Second National Conference on Internet of Things : Solution for Societal Needs
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Information Security Risk Management Framework for the Cloud Computing Environment

Dr. Arvind S. Kapse[1], Madhavi Basant[2]
[1]Professor, ISE Department, New Horizon College of Engineering, Bengaluru, Karnataka, India
[2]M. Tech. Scholar, Cyber Forensics and Information Security, ISE Department, New Horizon College of Engineering, Bengaluru, Karnataka, India

ABSTRACT

Cloud services provide organizations the opportunity for on-demand network access to a shared pool of configurable cloud environment. The security risks associated with cloud environment model are dependent on factors such as sensitivity of information assets, cloud architectures, storage cost and security controls involved in cloud services. Risk management framework is one of security assessment tool to reduce the threats and vulnerabilities of cloud computing environment. Based on risk management framework a prototype was developed using machine learning to automatically analyse the risks involved in cloud environment. [3] When used appropriately with the necessary precaution and control in place, cloud computing could yield a multitude of benefits, some unheard of until now and some yet to be discovered.

Keywords: Cloud computing, Risk assessment, Security, Data Privacy

I. INTRODUCTION

Cloud computing industry continues to grow at a fast-pace and have become one of the top technology trends. Companies can get advantage of the lower costs, efficiency and high scalability of cloud computing services. There is no upfront cost for installing and managing the software and hardware infrastructure for cloud environment [1]. Cloud computing also has brought many risks to organizations because they outsource IT resources, which results in providing access to third party. Therefore, such organizations might lose control over security of the data resource in the their cloud environment

Before moving to a cloud-computing environment, companies need to understand the business and legal risks, which is associated with cloud services, and have some effective planning in place to resolve those risks. [1] They lack experience incorporating cloud services from both a contracting and a technology domain. Companies need to review the risks of cloud environment and mitigate it. Organizations might mitigate cloud-computing risks through negotiation of contract clauses and service level agreements (SLA) and enforcement of the same [2]. The SLA should be the mutually agreed between the cloud service provider and the organization. If organizations already have agreements with cloud service provider

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

then they should apply security protocols in future cloud-contract negotiation.

Cloud computing environment is a major source of new vulnerabilities in therefore, it is important to establish several protocols, which will mitigate the risks, provide security and increase trust and confidence in cloud services. Risk management is one of the cloud services security mechanisms, which provides access and manage risks related to cloud computing environment and to prevent those risks from affecting organization's business goals [2].

1.1 Types of Risk in the Cloud

Policy and Organizational Risks — The risk of vendor lock-in through the use of proprietary interfaces, organizations face issues such as complying with various regulations, even though applications and data resource have been migrated from a traditional data center to a cloud service environment.

Cloud Service Failure — Cloud vendor also must deal with the risk of a cloud service failure and be prepared to mitigate these risks (eg: disaster recovery and business continuity planning). There is another type of risk to consider is, the loss of business reputation of an enterprises. For example, a cloud security breach could result in damage to the reputation of enterprises using that cloud services.

Technical Risks — Enterprises that uses cloud services also face technical risks such as resource exhaustion, which can occur when not managing cloud services resources effectively. Resource exhaustion can cause degradation of services and, in some cases, a failure to provide services at all in the cloud environment.

Interception of Data — The interception of "data in transit" to or from a cloud environment. This can be resolved by ensuring that all data transmissions are encrypted and that the endpoints for any data transmission are authenticated to ensure that they are legitimate.

Distributed Denial-of-Service Attacks —The cloud vendor and their Internet service providers are typically responsible for dealing with DDoS attacks. Organizations should discuss DDoS with cloud vendors to ensure that the proper controls are in place to resolve a DDoS attack. [8]

Legal Risks — Enterprises should maintain compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) or the Payment Card Industry Data Security Standard (PCI DSS). Many enterprise find it difficult or even impossible to achieve compliance while using cloud environment. Cloud vendor should thoroughly research any applicable regulations before planning a cloud service migration.

Changes in Jurisdiction — Enterprises may face varying requirements if cloud vendors are located in different geographic locations, each of which has its own set of law.

Data Privacy —Cloud vendor state in their contracts that they have the right to monitor customer data in the cloud environment and harvest data from it, then sell this data to third parties.

