Volume: 09 Issue: 02 Pages: 3382-3386 (2017) ISSN: 0975-0290

A Survey of Cloud Computing Approaches, Business Opportunities, Risk Analysis and Solving Approaches

Mohamed H. Farrag
Canadian International College, Cairo, Egypt
Email: Mohamed_farrag@cic-cairo.com
Mona M. Nasr
Faculty of Computers and Information, Helwan University, Cairo, Egypt.
Email: m.nasr@helwan.edu.eg

ABSTRACT

In recent years, cloud computing become mainstream technology in IT industry offering new trends to software, platform and infrastructure as a service over internet on a global scale by centralizing storage, memory and bandwidth. This new technology raises some new opportunities in producing different business operations which influence some new business benefits also some different risks issues are involved using cloud computing. This paper attempts to identify cloud computing approaches, highlights its business opportunities and help cloud computing user to analysis the cloud computing risks and to produce different solving approaches. This paper is targeted towards business and IT leaders considering a move to the cloud for some or all of their business applications.

Keywords -**Cloud computing, Cloud services, Data security, Deployment model, Risk analysis.**

Date of Submission: Sep 10, 2017 Date of Acceptance: Sep 28, 2017

I. INTRODUCTION

Managing IT risks remains a significant challenge for most companies, yet most companies are ever more reliant on IT. A typical company will have a vast number of activities, policies, and processes that help manage and mitigate digital risks. Cloud computing is not just another technology evolution to which this lifecycle must react. Rather, it brings a fundamental shift in how IT services are procured and provided. This new technology has different approaches, business opportunities and raise different risks with different solving approach. This paper give a survey of cloud computing approaches, business opportunities, risk analysis and solving approach. This Paper is organized as follows: section two demonstrates the cloud computing background, section three discusses business benefits of using cloud services. Section four highlights Cloud Computing risk analysis. While solving approachesin the fifth section, finally conclusion and future work are in the last section.

II. BACKGROUND

Cloud computing has different definitions from different perspectives; first it can be defined as "An internet-based model of computing, where the shared information, software and resources are provided to computers and other devices upon demand"[1].Also is defined as "is location agnostic and provides dynamically scalable and virtualized resources as services over the Internet" [2]. It uses virtualization, service-oriented software, and grid-computing technologies allow accessing resources and services offered by servers from different places. Also defines as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3].

2.1. Essential Characteristics Of Cloud Computing

Cloud computing model is composed of five essential characteristics [9]; **First character is "on demand capabilities" -** in which a business will secure cloud-hosting services through a cloud host provider which could be your usual software vendor. Users canhave access to your services and you have the power to change cloud services through an online control panel by adding or deleting users and change storage networks and software as needed.

Second character is "Broad network access"-cloud computing gives power to the user to usetheir smartphones, tablets, laptops, and office computers wherever they are located with a simple online access point. It also includes private clouds that operate within a company's firewall, public clouds, or a hybrid deployment.

Third character is "Resource pooling"-it gives users ability to enter and use data within the business management software hosted in the cloud at the same time, from any location at any time for multiple business offices and field service.

Fourth character is "Rapid elasticity"-cloud computing is flexible and scalable to suit your immediate business needs. User can quickly and easily add or remove users, software features, and other resources.

Volume: 09 Issue: 02 Pages: 3382-3386 (2017) ISSN: 0975-0290

Fifth character is "Measured service"-cloud computing provider can measure storage levels, processing, bandwidth, and the number of user accounts. The resources can be monitored and controlled from both your side and your cloud provider's side.

