Cloud Computing and Implication of Data Security

Aparicio Carranza, PhD[1], Hossein Rahemi, PhD[2], Harrison Carranza, MSIS[1] and Mdzafar Sadak, BT[1]
[1]New York City College of Technology - CUNY, USA
ACarranza@citytech.cuny.edu, HCarranza@citytech.cuny.edu, Mdzafar.Sadak@mail.citytech.cuny.edu
[2]Vaughn College of Aeronautics, USA
hossein.rahemi@vaughn.edu

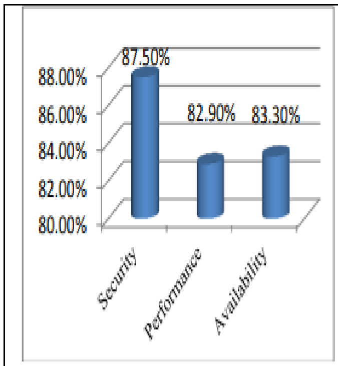
Abstract*– Cloud Computing is one of the most important advancements in technology since the invention of the Personal Computers. Cloud Computing refers to manipulating, configuring and accessing the applications via the Internet and provides various kinds of services to its users. One of the principal concerns of Cloud Computing is security "How secure is a cloud computing environment?" - Security is then one of the parameters that need to be tackled deeper before enterprises embrace this popular technology to a greater degree. With the cloud technology paradigm enterprise data are stored at a remote location and must be assured that is safe and be available at any time. Our effort is to report security feature results of our evaluation carried out on Public, Private, Community and Hybrid Cloud Computing; which includes differences between their services, architecture, deployment and development of services and the way to mitigate those security risks and issues.

Keywords—Data, Cloud Computing, Paradigm, Risks, Security

I. Introduction

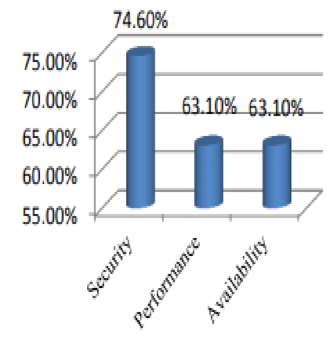
Cloud computing is a model for enabling ubiquitous convenient, on-demand network access to a shared pool of configurable computing resources(*networks, servers, storage, applications and services*) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. This cloud models promotes availability and are composed of five essential characteristics, three service models, and four deployment models [2]. Furthermore, Cloud security is also a broad term and it is a major concern. The security challenges Cloud computing presents are formidable, including those faced by Public Cloud whose infrastructure and computational resources are owned and operated by an outside party that delivers services to the general public via a multi-tenant platform, and by the Private Cloud which is hosted on institutions own premises and scales "only" into the hundreds or perhaps thousands of nodes, connected primarily using organization's private network links. Security concerns such as secure data transfer, secure software interfaces, secure stored data, user access control and data separation must be considered before moving to the Cloud [3].

International Data Corporation (IDC) conducted a survey of 244 IT executives/CIOs and their line of business colleagues about their companies' use of and views about IT cloud services. They have asked to rate the challenges/issues endorsed to the cloud/on-demand model. By comparing these two surveys, we observe from Fig. 1 and Fig. 2, that security challenges seem to be the top. From their survey we understand that the cloud providers should take much more care for security of data stored in the cloud [4].



Source: IDC enterprise portal, 2011

Fig.1 Rate of challenges/issues with the cloud



Source: IDC enterprise portal, 2010

Fig.2 Rate of challenges/issues with the cloud

Data requiring security includes corporate financial data, personally identifiable information (PII), and medical records. According to their survey,

