so that each client society performs with an adapted virtual program instance. Multitenancy, is relative to multitasking in operating systems. In computing, multitasking is a method by which multiple tasks, also known as processes, share mutual resources such as a CPU. Multitenancy, as multitasking, expounds some privacy and confidentiality fears.

Journal of Theoretical and Applied Information Technology
31st January 2014. Vol. 59 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Data reusability is a chief quality of cloud infrastructures, but recyclable objects must be judiciously monitored in case they engender a grim exposure. Data confidentiality could be penetrated accidentally, due to data remanence. Data remanence is the lasting of data that have been supposedly deleted. Due to virtual departure of logical drives and absence of hardware disjointing between numerous operators on a distinct infrastructure, data remanence may cause unwilling revelation of secretive information. But also nastily, an employer may request a bigger volume of disk space and then rummage for confidential data.

Data confidentiality in the cloud is connected to user authentication. Caring of a user's account from robbery is an illustration of a greater problematic of governing access to objects, including memory, gadgets, software etc. Authentication is the process of confirming trust in user identities, electronically attended in front of an information system. Deficiency of robust authentication can direct to illegal access to users account on a cloud, causing a hole in privacy.

Privacy is the wish of an individual to govern the expose of its personal data. Establishments dealing with private data are expected to follow a country's legal outlines that guarantees proper discretion and confidentiality safety [12]. The cloud exhibits a quantity of legitimate encounters concerning privacy subjects engaged in data stockpiled in several sites in the cloud, furthermore rising the peril of confidentiality and privacy gaps. Instead of its information being stored on the company's servers, data is kept on the provider's servers, which could be in Europe, Asia, or anywhere in the world. This doctrine of cloud computing clashes with a range of legal necessities, such as the European laws that entail that an institute should be always aware of its personal data locations.

5.3 Integrity

Integrity is a main feature of Security. It indicates that resources can be amended merely by accredited sides or in legal ways and references data, software and hardware protecting them from unsanctioned fabrication, alteration or obliteration.

In addition, such methods present the better distinguishability into revealing who or what may have modified data or system information, hypothetically altering their veracity. Authorization is the tool (i.e. IDS) by which a system defines what level of rights a specific authenticated user should have to secure its data hold by the system [13]. Due to the growing number of individuals and access points in a cloud environment, authorization is critical in guaranteeing that only authorized persons can access their data. A suitable firewall security policy shall also guarantee that intruders must struggle to access sensitive data [14].

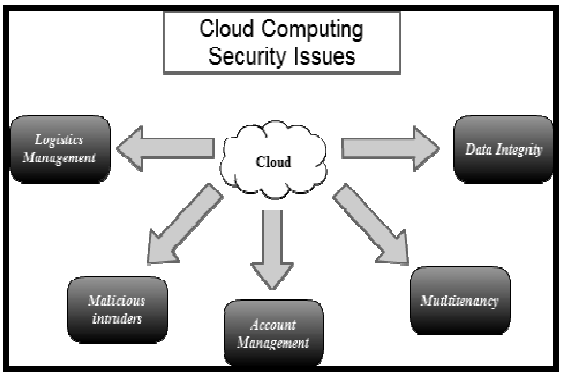

Figure 4: Cloud Computing Security Issues

6. BILLING

The price of the cloud services in the market depends on several factors, among them are:

- The computation time, usually an hour.
- The amount of storage.
- The number of transactions representing the number of access to storage.
- The input and output bandwidth: charge for inbound and outbound data transferred. Local network traffic is free.
- Instances of database servers.

7. CONCLUSON

Cloud Applications for business are still in their first stages. However, lot of experts has projected that the future is going to be Cloud computing solutions for large as well as small companies. The Cloud presents nevertheless some obnoxious aspects referring to ethic's view such as packaged products with no external control. Cloud clients need remote access control capabilities, which can give them more jurisdictions over their data, regardless of the cloud provider's physical locations. Also, automatic tools with remote-tracking capabilities could let cloud consumers monitor the employees activity.

The progression of cloud computing is theatrically shifting the prospect of information technology and finally turns the utility computing into a reality. Nonetheless, cloud computing offers an enormous range of benefits, but many challenges in this domain, including confidentiality, integrity, resource self-monitoring, energy management are

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

still waiting to be explored by the research community.