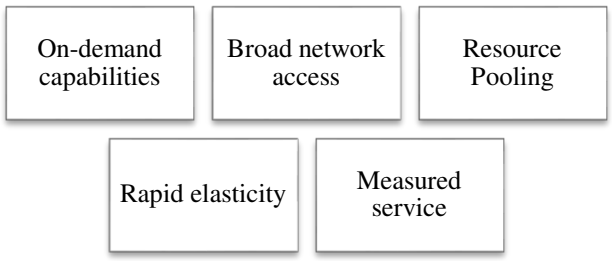

Figure 1. Cloud Computing essential characteristics

2.2. Cloud Computing Service Models

Cloud computing has three service levels provided by **Cloud service provider (CSP)** – "A third-party vendor that provides application delivery, hosting, monitoring, and other services through cloud computing" [9]. The current major cloud service providers are Microsoft, Hewlett Packard, IBM, Salesforce, Amazon and Google.

First isSoftware as a Service (SaaS): "Applications organizations use to perform specific functions or processes (e.g., email, customer management systems, enterprise resource planning systems, and spreadsheets)[9].

Second is Platform as a Service (PaaS) "Development environments for building and deployingapplications"[9]. These environments provide its customers with proprietary tools that facilitate the creation of application systems and programs that operate on the CSP's hosted infrastructure.

The third is Infrastructure as a Service (IaaS) "entire virtual data center of resources" [9] for example storage resources,network and computing resources.

2.3. Deployment Models

Cloud computing has different four deployments model first is **Private cloud**- it provisioned for single organization, it may exist on or off site and may be managed by organization or outsourced. Second deployment model is **Community cloud** - It provisioned for exclusive use by a specific community it also may be managed by one or more of the community organization and may be managed by community organization or outsourced. Third deployment model is **Public cloud** - It provisioned for general public, it exists on the premise of the cloud provider and may be owned, managed & operated by a business, academic or government organization or a combination. while the fourth model is **Hybrid cloud** It is a combination of two or more distinct cloud infrastructures and combines characteristics of private, public & community clouds [3].

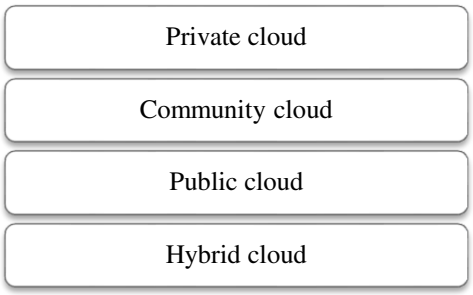

Figure 2. Cloud computing deployment models

III. BUSINESS BENEFITS OF USING CLOUD SERVICES

Cloud Services Support Business Process and it contributes business by different benefits, cloud computing aids for:

3.1. Cost Savings

Pay for only the computing resources they use rather than purchasing or leasing equipment that may not be fully utilized at all times [9]. Cloud computing gives full support to the equipment, personnel needs, infrastructure, space & utilities also reduced obsolescence and reduction of capital expenditures, reduced implementation costs [3]. It also reduced setup costs can be considered as a major advantage for cloud computing.

3.2. Speed Of Deployment

Can meet the need for computing resources much more quickly than most internal information technology functions [9]. By support rapid deployment and Time to fulfill request.

3.3. Scalability And Better Alignment Of Technology

Cloud computing services give the user power to Scale up and down its capacity. Also Ability to add or reduce capacity and support On-demand provisioning.

3.4. Decreased effort in managing technology

Decrease effort by reduced management effort, maintenance & support, it also simplified entry into or exiting from and business initiatives increased access to technical expertise

3.5. Environmental benefits

Environmental benefits like Less overall power consumption, Carbon emissions, physical land use, Disaster recovery and Business expansion (across town or across the globe). Cloud computing services also make the Backup recovery process is very easy in Infrastructure as a Service (IaaS) Providers.

IV. CLOUD COMPUTING RISK ANALYSIS

Cloud computing has different five sources of risk representing by Users, Enterprise, Network Provider, Cloud Provider and Environment.

Three factors are needed to determine if the risk is high or low, first one is the likelihood of an event, second factor is

Volume: 09 Issue: 02 Pages: 3382-3386 (2017) ISSN: 0975-0290

the size of impact if that event happens. While the third factor is the ease by which such an event can be mitigated [8].

In this sections we discuss the different risks for cloud computing.