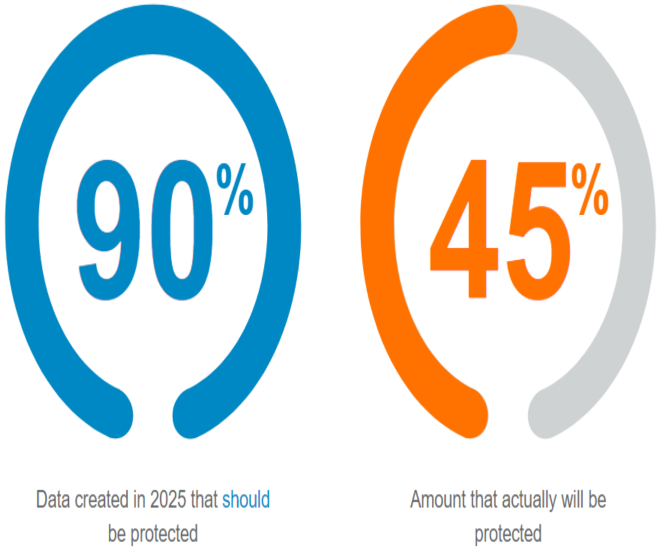


Fig. 3 Data Protection in future.

In another survey conducted by *rightscale.com* found that enterprises are migrating to Multi-Cloud platform. However, there was a slight increase in the number of enterprises that are using multiple public clouds or multiple private clouds [15].

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2019.1.1.375
ISBN: 978-0-9993443-6-1 ISSN: 2414-6390

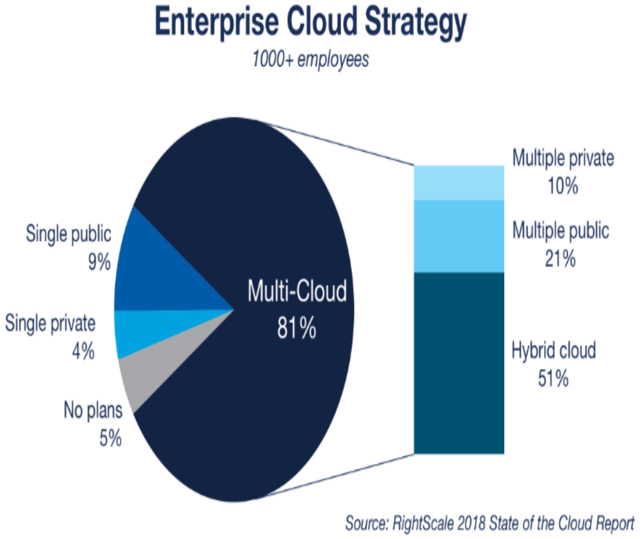


Fig. 4 Enterprise Cloud Strategy

The rest of the paper is organized as follows: Section I provided the motivation and background for the work. Section II, III and IV present Significance of Study, Cloud Deployment Models and Cloud Delivery Models respectively. Characteristics of Cloud Computing, Cloud Security Issues and Solutions, Cloud Service Provider (CSP) Level Attacks, and Experiments and Results are presented in Sections V, VI, VII and VIII. Finally our Conclusion is presented in Section IX.

II. SIGNIFICANCE OF STUDY

Today, we can easily notice how the nature of the Internet is changing from a place that we used to read web pages to an environment that allows the users to run software applications. One vision of the 21st century computing is that users will access the Internet services over lightweight portable devices rather than through some descendant of traditional desktop. Therefore, more and more enterprises are adopting the cloud model for their businesses, whether they are small or large organizations, as cloud computing provides low cost business solutions to their organizations. Cloud computing has promised tremendous advantages to organizations in terms of cost effectiveness, operational excellence and innovation. However, the main factor which enterprises are shifting to cloud is the low cost. Cloud helps to turn substantial investments into operational expenses, reduce management costs, operational costs and maintenance costs. Start-ups and small and mid businesses (SMB) prefer cloud computing solutions as they have limited investments and resources. Our effort in this paper is to cover the concerns of enterprises in adopting public, private, community and hybrid clouds for their respective organizations and list the differences among them in term of security issues.

Digital Object Identifier: (to be inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).

