International Journal of Computer Applications Technology and Research
Volume 11–Issue 06, 213-222, 2022, ISSN:-2319–8656
DOI:10.7753/IJCATR1106.1006

Multi-Criteria Parameter Factor in the Assessment of Public Cloud Services Providers' Associated Risks

Omojokun Gabriel Aju
Department of Computer Science
Adekunle Ajasin University
Akungba-Akoko, Nigeria

Abstract: The cloud computing technology is indisputably assisting individuals, businesses and institutions in increasing their capability, productivity and efficiency. It has eliminated the border restriction of obtaining specialized computing resources and expertise that are not available locally to the organizations and individuals without the need to invest in new infrastructure. However, in spite of the immeasurable benefits the technology promises, it has also raised major challenges, particularly as regards its information security and service availability, stressing the need for an elaborate technique of assessing the associated risk of selecting a particular public cloud services provider among available alternatives using the right risk criteria. This paper proposes an expanded multi-criteria risk parameters for the evaluation of public cloud service providers' associated risk to produce a more accurate results that meets the dynamic nature of the cloud technology.

Keywords: Cloud Computing, Cloud Service Providers, Risk Criteria, Information Security, Service Availability.

1. INTRODUCTION

The fast pace at which the organizations and individuals are embracing cloud computing services as the new major milestone in computing technology is a reflection that indeed the technology is an inventions breakthrough, as the technology delivers hosted services over the Internet thereby enabling the organizations to increase their capabilities in meeting computing resources demands while avoiding significant investments in physical infrastructure, training, personnel and software licensing.

Various organizations including commercial industries, academic institutions, military and other government agencies are fast embracing the cloud technology because of its promised benefits of cost reduction, efficiency and resources flexibility that provides organizations with the ability to use specialized computing resources without investing in new infrastructure.

In spite of the undisputed benefits that cloud technology brings, concerns are also being expressed as regards the challenges of the technology, including the potential loss of control of the customers' assets (Information Security and Privacy) by the cloud services providers (Yunchuan et al., 2014; Michael et al., 2015; Domingo-Ferrer et al., 2019; Li et al., 2019; Irshad et al., 2021) and the inability of the providers to guarantee constant availability of the public cloud networks (Liliana et al., 2014; Velliangiri et al, 2020; Qureshi et al., 2020). The fact that public cloud services are shared, externally provided and offered over internet network where users are able to gain access to computing resources from anywhere also makes the services more vulnerable to all forms of attacks (Mohiuddin et al., 2019; Abdurachman et al., 2019; Qureshi et al., 2020; Deebak et al., 2020).

The real and perceived concerns of providing, accessing and controlling services in externally provided multi-tenant cloud environments also slow or preclude the migration of services by major prospective organizations to the public cloud (Nautiyal and Wadhwa, 2019; Dong et al., 2019; Xu et al., 2019). Like every other inventions of technologies, there are various risks that are associated with public cloud services environment arising from the data security and privacy, network availability and performance, systems interoperability, governance and compliance complexity, among others.

The risk assessment in public cloud environment is so challenging compare to the traditional computing environment due to the cloud unique characteristics of on-demand self-service, multi-tenancy and rapid elasticity, which makes the technology more complex and dynamic in nature. Providing a service that meets the needs of subscribers is as important as entrusting adequate level of confidence on the users to ensure that they are taking the right decision of embracing such service, and such certainties of decisions can only be affirmed if there is a way to evaluate the risk associated with such decision, as it is expected that before initiating any substantive contract negotiations or operational integration with a cloud service provider, the prospective consumer should evaluate the cloud provider's competency and commitment to deliver the desired services over the target timeframe while meeting the stipulated service availability and security levels.

Therefore, a more risk dimensional focus area and parameter criteria for the accurate assessment of associated risk of the service environment will go a long way in providing some degree of confidence to the cloud service consumers in assisting them to make right selection decision.

2. PUBLIC CLOUD CHALLENGES

The International Organization for Standardization in ISO 31000:2009 defines risk as the effect of uncertainty on objectives (ISO 31000, 2009). It is expressed as a combination of the consequences of an event and the associated probability of occurrence with the potential to influence the achievement of an organization's objectives (Berg, 2010). Objectives can have different aspects such as financial, political, reputation or environmental goals depending on the individuals or organizations and can apply at different levels like strategic, project, product or process. It is not therefore unexpected that every individual and organization strives to assess the level of risk associated with their choices at every point in time in order to be guided in their decision making.

According to Stoneburner et al (2002), risk assessment is a process of assessing identified risks in term of their potential severity of loss and possibility of occurrence within a given timeframe. It involves three processes, namely, risk identification, risk analysis and risk evaluation. However, Cloud risk assessment is defined as a dynamic, step by step, repeatable process used to produce an understanding of cloud risks associated with relinquishing control of data or management of services to an external service provider (Akinrolabu et al., 2019). Various research studies have identified different concerns as the major fears of the potential public cloud consumers in the process of adopting appropriate public cloud providers. Daniele & Giles (2009), the Cloud Security Alliance (CSA, 2010); Shukla (2014); Mazhar et al (2015); Odun-AYO (2018); Wu et al (2019); Karajeh et al (2020) and Irshad et al (2021) identified information security as the major fear of the cloud services consumers.