4.1. Security Risks

The state of preventing a system from vulnerable attacks is considered as the system's security"[1]. Security risks apply for four categories covering physical access to infrastructure, systems & data, Physical location of systems, data, Logical access to the network, OS, applications & databases and network & data segregation Seven important arguments identity factors for risk in a cloud computing model (3)

4.1.1. Access control

"Organization allows only the authenticated users to access the data"[1]. The possibility of risk is more in case of sensitive data."

4.1.2. Availability

"Needs of the customers should be attended on time" [1] availability represented in some main arguments as cloud provider service interruptions, Data location/availability for restoration, network/connectivity interruptions, failure of the provider to adhere to SLAs and Service provider disaster recovery [3]

4.1.3. Network Load

"The computers and the servers crash due to high volume motion of data between the disks" [1], cloud network load can also prove to be detrimental to performance of the cloud computing system. Flexibility and scalability should be considered pivotal when designing and implementing a cloud infrastructure. The durability and the efficiency of the system, implementation of the application programming interface (API).

4.1.4. Integrity

In a cloud computing model data validity, quality and security affect's the system's operations and desired outcomes. The program efficiency and performance are addressed by the integrity of adherence to change management, procedures, incident management, and failure of the provider to adhere to SLAs, timeliness, accuracy, authorization and completeness [3].

4.1.5. Data Security

Data has "to be appropriately secured from the outside world" [3], Trust is an important factor which is missing in the present models as the service providers use diversified mechanisms.

4.1.6. Data Location

Service providers are not concentrated in a single location but are distributed throughout the globe. This could hinder investigations within the cloud and is difficult to access the activity of the cloud, where the data is not stored in a particular data center but in a distributed format. [1]

4.1.7. Data Segregation

Data segregation is represented in many ways first the available data is not correctly sent to the customer at all times of need. Second when recovering the data there could be instances of replication of data in multiple sites. Third the restoration of data must be quick and complete to avoid further risks.

The data can be manipulated, deleted or destroyed as a result of the **attack**. Such attacks can have serious implications to the end users. To prevent these attacks we need the **Encrypting** to ensure that the data is not hacked or attacked. Different types of attacks samples as comingling of data & other assets and unauthorized access to sensitive or trade secret information [3]

4.2. Privacy Risks

Privacy determines if the whether the data is disclosed to authorize recipients only. Another privacy issue in the domestic cloud structure is related to the rights possessed by the data owners to access their data.Two distinct cloud structures first structure is **domestic clouds** and **trans-border clouds**.In a domestic cloud structure, the complete cloud is physically located within the
The above privacy issues can also be extended to all other cloud computing environments in general [1]. As International laws affecting service provider location, regulatory compliance/legal liability and breach & incident management [3].

4.3. Consumer Risks

"The use of cloud computing services can cause risks to consumers" [1], when the provider makes changes to the terms on which the product is provided and the consumers remain unaware about it. These types of risks may be avoided by universal Terms of Service, Additional Terms, Program Policies, Privacy Policy and Copy Right Notices.