III. CLOUD DEPLOYMENT MODELS

The (NIST) National Institute of Standards and Technology identifies four distinct deployment models: public, private, community and hybrid clouds.

a) Public Cloud: The public cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services (CSP) [5]. In public cloud, resources are offered as a service, usually over the Internet connection, for a pay-per-usage fee. Users can scale their usage on demand, and do not need to purchase hardware to use the services. Public cloud providers manage the infrastructure and pool resources into the capacity required by its users [6]. Google, Amazon Web Services (AWS), Salesforce.com and Microsoft Azure are examples of public cloud vendors who offer their services to the general public [7]. Data created and submitted by consumers are usually stored on servers of third party vendor [8].

The advantages of public cloud include:

- ❖ *Data availability and continues uptime*
- ❖ *24/7 technical service*
- ❖ *On demand scalability*
- ❖ *Easy and inexpensive setup*
- ❖ *No wasted resources*

Drawbacks:

- ❖ *Data security*
- ❖ *Privacy*

b) Private Cloud: A private cloud is one that provides services to a single entity [2]. It may be managed by the organization or a third party or may exist on premise or off premise [5]. The cloud infrastructure is accessed only by the members of the organization or granted by third parties. The purpose is not to offer cloud services to the general public, but to use it within the organization, for example and enterprise that wants to make consumer data available to their different locations [8]. A private cloud provides better security than public clouds do, and cost saving in case it utilizes the resources.

The advantages of private cloud include:

- ❖ *Dedicated hardware means increased security*
- ❖ *The transition from physical to virtual servers lead to better flexibility*
- ❖ *Fully utilizes hardware with better resource management*

Disadvantages:

- ❖ *Higher cost compare to public cloud*
- ❖ *Security risks still exist*
- ❖ *Resource utilization is expensive*

c) Community cloud: The cloud is managed by several organizations and supports a specific community that has the same interest. It is somewhat similar to a private cloud, but the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security and regulatory considerations [9].

Advantages:

- *Share cost of cloud services*
- *Lower cost*

Disadvantages:

- *Not the right choice for every organization*
- *Slow adoption to date*
- *Fixed amount of bandwidth and data storage*

d) Hybrid Cloud: Hybrid cloud infrastructure is composed of two or more clouds (*public, private or community*) [9]. A hybrid cloud is a composition of at least one private cloud and at least one public cloud. It has composed infrastructure of two or more clouds that are unique entities, but at the same time bound together by standardized or proprietary technology that enables data and application portability [10].

Advantages of Hybrid cloud include:

- *Reduce capital expenses*
- *Offers controls and supports*
- *Improves resources allocation*
- *Cloud bursting happens to fully utilize resources*

Disadvantages:

- *High cost and maintenance*
- *Security issues*
- *Privacy and data integrity concerns*
- *Compatibility*

IV. CLOUD DELIVERY MODELS

Above we have discussed deployment models of cloud computing. Now we will introduce three fundamental service models: Infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

a) Infrastructure as a Service (IaaS): In this model, Cloud computing providers offer physical and virtual computers, extra storage networking devices etc. The virtual machines are run by hypervisors that is organized into pools and controlled by operational support systems. It is the cloud users responsibilities to install Operating System images on the virtual machines as well as their application software. Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE) are some popular examples of Iaas [11]. This model is shown in Fig. 5.

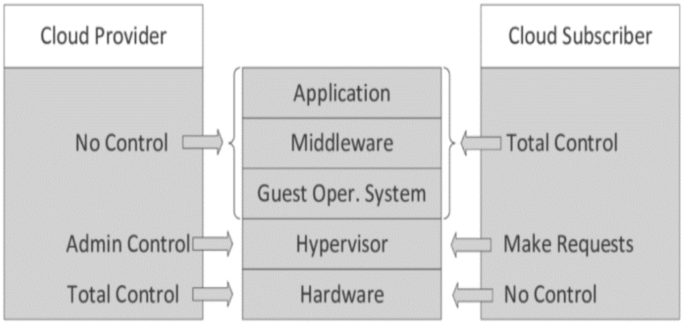


Fig.5 IaaS Control Responsibilities.

b) Platfrom as a Service (PaaS): Platform as a Service refers to computing platform such as web servers, databases, operating systems and programming environments, where the cloud user uses software or platforms offered by Cloud Service Providers (CSP). Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Google App Engine, Apache Stratos [11]. This model is shown in Fig. 6.