Charanya et al (2013); Mohammed et al (2013); Srivastava and Khan (2018); Deebak et al (2020) and Alghofaili et al (2021) considered data sovereignty as a major challenge in the public cloud environment, the researchers based their conclusion on the fact that most public cloud services providers or their data centres are mostly located outside the jurisdiction of the service consumers, or when such service providers or their data centres are located within the jurisdiction of the service consumers, they are mostly owned by third party agents. Sah et al (2014); Siddiqui (2019); Dong et al (2019); Abdurachman et al (2019); and Tabrizchi and Rafsanjani (2020) insisted that the multi-tenancy method of service delivery using resources pooling through the virtualization technology creates great security risks, as public cloud service providers deliver services to multiple customers (tenants) by sharing the same computing resources.

Eric et al (2012); Hashizume et al (2013); Kamal et al (2014); Yunchuan et al (2014); Michael et al (2015); Paul et al (2018); Kumar et al (2018); Verma and Sharma (2019); Wu et al (2019) and Alghofaili et al (2021) reported data security and privacy as the major obstacles hampering the widespread adoption of public cloud computing. The studies observed that most of the services (SaaS and PaaS) providers do not have access to the physical security system of data centres, they mostly rely on third party to achieve full data security and the fact that consumers are to handover their data to a third party is a major challenge.

Srivastava and Khan (2018); Verma and Sharma (2019); Dong et al (2019) reported network availability, performance unpredictability and system interoperability as the main challenges facing the organizations' decision of moving to the public cloud. Liliana et al (2014); Singh (2017) and Alghofaili et al (2021) presented lack of interoperability standards as a threat within the public cloud environment since there is neither standardized communication between and within public cloud providers nor standardized data export format. It is therefore difficult to migrate from one cloud service provider to another or bring back data and process it in-house, this makes it difficult to establish security frameworks for cloud heterogeneous environments.

There are few risk assessment frameworks and models which are designed for the public cloud consumers to assist them in their selection of public cloud services providers during the cloud adoption based on various criteria and risk focus using different methodologies, such as Chandran and Angepat (2010), QUIRC by Prasad and Ben (2010), SecAgreement by Matthew and Rose (2012) and Microsoft by Greg and Pierre (2016), among others. However, this study is exclusively concern with the suitability of the existing parametric criteria and the focus area of risk in the public clouds to derive accurate risk values for the purpose of decision making in the selection of the appropriate public cloud provider among many alternatives.

3. THE EXISTING RISK CRITERIA

The issue of designing risks assessment frameworks and models for cloud environment started in 2009 with the design and publication of Cloud Computing Information Assurance Framework by the European Union Agency for Network and Information Security (ENISA) (Daniele and Giles, 2009). The framework followed ISO/IEC 27005:2008 risk level estimation approach for the traditional information systems and categorized the public clouds security risks into four groups: policy and organization risks, technical risks, legal risks and the other scenarios not specific to cloud technology. The framework uses generic qualitative approach while focusing on the information security within the cloud environment.

Prasad and Ben (2010) presented a quantitative risk assessment framework (QUIRC) for public cloud security based on the Federal Information Processing Standards (FIPS) of the US Federal Information Security Management Act (FISMA) and adapted the Wide-band Delphi method of rankings which is based on experts opinion about the likelihood and consequence of threats to assess the security risks associated with public cloud services providers. However, the framework was a localized work as it was based on the US Federal Information Security Management Act (FISMA) for information processing within the public sector in the United States of America (USA) which makes it a public policy.

Chandran and Angepat (2010) proposed a public cloud risk assessment framework based on Trust Matrix Approach for security risk analysis to ensure that formal risk assessments are aligned with the enterprise-wide framework to facilitate transparency and increase trust level between the cloud customers and the cloud providers. The framework used two variables, namely "Data Cost" and "Providers' History" as risk criteria. In "data cost" users can assign a cost to data based on the data's criticality whereas "Provider's history" includes the record of the past services provided by the provider to consumers. The framework also focuses on the information security aspect of the public cloud technology.

Peiyu and Dong (2011) produced a cloud information security risk assessment model for public cloud services consumers based on theory of Analytic Hierarchy Process (AHP) by listing eight (8) kinds of threats to cloud security principles and their corresponding correlation coefficients to get the information security risk assessment of public cloud service provider. The model specifically focus on information security aspect of the public cloud using security as the only criteria and eight security threats that are peculiar to cloud technology as sub-criteria.

Feng et al (2012) presented a risk management framework for public cloud consumers on the basis of service providers' previous works focusing on the public cloud information security. The aim of the work was to assist the public cloud consumers to ascertain the risk associated with adopting a particular public cloud service provider by reviewing the service providers' previous services to their customers. The framework analyses the security status of cloud service providers by reviewing historical incidents associated with the service providers and introduces the involvement of third party assessment agency to ensure thorough analysis of the provider's capability. Matthew and Rose (2012) developed a cloud risk assessment model (SecAgreement) based on the Service Level Agreement (SLA) negotiation standard to allow security measures to be expressed on service description terms and service level agreement. The approach defines a cloud service matchmaking algorithm to assess and rank the SLA by their risk, allowing the consumers to quantify risk, identify any policy compliance gaps that might exist, and thus select the public cloud services providers that best meet their security needs.