II. LITERATURE SURVEY

The literature review of this paper begins with the status of cloud contracting in Canada and the US government, followed by a review of the rewards and risks of cloud computing. It identifies risk management strategies through negotiation of key contract terms and SLAs [7]. The main goal of the research was to identify major contract terms needed

to mitigate risks as organizations move to a cloud-computing environment.

The risk management framework provides key terms to organizations, a checklist of cloud services clauses to add in the contract in order to protect their interests from a business and legal contracting point of view. This paper also includes key points important for negotiation of cloud services contracts, which included governance and Software as a Service strategy, project management and vendor performance management. [4]

2.1 Service model of cloud computing:

Software as a Service (SaaS) – Cloud services delivers an application, which is already customized with all of the required hardware, software, operating system, and network to be accessible by various consumers by using the internet services without the need to install software on the servers.

Platform as a Service (PaaS) – Cloud services offers an environment and all the requirements such as software tools, libraries, software programming languages, and services for cloud consumers to develop or install their own software applications and tools). The applications are then delivered to the users via the Internet services.

Infrastructure as a Service (IaaS) – Cloud services offers fundamental computing resources such as processing, servers, data storage, and networks for cloud customers to install and run their own operating systems and applications. Cloud computing services can be deployed in four ways dependent on consumers' requirements such as public cloud, private cloud, community cloud and hybrid cloud.[4]

2.2 Cloud services deployment models

Public Cloud – Cloud environment are made available to public customers over a public network. Multiple enterprises can work and access the provided infrastructure and resource at the same time. The public cloud model is managed and owned by a third party: a cloud vendor.

Private Cloud – Cloud services are dedicated only to a specific consumers (enterprises) and offer the security and control over client data resource. A private cloud may be controlled and owned by the organization itself or a cloud vendor

Community Cloud – Cloud infrastructure is equipped for a group of consumers (enterprises) which have the same shared requirements. They can share resources by using the connections between the associated enterprises. The community cloud can be controlled and owned either by the relevant community enterprise or a cloud vendor.

Hybrid Cloud – A hybrid cloud is a mixture of two or more types of cloud deployment models such as public, private, or community. They are connected together to allow for the transfer of data resource and application between them but without affecting each other services and structure.[4]

Risks can be reduced during various stages from selection of the cloud vendor, pre signing of the contract and post signing of the contract. Below are the mentioned stages for risk management mitigation :
Due Diligence Stage (cloud vendor selection)

Business, Legal and Regulatory Risk Mitigation Stage (negotiation of contract)

Vendor Performance Management(on boarding, during and post contract terms, review of SLA metrics, audits).

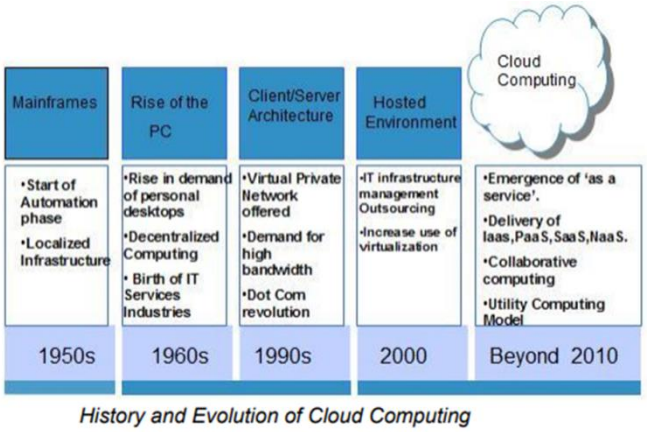

Figure 1: History and evolution of Cloud Computing

III. PROPOSED METHODOLOGY

Many organizations have switched to cloud computing environment, but often this adoption has not involved full-fledged risk management methodologies. Instead, they trust cloud providers to take care of security. Security is an important consideration for those looking to access cloud technologies. Cloud Vendor must also be concerned about privacy, availability and reliability, disaster recovery, business continuity, scalability, compatibility and standardization.[3]

Risk management of cloud computing is a mechanism for managing the risks or threats facing by an organization that may result in damaging the resources and to provide best course of action for identifying and resolving risk issues. Some of the objectives of cloud computing risk management are increasing system security, protecting and enhancing the organization's assets, optimizing operational efficiency and making well-informed decisions

The key points for organizations to mitigate the risks associated with contracting with cloud services is mentioned below:

1. Organizations should perform due diligence to reduce the risks at the pre-contract level
2. Cloud services contract and SLA metrics should be incorporated into cloud vendor contracts to mitigate risk in cloud environment.
3. Cloud service providers are becoming more willing to accept some of the risks and are starting to work with organizations to negotiate mutually acceptable contract terms.