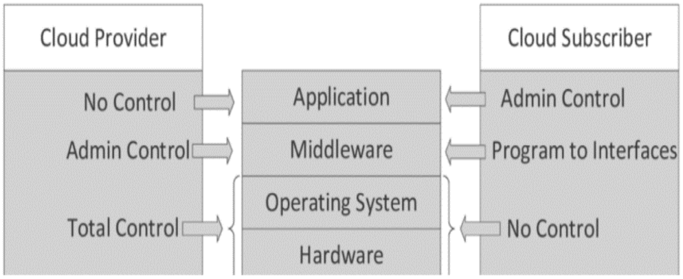


Fig.6 PaaS Control Responsibilities

c) Software as a Service (SaaS): In Software as a Service environment cloud users can use software that is already installed and running on the cloud infrastructure. This solution eliminates the need of installing and running the software on local computers. Additionally, the need for software maintenance and support is eliminated. Some examples of (IaaS) are Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, and Google Compute Engine (GCE) [9]. This model is shown in Fig. 7.

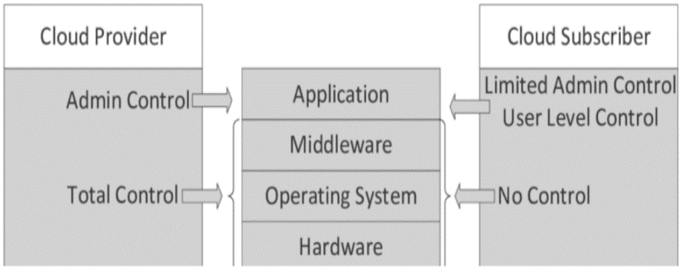


Fig.7 SaaS Control Responsibilities

V. CHARACTERISTICS OF CLOUD COMPUTING

According to the NIST organization, cloud computing contains the following five essential characteristics [5]:

a) On-Demand Self-Service: Provision computer services such as email, network, application and computer capabilities. It also provision server service without human interaction from each service provider.

b) Broad Network Access: Computing capabilities are available over the network and can be accessed through standard mechanisms that promote the use of heterogeneous thin or thick client platform.

c) Resource Pooling: The computing resources of the providers are pooled to support multiple consumers using a multi-tenant model with different virtual and physical resources dynamically assigned and reassigned according to consumer demand. The consumer has no idea or knowledge over the exact location of the resources but can access and use data at any time from any location.

d) Rapid Elasticity: Computing capabilities can be rapidly and elastically provisioned. The resource pooling and self-service makes it possible. The provider can automatically distribute more or less resources from the available pool.

e) Measured Service: Cloud systems, in this case, automatically control and manage resource used by leveraging a metering capability at some level of abstraction as it is seen appropriate to the type of service.

VI. CLOUD SECURITY ISSUES AND SOLUTIONS

This section discusses the specific security issues and existing solutions to secure cloud computing environments.

The top seven security threats to cloud computing and analyzed by the Cloud Security Alliance (CSA) are described below [12]:

a) ***Abuse and Nefarious Use of Cloud Computing:*** Abuse and nefarious use of cloud computing is one of the major threats identified by the CSA. An example of that is the usage of botnets to spread spam and malware. Attackers can access a public cloud, for instance, and discover a way to upload malware to thousands of computers and use the power of the cloud infrastructure to assault other machines. Suggested remedies by the CSA:

- *Stricter initial registration and validation procedures*
- *Enhanced credit score card fraud tracking and coordination.*
- *Comprehensive introspection of customer network traffic.*
- *Monitoring public blacklists for one's own network blocks.*

b) ***Insecure Application Programming Interfaces:*** As software interfaces or APIs are what customers use to have interaction with cloud services, those must have extraordinarily secure authentication, access control, encryption and activity monitoring mechanisms - specifically when third parties begin to construct on them. Suggested remedies by CSA:

- *Analyze the safety version of cloud provider interfaces.*
- *Ensure best authentication and access controls are carried out in concert with encrypted transmission.*
- *Recognize the dependency chain associated with the API.*

c) ***Malicious Insiders:*** The malicious insider danger is one that is important as many providers do not reveal how they hire people, how they provide them access to assets or how they monitor them. Suggested remedies by CSA:

- *Enforce strict supply chain management and operate a comprehensive supplier evaluation.*
- *Specify human resource necessities as a part of legal contracts.*
- *Require transparency into entire information security and management practices, as well as compliance reporting.*
- *Identify security breach notification techniques.*

d) ***Shared Technology Vulnerabilities:*** IaaS providers usually share infrastructure. Unfortunately, the components on which this infrastructure is primarily based were not designed for that. To ensure that consumers do not thread on different territories, monitoring and robust compartmentalization is required. Suggested remedies by CSA:

- *Implement security best practices for installation / configuration.*
- *Observe surroundings for unauthorized adjustments / activity.*
- *Promote robust authentication access control for administrative access and operations.*
- *Enforce service level contracts for patching and vulnerability remediation.*
- *Conduct vulnerability scanning and configuration audits.*

e) ***Data Loss/Leakage:*** Without a backup or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top threats for companies as they may lose their reputation. Suggested remedies by CSA:

- *Implement robust API access control.*
- *Encrypt and protect integrity of data in transit.*

- *Analyze data protection at each layout and run time.*
- *Implement strong key generation, management and storage, and destruction practices.*
- *Contractually call for providers to wipe persistent media earlier than it is released into the pool.*
- *Contractually specify provider backup and retention techniques.*

f) ***Account, Service & Traffic Hijacking:*** Account, service and traffic hijacking is another trouble that cloud users should be aware of. These threats vary from man-in-the-middle attacks, to phishing and spam campaigns, to denial-of-service attacks. Suggested remedies by CSA:

- *Prohibit the sharing of account credentials among customers and services.*
- *Leverage robust two-factor authentication strategies where possible.*
- *Employ proactive monitoring to identify unauthorized activity.*
- *Understand cloud provider safety policies and service level agreements.*

g) ***Unknown Risk Profile:*** Security must continue being the top part of the concerned list. Code updates, vulnerability profiles, security practices, intrusion tries - all things must continually be kept in mind. Suggested remedies by CSA:

- *Disclosure of applicable logs and data.*
- *Partial/full disclosure of infrastructure details (eg. Patch, levels, firewalls)*
- *Monitoring and alerting on necessary information.*

VII. CLOUD SERVICE PROVIDER (CSP) LEVEL ATTACKS

The shared nature of the cloud and increased demand of cloud resources could be an attractive target to attackers. End users should take into consideration the vulnerabilities of cloud computing before migrating to it. Examples of shared resources are computing capacity, storage and network which exposes the cloud to many security breaches that are listed below:

a) Guest-hopping attack: In this type of attack, an attacker will try to get access to one virtual machine by penetrating another virtual machine hosted in the same hardware. One of the possible mitigations of guest hopping attack is the Forensics and VM debugging tools to observe the security of cloud. Another possible Mitigation is called High Assurance Platform (HAP) [13].