Mouna et al (2015) proposed a multidimensional approach towards a quantitative assessment of information security risks in the public clouds model. The model illustrates how a quantitative risk assessment of public cloud service providers can be carried out based on a systematic, extendable and modular approach. The model views information security risks as segmentation of the public cloud world according to its dimensions, where a dimension can be defined as an elementary aspect of risk sphere. The model uses a new approach to threats classification using dimensional method and a quantitative assessment of the associated risks based on the number of identified dimensions allowing the model to be modular and extendable in nature, although, no specific risk criteria was stated for the assessment purpose.

Greg and Pierre (2016) designed a cloud risk decision framework that was based on the ISO 31000 standard (ISO 31000, 2009) to assist the cloud consumers to take appropriate risk decision before moving to the cloud by using the framework as a template in assessing the risks associated with a particular cloud providers. The framework based the cost of the data security breach in the public clouds to the prospective consumers into four groups of operational risk, market and finance risk, strategies risks and compliance risks and used qualitative assessment approach to evaluate the risk level based on these four risk types. Cayirci et al (2016) presented a public cloud adoption risk assessment model (CARAM) based on the three existing frameworks of ENISA, Cloud Security Alliance's Consensus Assessment Initiative Questionnaire (CAIQ) and the French National Commission on Informatics and Liberty (CNIL) developed in Europe for assisting public cloud services consumer to select a cloud services provider that fits their security risk profile best. The model essentially focuses on information security risk by adopting the ENISA's thirty-five (35) security risk elements and the Cloud Security Alliance's CAIQ eleven (11) security risk control areas.

Sivasubramanian et al (2017) produced a cloud risk assessment model for public cloud services consumers based on the probability of an incident occurring, which is mapped against the estimated negative impact. The model used the Information Assets and Risk, Privacy and Confidentiality Concerns, Data Governance for its risk assessment which is principally based of the Data Cost variable. The Expression of Needs and Identification of Security Objectives (EBIOS) method for evaluating and treating risks, that aims to determine the security actions to implement which focuses on six key categories of security objectives (SO) (i.e. Confidentiality, integrity, availability, multi- party trust, mutual audit ability and usability) and the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method of assessment of vulnerabilities and threats on the basis of the operating assets of a company were adopted in the assessment. The authors have followed the traditional route to security risk assessment, concentrating on the local organization, their critical assets (data), threats, and likelihood of impact, without paying attention to the supplier network nor fully understanding its interrelated consequences.

Akinrolabu et al (2019) presented a quantitative risk assessment model, termed Cyber Supply Chain Cloud Risk Assessment (CSCCRA) based on the systematic analysis of cloud risks, the visual representation of the cloud supply chain, and the assessment of the cyber security posture of cloud suppliers through the use of experts and evaluation of supply chain. The authors adopt the use of information of the parties involved in the development, hosting, management, monitoring and use of the cloud services (i.e. the supply chain).

The model takes a multi-disciplinary approach to assessing the dynamic, evolving and interconnected risks in the cloud, applying different knowledge areas in the identification, analysis, and evaluation of these risks. It combines factors such as security, supplier selection, systems thinking, decision support systems, quantitative risk modelling, and supply chain mapping in a multi-stage approach.

It is obvious that the existing frameworks and models cannot provide accurate risks level evaluation of the public cloud services providers to assist the prospective consumers in their selection decision making processes (Alghofaili et al (2021), this is because the existing models and frameworks focuses the assessment of associated risks of public cloud providers only on the information security aspect of the public cloud services and therefore limit their risk criteria on information security. The motivation for this study is therefore drawn from the limitations of the existing risk focus areas and parametric criteria for the purpose of evaluating the associated risks of specified public cloud providers for the purpose of selecting the best alternative among the various service providers.

4. PROPOSED RISK CRITERIA

It has been observed from the reviewed literatures that the existing models focus on the security of information in the cloud in their risk assessment process as a means of selecting the appropriate public cloud provider. However, the rapid expansion of public clouds services from the predominantly established data storage services facilities to many other services, such as real-time enterprise networking, educational mobility solutions, digital videos services, financial and industrial intensive processing solutions, national satellite monitoring services, offices on motion services, among other numerous services have made the services availability and performance a major area of concern (Yogeshwaran et al., 2017; Dong et al., 2019; Jouini and Rabai, 2019).

Unfortunately, none of the existing public cloud providers' risk assessment work in the reviewed literature has considered the public cloud services availability and performance as a major focus in the assessment of risks for the purpose of selecting appropriate public cloud service provider, resulting in the restriction of the criteria for the risk assessment to information security area. To address this deficiency in the risk focus areas and the selection of the risk criteria, this study is hereby proposing wider areas of risk focus and assessment criteria.