In our paper, we have presented an overview of cloud computing, its types and some of its major facets. We also believe that research topics discussed in this article such as multitenancy can be explored and remedied in future publications. Until then, cloud environment will remain gloomy. Our research questions will focus on application and data security over the cloud, we intend to build a multi-tenant security architecture targeting different levels of security of data with a typical cloud design. This model is meant to be more dynamic and based on distributed IDS.

REFRENCES:

[1] B.P. Rimal, A. Jukan, D. Katsaros & Y. Goeleven, "Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach", *Journal of Grid Computing*, Vol. 9, No. 1, 2011, pp. 3-26.

[2] B. Narasimhan & R. Nichols, "State of cloud applications and platforms: The cloud adopters' view", *Computer*, Vol. 44, No. 3, 2011, pp. 24-28.

[3] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg & I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", *Future Generation Computer Systems*, Vol. 25, No. 6, 2009, pp. 599-616.

[4] V. Prakash, & S. Gopalakrishanan, "Cloud computing solution - Benefits and testing challenges", *Journal of Theoretical and Applied Information Technology*, Vol. 39, No. 2, 2012, pp. 114-118.

[5] I. Foster,Y. Zhao,I. Raicu & S. Lu, "Cloud Computing and Grid Computing 360-degree compared", *Grid Computing Environments Workshop,GCE'08*, 2008, pp. 1-10.

[6] L. Wang, G. Von Laszewski, A. Younge, X. He, M. Kunze, J. Tao & C. Fu, "Cloud computing: A perspective study", *New Generation Computing*, Vol. 28, No. 2, 2010, pp. 137-146.

[7] Q. Zhang, L. Cheng & R. Boutaba, "Cloud computing: State-of-the-art and research challenges", *Journal of Internet Services and Applications*, Vol. 1, No. 1, 2010, pp. 7-18.

[8] H. Kamal Idrissi, A. Kartit, M. El Marraki, "A taxonomy and survey of Cloud computing," *Security Days (JNS3)*, April 26-27, 2013, pp. 1-5.

[9] M.K. KHAN, & Q. MALLUHI, "Establishing trust in cloud computing". *IT professional*, Vol. 12, No 5, 2010, pp. 20-27.

[10] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey", *in Proceedings of the 6 International Conference on Semantics*, Knowledge and Grids, 2010, pp. 105-112

[11] T. DILLON, C. WU & E. CHANG, "Cloud computing: Issues and challenges", *Advanced Information Networking and Applications (AINA)* Ieee, 2010. pp. 27-33.

[12] L.M. KAUFMAN, "Data security in the world of cloud computing". *Security & Privacy, IEEE*, Vol. 7, No 4, 2009, pp. 61-64.

[13] A. Kartit, A. Saidi,F. Bezzazi, M. El Marraki & A. Radi, "A new approach to intrusion detection system", *Journal of Theoretical and Applied Information Technology*, Vol. 36, No. 2, 2012, pp. 284-289.

[14] A. Kartit, M. El Marraki, A. Radi & B. Regragui, B, "On the security of firewall policy deployment", *Journal of Theoretical and Applied Information Technology*, Vol. 22, No. 2, 2010, pp. 84-92.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Comparative Study on Cloud Computing Storage Solutions

	Drive	**Dropbox**	**HubiC**	**ICloud**	**SkyDrive**
Company	Google	Dropbox	OVH	Apple	Microsoft
Free Storage	5 GB	2 GB	25 GB	5 GB	7 GB
Pricing plans	25GB: $2.49 per month; 100GB: $4.99 per month; 1TB: $49.99 per month. 16TB for $799.99 per month	50GB: $9.99 per month / $99 per year; 100GB: $199 per year / $19.99 per month; 1TB and up: starts at $795 for five users	100GB: $9.99 per year	25GB: $32 per year; 55GB: $80 per year;	20GB: $10 per year; 50GB: $25 per year; 100GB: $50 per year
Maximum File size	10GB	Unlimited	10GB	250MB	2GB
Encryption on servers	No	Yes	No	Yes	Yes
Sharing	Yes	Yes	Yes	No	Yes