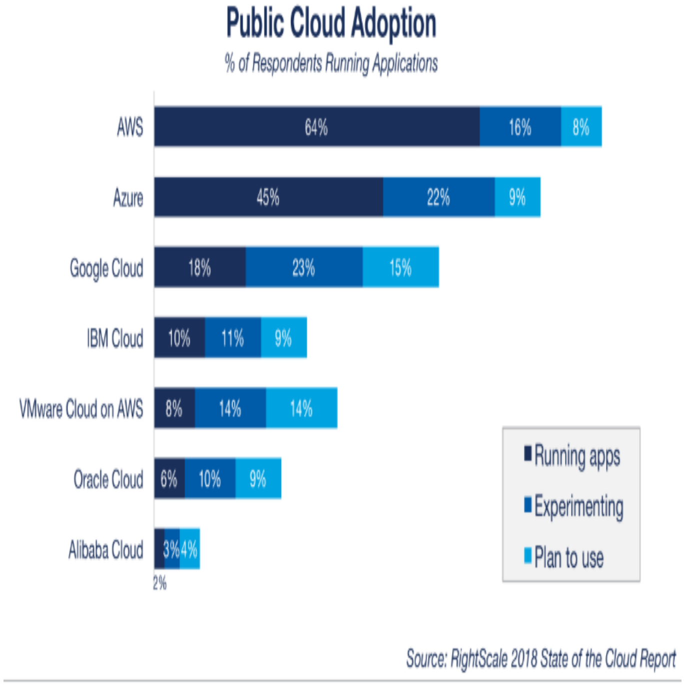
b) SQL Injection: SQL injection is often used to attack websites. The procedure is by injecting SQL commands into a database of a certain application from the web to crash that database system. To mitigate SQL injection attacks: assign the least possible privileges to users who have permissions to access the database [14].

c) Malicious insider: One of the cloud computing challenges of the service providers is when its employee is granted access to sensitive data of all customers' administrators. Such system privileges can expose this information to security threats. Strict security planning, security auditing can minimize this security threat [12].

As we have found tremendous amount of vulnerability and security issues on the cloud, therefore we will Experiment security and performance issues using Microsoft Azure Public Cloud architecture.

VIII. EXPERIMENTS AND RESULTS

Azure Continues to Grow Quickly and Reduce the AWS Lead, Especially Among Enterprises (as seen in Fig. 8). In 2018, AWS continued to lead in public cloud adoption, but other public clouds are growing more quickly. Azure especially is now nipping at the heels of AWS, especially in larger companies [15].



Source: RightScale 2018 State of the Cloud Report

Fig. 8 Public Cloud Adoption

However, if we discuss their services based on geographical locations they have more than 100 data centers all around the world (as shown in Fig. 9). Additionally they operate a large amount of virtual cloud features, benefits and services to the end users [16].

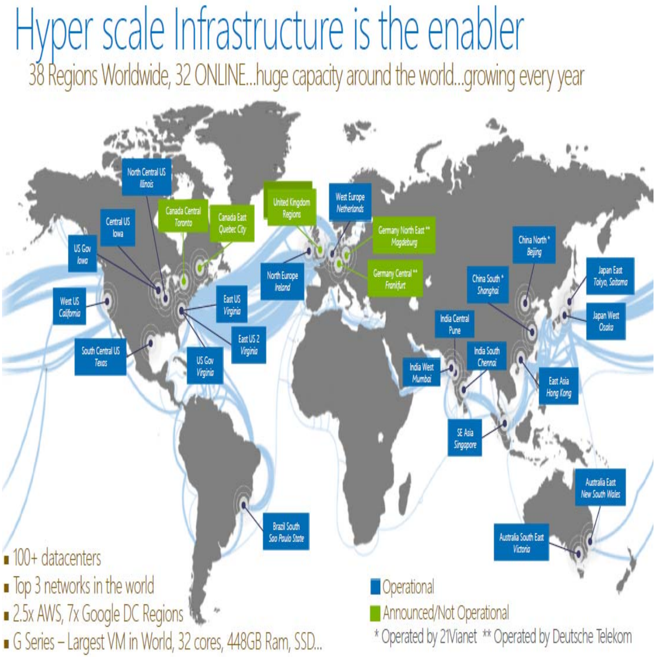
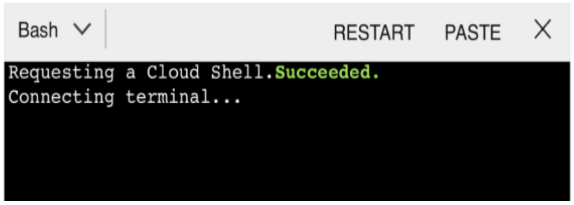