4.1 The Risk Area of Focus

4.1.1 Information Security

The existing public cloud service providers risk assessment models, such as Prasad and Ben (2010); Chandran and Angepat (2010); Peiyu and Dong (2011); Matthew and Rose (2012); Mouna et al (2015); Greg and Pierre (2016); Cayirci et al (2016); Sivasubramanian et al (2017) and Akinrolabu et al (2019) all focused on the information security as an area of risk within the public cloud environment as reflected in the choice of risk criteria used in the models. As cloud services are provided through the internet technology, it causes the cloud computing systems to inherits those security challenges that are peculiar to the internet technology resulting to number of vulnerabilities within the public cloud services environment as data is being indiscriminately shared among the varied systems which affects the validity, quality and security of the data in the public clouds (Rana and Mohammed, 2016; Qureshi et al., 2020 and Deebak et al., 2020). Therefore, taking the security of data (Assets) to be placed in the cloud as a factor in the process of assessing the associated risks of cloud service providers to examine the level of protection by the service provider(s) cannot be overemphasised.

4.1.2 Service Availability and Performance

Liliana et al (2014); Srivastava and Khan (2018); Verma and Sharma (2019); Dong et al (2019); Aldribi et al (2020) and Alghofaili et al (2021) presented cloud network availability, performance unpredictability and system interoperability as major challenges facing organizations' decision of moving to the cloud. The authors posited that the availability and performance of public cloud services are heavily dependent on the supporting technological infrastructure, and that the available bandwidth, reliability and resiliency of local and international network connections could have a significant impact on consumers' public cloud experience. Yogeshwaran et al (2017); Mohiuddin et al (2019); Nautiyal and Wadhwa (2019) and Velliangiri et al (2020) observed that the expansion of public cloud services beyond the data storage services to real-time enterprise networking, education mobility solutions, digital videos services, financial and industrial intensive processing solutions has introduced cloud service availability and performance as a serious risk concern to the consumers and a major factor in the adoption of public clouds.

A research from the University of California tracked the availability and outages of four major cloud providers in the United States of America and found out that overloads on the cloud systems caused programming errors resulting in system crashes and failures. Likewise, due to inefficient business continuity and backup recovery mechanism, public cloud services experience periods of unavailability ranging from minutes to days, resulting in loss of confidence among the customers which brought up fresh debates on the capability of the cloud technology in handling certain critical computing services. For example, In March 2018, Amazon Web Services (AWS) was hit by a cloud outage that silenced Amazon's Alexa and affected hundreds of enterprise services including Atlassian, Slack, and Twilio. The outage happened in the data centres in Virginia when the Direct Connect dedicated links from AWS North Virginia region to other server warehouses and premises on the East Coast got disabled and the outage lasted for about 4 days.

More worrisome, natural disasters also present significant risks in the cloud services environment. For example, in August 2018, Microsoft suffered an outage caused by a severe lightning storm in the San Antonio; Azure's South-Central United States data centre region was down for quite a while. Customers across the world using Active Directory and Visual Studio Team Services faced trouble for more than 24 hours. Therefore, service availability and performance plays a major role in cloud computing as the needs of the customers should be attended to at all times. Regrettably, the existing models practically focused only on information security as an area of risk at the exclusion of services availability and performance.

4.2 The Risk Assessment Criteria

Chandran and Angepat (2010) used "Data Cost" and "Cloud Providers' Service History" as risk criteria to assess the risks associated with the public cloud service providers. Feng et al. (2012) used the "Cloud Providers History" as a risk criteria in the assessment of the public cloud service providers' risks. Matthew and Rose (2012) relied on the information security contractual obligations embedded in Service Level Agreements (SLA) to assess the potential risk associated with a service provider while Daniele and Giles (2009), Mouna et al. (2015), Cayirci et al. (2016); Greg & Pierre (2016); Sivasubramanian (2017) and Akinrolabu et al (2019) used the lists of information security threats within the public clouds to assess the associated risks of the public cloud service providers. These criteria are not sufficient in providing an accurate evaluation of risks level to the public cloud consumers as they are specifically based on the information security risk aspect of the public clouds. While these two risk criteria can be considered as major criteria in the determination of information security risk within the public clouds, they are not able to specifically affect the public cloud services availability and performance; neither do they cover all the public cloud services information security loopholes.

Therefore, in addition to the "Data Cost"(Asset Cost) and "Providers' History" from the existing models (Chandran and Angepat, 2010; Feng et al., 2012; Mouna et al., 2015; Greg and Pierre, 2016) and others, three additional risk criteria of **Service Location, Adopted Technology** and **People** are introduced in this research study as these three criteria have been identified as major cloud risk determinants in the public clouds that have direct and indirect effects on the information security as well as the services availability and performance of the public cloud services.

4.2.1 Data Cost

In assessing the risk that is associated with selecting a particular public cloud provider, it is essential that the value, critically and sensitivity of the data or assets to be transferred to the cloud is recognized as well as the service providers' reputation (Armbrust et al, 2010; Aissaoui et al., 2017; Domingo-Ferrer et al., 2019). The under-classification of data or assets could result in such assets being placed in an inappropriate cloud service that cannot provide expected level of protection and services. Conversely, over-classification of assets could lead to unnecessary demand of protection and services being specified leading to excessive costs resulting in suitable cloud services providers being rejected (Scott et al, 2010). Therefore it is crucial that the consumers accurately assess the value, criticality and sensitivity of the assets to be placed on the public cloud and correctly classifies it to ensure that the appropriate cloud service provider that meets expected services and protection is shortlisted and selected.