Volume: 09 Issue: 02 Pages: 3382-3386 (2017) ISSN: 0975-0290

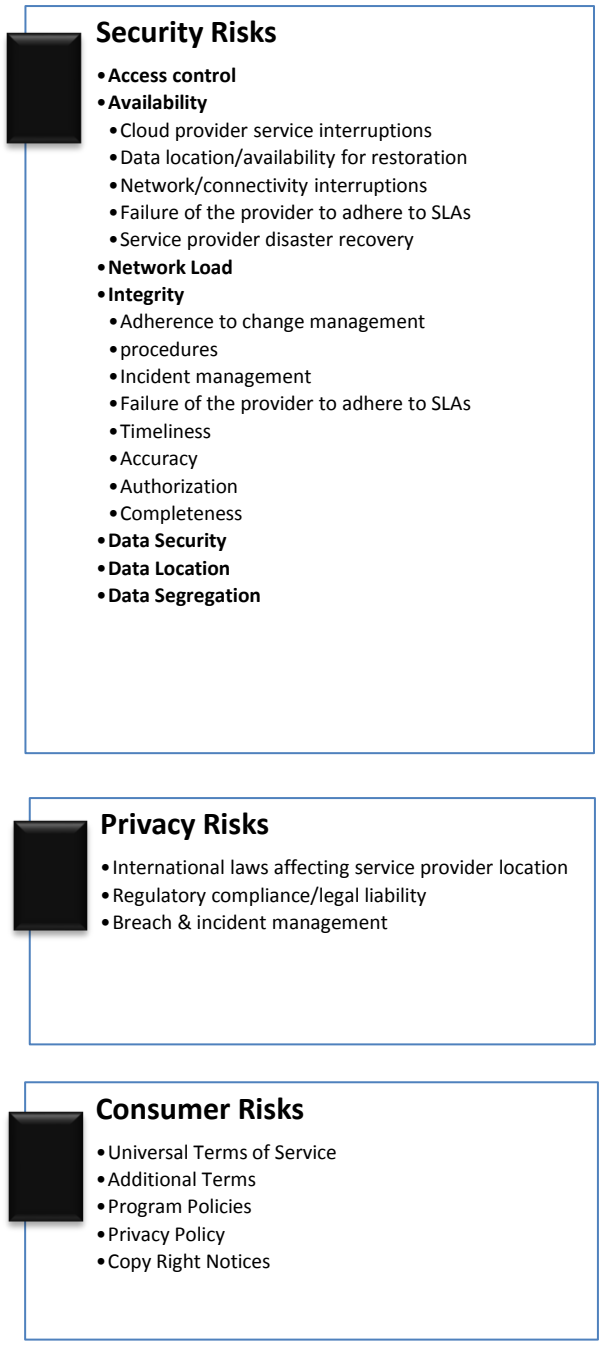

Figure3.Cloud Computing Risk analysis

V. SOLVING APPROACHES

Some important arguments play an important role for eliminating different cloud computing risks first is **Risk Response** Once risks have been identified and assessed in the context of organizational objectives relative to cloud computing, management needs to determine its risk response. There are four types of risk responses:
Avoidancenot moving to the cloud or considering only private cloud types of solutions as viable options, **Reduction**Implementing control activities and taking actions to reduce risk likelihood, risk impact, or both, **Sharing**Reducing risk likelihood or risk impact by transferring or otherwise sharing a portion of the risk and **Acceptance**Taking no action to affect risk likelihood or impact. For example, when an organization does not have direct ability to manage the controls of its CSP, the organization is accepting an increased level of inherent risk [9].

Users need to ensure that all the security risks are eliminated by having various security mechanisms in place to estimate data security risk before placing data in the cloud and assure customers that their data is safe with the service various providers within the cloud network

Some good mechanisms help to increase and identify the risk response, first are **Data-flow analysis to**understand the information life cycle by develop data-flow schematics and develop policies to periodically review & update data-flow documentation [3].

Second is **Managing risks associated with unique cloud computing components**can be reached by Maintain application & technology layer inventory when develop inventory in conjunction with the data-flow analysisanddevelop controls to address risks associated with each layer of the cloud “stack” [3].

Third is Audit & compliance is an understanding cloud risks & regulatory implications by Leverage existing risk assessment tools & control frameworks, Assessing control maturity and vendor management [3].
When considering risk mitigation strategies, the options are to **avoid** - prevent it from happening, **Reduce** - actively plan and manage to limit occurrence and severity or to **outsource** - hand over to other parties such as the provider. Also to **accept** - because the cost of mitigation outweighs the risk itself or simply because you cannot control it [8].
Many proper risks analysis approaches for cloud computing helping to identify and eliminate the different risks as:

5.1. Secure Socket Layer (SSL)

The Secure Sockets Layer (SSL) is "a commonly-used protocol for managing the security of a message transmission on the Internet". SSL is a secure protocol developed for sending information securely over the Internet. Many websites use SSL for secure areas of their sites, such as user account pages and online checkout. Usually, when you are asked to "log in" on a website, the resulting page is secured by SSL.