Hyper scale Infrastructure is the enabler
38 Regions Worldwide, 32 ONLINE...huge capacity around the world...growing every year
North Central US Illinois
Central US Iowa
US Gov Iowa
West US California
South Central US Texas
Canada Central Toronto
Canada East Quebec City
East US Virginia
East US 2 Virginia
US Gov Virginia
United Kingdom Regions
West Europe Netherlands
North Europe Ireland
Germany North East ** Magdeburg
Germany Central ** Frankfurt
China North * Beijing
China South * Shanghai
Japan East Tokyo, Saitama
Japan West Osaka
India Central Pune
India South Chennai
India West Mumbai
East Asia Hong Kong
SE Asia Singapore
Australia East New South Wales
Australia South East Victoria
Brazil South Sao Paulo State
100+ datacenters
Top 3 networks in the world
2.5x AWS, 7x Google DC Regions
G Series – Largest VM in World, 32 cores, 448GB Ram, SSD...
Operational
Announced/Not Operational
* Operated by 21Vianet ** Operated by Deutsche Telekom

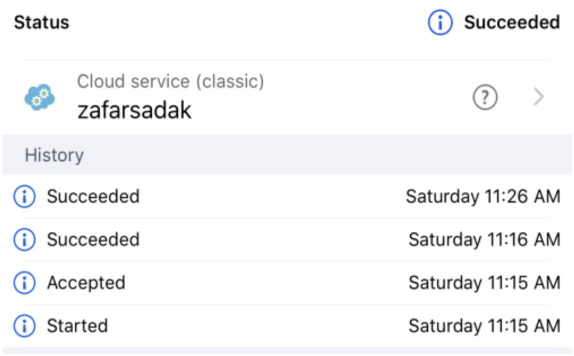
Fig. 9 Microsoft Azure Networks Worldwide.

Below is a simple interface of cloud computing in Microsoft Azure that has been part of our experimentation exercises. To experiment cloud performance and security level We have used Microsoft Azure cloud student account (https://portal.azure.com/). This is shown in Fig. 10 and Fig. 11.



```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...
```

Fig. 10 Confirmed successfully connected to the cloud terminal.



Status — Succeeded

Cloud service (classic)
zafarsadak

History

Succeeded	Saturday 11:26 AM
Succeeded	Saturday 11:16 AM
Accepted	Saturday 11:15 AM
Started	Saturday 11:15 AM

Fig. 11 Data successfully sent to the cloud.