In the process of assessing the assets cost, certain important considerations must be noted as regards the assets and the reputation of the service providers, such as:

i. The owner(s) of the assets/data
ii. The users of the assets/data
iii. The businesses or services supported by the assets/data
iv. The legislation that applies to the information
v. The share values of the service providers and the assets owner(s)
vi. The impact of the assets on the owner's organization and business

Data cost is considered as one of the criteria variables because the consumers can assign a cost to the data based on the data's value, criticality and sensitivity, with its impact on the consumers' organization reputation and service.

4.2.2 Providers' History

Provider's History is considered as another parameter in the process of determining the risk that is associated with a particular public cloud service provider as it includes the record of the past services provided by the service providers to their customers, enabling the consumers to assess the provider(s) service reliability (Chandran & Angepat, 2010; Feng et al (2012). By examining the history of service providers, the prospective consumer would be empowered with information regarding the providers' years of service experience, the nature of rendering services and the industries of the past and existing customers with the customers' locations, the service availability rates of the past services, among other information.

More importantly, the information about the service providers can also reveal the percentage of services directly supply by the service providers and the percentage that is contracted to other parties (subcontractors) and the locations of these subcontractors. The service providers' past and existing relationships with these others parties and the reliability of services of the parties can be examined, this will allow the prospective consumers to rate the service providers.

4.2.3 Service Location

Charanya et al (2013); Mohammed et al (2013); Srivastava and Khan (2018) and Deebak et al (2020) identified data sovereignty risk as a major challenge in the public cloud environment, the researchers based their conclusion on the fact that most public cloud services providers or their data centres are mostly located outside the jurisdiction of the service consumers. The information and data laws differ from country to country; therefore the laws that influence the access of information held by the service providers vary from country to country based on the location of such information (data) or service providers. Hashizume et al (2013); Velliangiri et al (2020) and Alghofaili et al (2021) reported that the movement of data into the public cloud and potentially across and between legal jurisdictions including offshoring of data processing allows certain practices that provide intruders with gates to the information in the cloud, more so that it is difficult to guarantee that a copy of data or its backups are not stored or processed in a certain jurisdiction.

In certain instances, a service provider may be compelled by a foreign law enforcement agency or legally constituted court to provide data belonging to their customers, while legally prohibited from notifying the customer(s) of such disclosure request. In some circumstances, service providers outsource or sub-contract part of the delivery of the service to a third-party leading to additional data sovereignty risks. For example, in August 2014, Microsoft was ordered by a United States Federal Court to turn over customers' data stored in its Republic of Ireland data centre, the Federal Court Judge (Loretta Preska) rejected Microsoft's argument that a United States' search warrant does not extend beyond the country's border (Jaikumar, 2014). Therefore, it is very important for the service consumers to identify the legal jurisdictions in which their data will be stored, processed or transmitted and how the laws of those countries could impact on the confidentiality, integrity, availability and privacy of the data.

Furthermore, certain locations are known for experiencing frequent natural disasters such as flood, earthquake, hurricanes, tsunamis or volcanic eruptions which can affect the cloud service availability and invariably the information availability to the consumers. In 2012, the Atlantic hurricane season saw the arrival of Sandy, the 2nd-costliest hurricane in U.S. history. The floods and power outages wreaked havoc on data centres in New York, New Jersey, Florida and the surrounding areas resulting in the disruption of access to data stored in the public cloud globally, particularly the credit card services for days. The incident perhaps opened up broader discussions around the impact of natural disasters on businesses and services continuity, that nothing is immune to the wrath of Mother Nature, not even the cloud (Uri, 2013).

4.2.4 Adopted Technology

Srivastava and Khan (2018); Verma and Sharma (2019) and Dong et al (2019) reported service availability, performance unpredictability and system interoperability as challenges confronting the organizations' decision of moving to the public cloud. Liliana *et al*. (2014); Srivastava and Khan (2018) and Verma and Sharma (2019) presented the lack of interoperability standards as a major threat within the public cloud environment. Sah et al. (2014); Dong et al., (2019); Mohiuddin et al., (2019); Aldribi et al (2020) and Yang et al (2020) insisted that the multi-tenancy method of service delivery using resource pooling through the virtualization technology creates great privacy and service availability risks, as service providers deliver services to multiple customers (tenants) by sharing the same computing resources.

While resource pooling and sharing has its benefits in terms of costs, it does introduce some form of risks related to either infrastructure virtualization or data commingling that must be considered by the cloud service consumers. Virtualization is an important technology in the delivery of public cloud services as it enables information systems to be abstracted from the underlying hardware using a hypervisor (that is, software that enables a host server to run multiple guest operating systems concurrently).

The most often cited area of concern of this technology is that a malicious customer could exploit vulnerability within the hypervisor to gain access to another customers' information by performing a 'guest-to-host' or 'guest-to-guest' attack. Also, some cloud services such as SaaS and PaaS use logical controls within the application or platform and supporting infrastructure to isolate access to each customer's data. However, the data are usually commingled within the application, database and back-up systems. This places complete reliance on the quality of the design, implementation and enforcement of access controls within the platforms and applications.

More importantly, denial of service (DoS) attacks is an inherent risk for all Internet facing services. The use of cloud services may increase the risk of such an attack as the aggregation of multiple customers into a single service may present a more attractive target for attackers. Therefore, a customer may suffer associated or collateral damage in form of service unavailability in an attack against a service provider or a co-customer. The service providers adopted protocols and technologies, such as, Anycast, Application Delivery Networks and Content Delivery Networks in distributing network traffics and computer processing can determine the extent of such attack against their services platforms.