3.1 Effective Risk Mitigation Steps [5]

STEP 1: Examine the business context- This refers to assessing the types of services and data resource handled (eg: customer records, credit card numbers, and prescriptions). Cloud vendors face numerous negative scenarios when analyzing these threats for each service and data resource.

STEP 2: Review application security - Assessing the security of applications is a critical step in risk management. It is important to determine what features an application offers to mitigate risk. Cloud vendor also should consider how robust these features are. Suppose if an application encrypts the data at rest to protect its confidentiality, what encryption algorithm and key length are used, and how strong are the algorithm and key combination.

STEP 3: Construct a data-centric governance plan – Data governance involves the management of data resource throughout an enterprise, such as making backups and archiving old data resource. A survey which was conducted in 2013, shows that nearly half of all enterprises didn't have a data governance policy. This can increase the chances that data resource will be misplaced or compromise. It is important for organizations who are using cloud services to know where their data resource is stored and to restrict the access. The virtual machines on which the data resource resides should be authorized to restricted individuals only.

STEP 4: Test and retest. After a data-centric governance plan has been implemented, cloud vendor should periodically test data resource. This includes actions such as verifying the integrity of backup data resource, ensuring that archived data resource is stored securely and making sure that unnecessary data resource is destroyed properly. Authorized users must be able to find data on demand, such as that needed to respond to e-discovery requests. Testing should be performed periodically on data resource to ensure that these controls works as intended.[6]

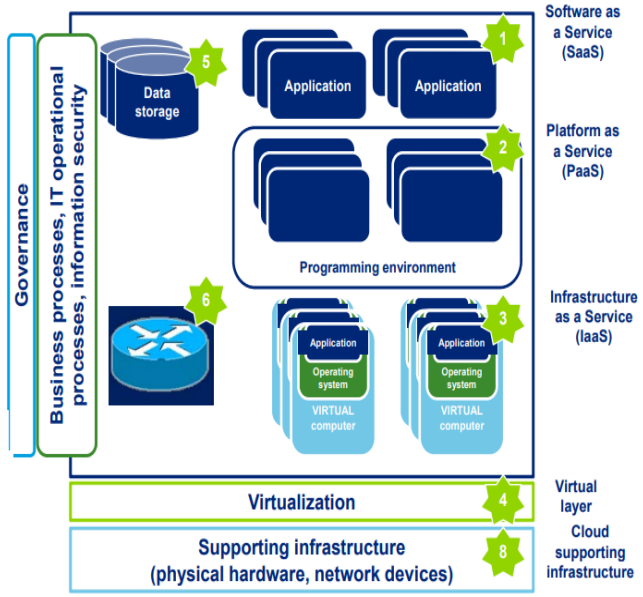

Figure 2: Cloud Computing Framework

IV. CONCLUSION

Risk management framework can be decided based on its effectiveness on a cloud environment. Applying cloud computing risk management model without the proper care, due diligence and control, is bound to cause major unseen problems in future. By being aware of the risk and other issues related to cloud computing environment, organizations are more likely to achieve their objective as they manage the risks in their dynamic and cost effective environment that likely will become the most secure computing model of the future. Cloud computing is relatively new in its current form, given that, it is best applied to specific low to medium risk business areas.

V. REFERENCES

[1]. Kathy English, "Cloud Computing: Risk Mitigation Strategies from a Contracting Perspective" April 2015

[2]. Vinit Kumar, "Information Management in Cloud Environment: Risks and Mitigation Strategies" February 2018

[3]. Erdal Cayirci, Alexandr Garaga,"A risk assessment model for selecting cloud service providers" September 2016

[4]. Mariana Carroll, "Secure cloud computing: Benefits, risks and controls" September 2011

[5]. Chiang Ku Fan,"The Risk Management Strategy of Applying Cloud Computing" 2012

[6]. Rana Alosaimi,"Risk Management Framework for Cloud Computing : A Critical Review", August 2016

[7]. Jordi Guitart, "Introducing Risk Management into Cloud Computing", August 2016

[8]. Usha Kiran Marichetty, "The Use of Effective Risk Management in Cloud Computing Projects", October 2017