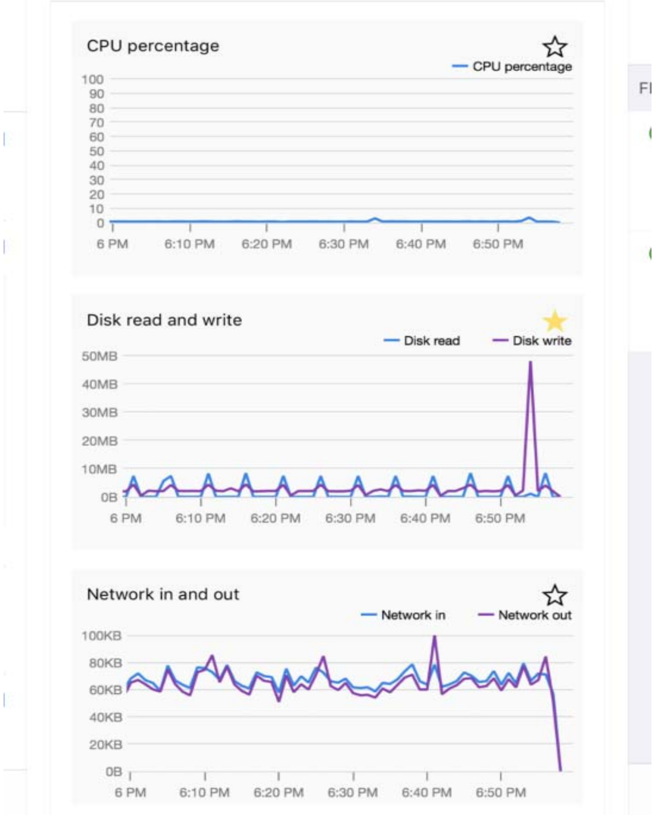


Fig. 12 CPU, Read, Write and Network usage while transferring data.

Microsoft Azure provides the necessary cloud platform to reduce not only the time to discovery, but also the cost of discovery – Fig. 12 shows these features. Anyone can try Microsoft Azure by themselves and discover firsthand that is easy to set up and go live.

IX. CONCLUSION

The Cloud computing model has the ability to scale up services and virtual resources on demand. No big investments are required to update the infrastructure - it is a cost saving solution. In fact cost is almost zero when resources are not in used (*pay per use*). In this paper we have provided a basic definition of cloud computing, its architecture and characteristics and discussed the security issues/concerns related to cloud technology infrastructure. Different kinds of delivery models and how they provide services are also shown. The four cloud deployment models have their own merits and challenges. Therefore, security will always be an issue. Mitigation of risks and issues are the important and were described the possible ways to reduce risks such as: to implement proper access control, monitoring, auditing and some standard data security mechanism. Further research needs to done on these topics to optimize performance and minimize security issues in the cloud for future technology advancements.

REFERENCES

[1] Brown, Evelyn A. “Final Version of NIST Cloud Computing Definition Published.” NIST, 8 Jan. 2018, www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published.

[2] RUPARELIA, NAYAN B. *Cloud Computing*. MIT Press, 2016. *JSTOR*, www.jstor.org/stable/j.ctt1c2cqk4.

[3] “Cyber Security Research - Cameron University.” *CU Fast Facts - Cameron University*, www.cameron.edu/cybersecurity/research.

[4] Beckham, J. (2011) *The Top 5 Security Risks of Cloud Computing.* Retrieved February17, 2012 from http://blogs.cisco.com/smallbusiness/the-top-5-security-risks-of-cloud-computing/

[5] P. Mell and T. Grance, “The NIST definition of cloud computing (draft),” NIST special publication,800(145),7,2011

[6] G. Lewis,”Basics about cloud computing”, Software Engineering Institute Carniege Mellon University, Pittsburgh,2010.

[7] T. Mather, S Kumaraswamy and S. Latif,”Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance,” Published by O’Reilly Media Inc, 1005 Gravenstein Highway North, Sebastopol,CA 95472,2009

[8] O. Hamren. (2012).M.S. Thesis .”Mobile phones and cloud computing”.

[9] W. Jansen and T. Grance,”Guidelines on security and privacy in public cloud computing”. NIST special publication 800-144,2011

[10] P. Mell and T. Grance,”Effectively and securely using the cloud computing paradigm,” NIST information technology lab, 2009

[11] Amir. “IaaS PaaS & SaaS Explained with Examples & Comparison.” *WebSpecia*, 9 Apr. 2018, blog.webspecia.com/cloud/iaas-paas-saas-explained-examples-comparison.

[12] Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009. DOI: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[13] Center of Protection of National Infrastructure Information Security Briefing Cloud Computing Briefing.pdf

[14] Rohit Bhaduria, Rituparnan Chaki, Nabendu Chaki,”A Servey on security issues in Cloud Computing” https://arxiv.org/abs/1109.5388

[15] *Cloud Computing Trends: 2018 State of the Cloud Survey*, www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2018-state-cloud-survey.

[16] “The Channel Company.” *The Channel Company*, www.thechannelco.com/.