These concepts explain the importance of service availability, performance unpredictability and system interoperability as decisive elements in the provision of public cloud services. The elements are product of the technologies being adopted by the cloud providers, such as operating systems, virtualization systems, network systems, cooling system, security protocols (such as, encryption protocols and authentication methods), application programming interface, and database management systems. Unfortunately, these important elements were not considered in the existing works. It is therefore certain that the types of technologies adopted and the adoption rate of new technologies by the public clouds providers play major role in the service delivery of the offered services and such important element cannot be ignored in the process of assessing the risks associated with the public cloud services providers for the purpose of selecting the appropriate provider that meets the requirements of the consumer among the available alternatives.

4.2.5 The People

The peoples' dimension of the public cloud technology which encompasses all its classes of users and their roles cannot be overemphasized in the process of assessing risks associated with public cloud service providers. Gouda et al. (2014); Yunchuan et al. (2014); Michael et al. (2015); Domingo-Ferrer et al., 2019 and Tabrizchi and Rafsanjani (2020 observed that the inability of the public cloud consumers to ascertain the service providers' employees' reliability and trustworthiness, and whether a service provider has appropriate procedures in place to ensure that its personnel are reliable and trustworthy is a common concern for organizations planning to use public cloud services.

Farhad and Sajjad (2012); Kumar et al (2018); Jouini and Rabai (2019); Yang et al (2020) considered public cloud service providers insider threat as a major concern to the public cloud consumers, as unauthorized access to sensitive information by the service provider's employees is a common concern for organizations' planning to use cloud services.

The idea of handing over important data to another company which reliability and trustworthiness of its employees cannot be ascertained worries some individuals and organizations. For example, on 28 February, 2017, an Amazon Web Services Engineer trying to debug a Service Storage System (S3) at their Virginia data centre accidentally typed an incorrect command and much of the Internet including many enterprise platforms and cloud servers critical-mission services were down for 5 hours resulting to cloud services international outage. The outage from the provider that owns roughly a third of the global public cloud market reignited debate on the risks of public cloud (Joseph, 2017).

The public cloud service customers should ascertain the experience and expertise of the key employees and whether the service providers have appropriate procedures in place to make sure their personnel are reliable, trustworthy and do not pose a security risk to their clients. Though, the level of assurance available to the consumers vary significantly depending on the physical location of the service provider's services and its employees, as it may be very easy to ascertain such security check of the service provider's employees if the prospective customer is within the same geographical jurisdiction as the service provider. However, where a service is delivered or supported from another geographical jurisdiction (country) these security checks procedures may be very difficult to undertake or even impossible. In such circumstances, the prospective customers may consider whether the available alternatives to the service provider can provide an equivalent level of assurance. Although, while vetting may prevent service providers from employing someone that has a history of being untrustworthy, it does have its limitations, as vetting that reveals a criminal record may result in a potential employee being rejected. In the same manner, candidates that are untrustworthy but have never been caught or have not been convicted may not be identified. So also, previously trustworthy employees may become untrustworthy if they become disgruntled or their personal circumstances change.

Interestingly, the on-demand self-service characteristic of cloud computing also introduces security concerns as the customers' registration processes (usually, web-based self-registration) are not always robust to confirm a customer's identity. This weakness can allow a malicious customer(s) to register for services to be used for malicious activities that may include attempting to subvert the access controls to gain unauthorized access to another customer's data. These human involvements in the activities of the cloud services have major implications on both the service providers and consumers organizations, and this should be a major criterion for consideration in the assessment of the risks associated with public cloud service providers.

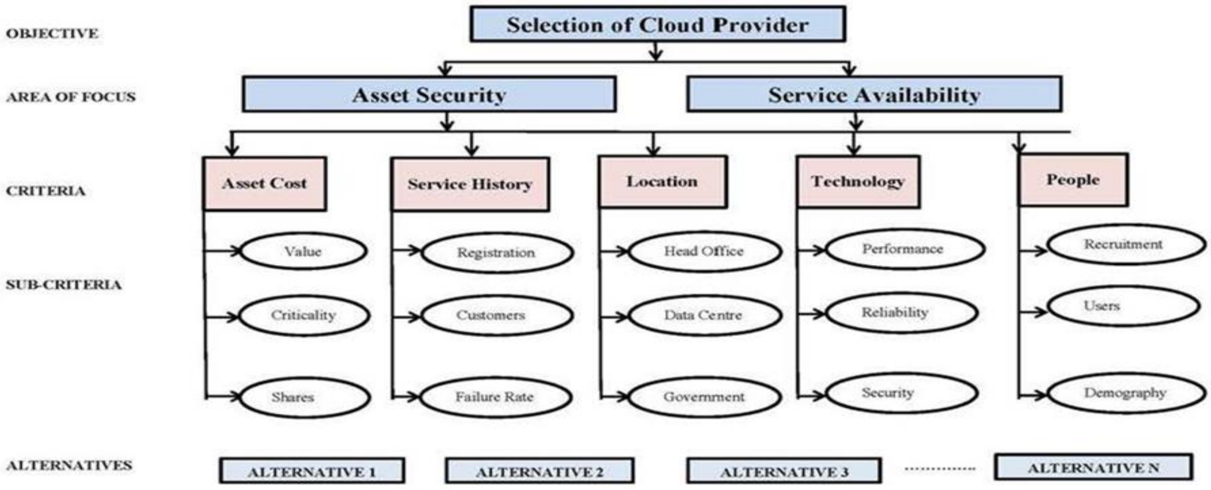

Figure 1: The Hierarchy of the Selection Parameters and the service Providers Alternatives