5.2. Digital signatures

"Electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged". Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender

Volume: 09 Issue: 02 Pages: 3382-3386 (2017) ISSN: 0975-0290

cannot easily repudiate it later. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real. Signatures are commonly used to authenticate documents. When you sign a physical document, you are authenticating its contents. Similarly, digital signatures are used to authenticate the contents of electronic documents. They can be used with PDF, e-mail messages, and word processing documents.

5.3. Authentication Protocols

The protocol by which an entity on a network proves its identity to a remote entity. Typically, identity is proved with the use of a secret key, such as a password, or with a stronger key, such as the key on a smart card. Some authentication protocols also implement mechanisms to share keys between client and server to provide message integrity or privacy.

VI. TRUST MATRIX

Trust matrix use three variables, **'Data cost'** is considered as one of the variables because the users can assign a cost to the data based on the data's criticality. **'Provider's History'** is considered as another parameter since it includes the record of the past services provided by the provider to the customers. The variable parameter **'Data Location'** is used to provide details about the data located in sensitive sites [1].

- X axis represents the data cost.
- Y axis represents the service provider's history.
- Z axis represents the data location.

The trust matrix helps to show areas of Low Risk/High Trust Zone and High Risk/ Low Trust Zone [1].
In all ways you need to continue monitor the effectiveness of its ERM program to verify that the program adequately addresses the relevant risks and facilitates achieving the organization's objectives.

VII. CONCLUSION AND FUTURE WORK

This study highlights different cloud computing approaches, and its business benefits and a list of security risks and some solving approaches for these risks. The development of cloud computing may lead to significant changes in the way companies consume IT, moving from managing large technology stacks to purchasing business-level services. Companies will lose control of the way in which their services are run, needing instead to choose between the terms and conditions offered by different service providers. That make as important need to have a better understanding of risk and how it is mitigated. Being aware of the risks and other issues related to cloud computing, executives are more likely to achieve their organization's objectives.

Future work is to give more researches for cloud computing risk analysis to develop a cloud management frameworkwill be based on different business-driven policies that help organization to identify and eliminate the risk cloud computing factors to improve its reliability and to aid different organization to achieve its goals.

REFERENCES

[1] Chandran S. and Angepat M., "Cloud Computing: Analyzing the risks involved in cloud computing environments," in Proceedings of Natural Sciences and Engineering, Sweden, pp. 2-4, 2010.

[2] Morin, J. H., Gateau, B.: Towards Cloud Computing SLA Risk Management: Issues and Challenges. In 45th Hawaii International Conference on System Sciences, 2012

[3] Seth, F., Matt, L., Rod, W., "Risk Management & Cloud Security Setting & Enforcing Policy", BKD, LLP, accounting today.

[4] Turner, S. "Benefits and risks of cloud computing.",Journal of Technology Research, 2012

[5] Baldwin, A., Pym, D., & Shiu, S. Enterprise information risk management: Dealing with cloud computing. In Privacy and Security for Cloud Computing (pp. 257-291). Springer London.(2013).

[6] Stokes, D. (2013). Compliant Cloud Computing–Managing the Risks. PHARMACEUTICAL ENGINEERING.

[7] Fitó, J. O., & Guitart Fernández, J. (2012). Introducing risk management into cloud computing.

[8] Schotman, R., Shahim, A. & Mitwalli, AH,"Cloud Risks - Are we looking in the right direction?", (May 2013).

[9] C. Horwath. "Enterprise Risk Management for Cloud Computing," COSO, 2012, June.

[10] Catteddu, D. Cloud Computing: benefits, risks and recommendations for information security (pp. 17-17). Springer Berlin Heidelberg. (2010).

[11] Chou, Y., & Oetting, J. (2011). Risk assessment for cloud-based IT systems. International Journal of Grid and High Performance Computing (IJGHPC), 3(2), 1-13.