5. CONCLUSION

The challenges faced by the public cloud consumers in the process of selecting appropriate public cloud providers that meet their organization's requirements. The selection decision becomes more complicated in case of multiple service providers, conflicting criteria and imprecise parameters, stressing the need for comprehensive criteria that factors the dynamic nature of public clouds computing systems. Therefore, in addition to the two major parametric criteria (Data Cost and Provider's History) adopted by the majority of the existing models and frameworks, newly established risk criteria have been added, these are Service Location, Adopted Technology and the People.

The extension of the risk criteria as assessment parameters is made necessary as a result of the extension of risk assessment focus areas to include service availability and performance in addition to the information security, so as to produce a more accurate risk assessment of the public cloud service providers that can assist the public cloud consumers to make appropriate selection decision among the available public cloud services providers.

6. REFERENCES

[1] Abdurachman, E.; Gaol, F.L and Soewito, B. (2019). Survey on Threats and Risks in the Cloud Computing Environment. Procedia Computer Science, Vol.161, pp. 1325–1332.

[2] Aissaoui, K.; Idar, H. A.; Belhadaoui, H and Rifi, M. (2017). Survey on Data Remanence in Cloud Computing Environment. In the Proceedings of the International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS, 2017), Fez, Morocco, 19–20 April 2017.

[3] Akinrolabu, O., Nurse, J. R. C., Martin, A and New, S. (2019). Cyber risk assessment in cloud provider Computers and security Vol. 87: 101600.

[4] Aldribi, A.; Traoré, I.; Moa, B and Nwamuo, O. (2020). Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking. Computers and Security. Vol. 88: 101646.

[5] Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. A and Al-rimy, B. A. S. (2021). Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. Applied. Science 2021, 11, 9005. https://doi.org/10.3390/app11199005.

[6] Armbrust, M., Fox, A., Katz, R., Konwinski, A., et al. 2010. A View of Cloud Computing. Communication of the ACM, Vol. 53, No. 4, pp. 50-58.

[7] Berg, H. (2010). Risk Management: Procedures, Methods and Experiences, Bundesamt für Strahlenschutz, Salzgitter, Germany, 2010.

[8] Cayirci, E., Garaga, A., Santana de Oliveira, A., Roudier, Y. (2016). A Risk Assessment Model for Selecting Cloud Service Providers. Journal of Cloud Computing: Advances, Systems and Applications. Vol. 5, No. 14.

[9] Chandran, S. P. and Angepat, M. (2010). Cloud Computing: Analyzing the risk involved in cloud computing environments. In Proceedings of the International Conference on Natural Sciences and Engineering, Sweden, pp. 2–4

[10] Charanya, R., Aramudhan, M., Mohan, K. and Nithya, S. (2013). Levels of Security Issues in Cloud Computing. International Journal of Engineering and Technology, Vol. 5, No. 2. pp. 1912-1920.

[11] Cloud Security Alliance (CSA). (2010). 'Top Threats to Cloud Computing V1.0. www.cloudsecurityalliance.org/topthreats (Accessed: 13 December, 2021)

[12] Daniele, C. and Giles, H. (2009). Cloud Computing: Benefits, risks and recommendations for information security. ENISA, Crete (Greece). https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

[13] Deebak, B.; Al-Turjman, F and Mostarda, L. (2020). Seamless secure anonymous authentication for cloud-based mobile edge computing. Journal of Computers and Electrical Engineering. Vol. 87, 106782.

[14] Domingo-Ferrer, J.; Farràs, O.; Ribes-González, J and Sánchez, D. (2019). Privacy-Preserving Cloud Computing on Sensitive Data: A Survey of Methods, Products and Challenges. Computer Communications. Vol.140, pp. 38–60.

[15] Dong, S.; Abbas, K and Jain, R. (2019). A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. IEEE Access, Vol. 7, pp. 80813–80828.

[16] Eric, H., Ed, M. and Karen, G. (2012). Risk Management for Cloud Computing. TechTarget, MA 02466, USA.

[17] Farhad, S. G and Sajjad, H. (2012). Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy. International Journal on Scientific and Technology Research. Vol. 1, No.6. pp. 49-54

[18] Feng, X., Yong, P., Wei, Z., et al. (2012). A Risk Management Framework for Cloud Computing. IEEE 2nd International Conference on Cloud Computing and Intelligent Systems, pp. 476-480. China.

[19] Gouda, K. C., Dines, D., Anurag, P., *et al.* (2014). Migration Management in Cloud Computing. International Journal of Engineering Trends and Technology, Vol. 12, No. 9. pp. 466-472

[20] Greg, S. and Pierre, N. (2016). Cloud Risk Decision Framework: Principles and Risk-Based Decision-Making for Cloud-Based Computing. Microsoft Inc., USA.

[21] Hashizume, K., Rosado, D., Medina, E.F., et al. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications. Vol. 4, No. 5

[22] International Organization for Standardisation (ISO). (2009). ISO 31000: Risk management - Principles and guidelines. https://www.iso.org/standard/43170.html

[23] Irshad, A.; Chaudhry, S.A.; Alomari, O.A.; Yahya, K and Kumar, N. (2021). A Novel Pairing-Free Lightweight Authentication Protocol for Mobile Cloud Computing Framework. IEEE System Journal. Vol. 15, pp. 3664–3672.

[24] Jaikumar, V. 2014. Data Security and Privacy Issues in the Cloud: Microsoft ordered to turn over customer data stored in the cloud. [Online]. Available: https://www.computerworld.com/article/2490690/technology-law-regulation/microsoft-ordered-to-turn-over-customer-data-stored-in-the-cloud.html. (Accessed: 21 October, 2021).

[25] Joseph, T. (2017). The 10 Biggest Cloud Outages of 2017. https://www.crn.com/slide-shows/cloud/300089786/the-10-biggest-cloud-outages-of-2017-so-far.htm/pgno/0/5. (Accessed on: 4 September, 2021).

[26] Jouini, M and Rabai, L.B.A. (2019). A Security Framework for Secure Cloud Computing Environments. In Cloud Security: Concepts, Methodologies, Tools, and Applications; IGI Global: Hershey, PA, USA, pp. 249–263.

[27] Kamal, K. H., Ruchi, D. and Rakesh, R. (2014). Security and Privacy Issues of Cloud and Grid Computing Networks. International Journal on Computational Sciences and Applications. Vol. 4, No. 1. pp 83-91.

[28] Karajeh, H.; Maqableh, M and Masa'deh, R. (2020). Privacy and Security Issues of Cloud Computing Environment. In the Proceedings of the 23rd IBIMA Conference Vision, Valencia, Spain, 13–14 May 2020.

[29] Kumar, P. R.; Raj, P. H and Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science. Vol.125, pp. 691–697.

[30] Li, H., Liu, L., Lan, C., Wang, C and Guo, H. (2020). Lattice-Based Privacy-Preserving and Forward Secure Cloud Storage Public Auditing Scheme. IEEE Access, Vol. 8, pp. 86797-86809.

[31] Liliana, F.B. S., Diogo, A.B. F., Joao, V.G., et al. (2014). Cloud security: state of the art, in: Security,

Privacy and Trust in Cloud Systems. Springer, Berlin, Heidelberg. pp. 3–44.

[32] Matthew, H. L. and Rose, G. (2012). SecAgreement: Advancing Security Risk Calculations in Cloud Services. In proceedings of 2012 IEEE 8th World Congress on Services, Honolulu, HI. pp. 133-140.

[33] Mazhar, A., Samee, U. K. and Athanasios, V. (2015). Security in cloud computing: Opportunities and challenges. Information Science, Elsevier. Vol. 305, pp. 357-383.

[34] Michael, M., Rajiv, R., Lizhe, W., et al. (2015). CloudGenius: a hybrid decision support method for automating the migration of web application clusters to public clouds. IEEE Transaction on Computers, Vol. 64, No. 5. pp. 1336-1348.

[35] Mohammed, A. A., Ben, S. and Eric, P. (2013). A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds. Journal of Software, Vol. 8, No. 5. pp. 1068-1078.

[36] Mohiuddin, I.; Almogren, A.; Alrubaian, M and Al-Qurishi, M. (2019). Analysis of Network Issues and their Impact on Cloud Storage. In the Proceedings of the 2nd International Conference on Computer Applications & Information Security (ICCAIS, 2019), Riyadh, Saudi Arabia, 1–3 May 2019.

[37] Mouna, J., Latifa, B. R. and Ridha, K. (2015). A Multidimensional Approach Towards a Quantitative Assessment of Security Threats. In Proceedings of the 6th International Conference on Ambient Systems, Networks and Technologies. Procedia Computer Science 52, Elsevier, pp. 507-514.

[38] Nautiyal, S and Wadhwa, S. (2019). A Comparative Approach to Mitigate Economic Denial of Sustainability (EDoS) in a Cloud Environment. In the Proceedings of the 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 21–22 November 2019.

[39] Odun-Ayo, I., Agono, F and Misra, S. (2018). Cloud Migration: Issues and Developments. In the Proceedings of the International MultiConference of Engineers and Computer Scientists (IMECS 2018), Hong Kong. Vol. 1.

[40] Paul, V., Pandita, S and Randiva, M. (2018). Cloud Computing Review. International Research Journal of Engineering and Technology (IRJET), Vol. 5 Issue 3. pp. 1454-1456.

[41] Peiyu, L. and Dong, L. (2011). The New risk assessment model for information system in Cloud Computing environment, Procedia Engineering 15, Elsevier, pp. 3200 – 3204.

[42] Prasad, S. and Ben, W. (2010). QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. In Proceedings of the IEEE 3rd International Conference on Cloud Computing, pp. 280-288.

[43] Qureshi, A.; Dashti, W.; Jahangeer, A and Zafar, A. (2020). Security Challenges over Cloud Environment from Service Provider Prospective. Cloud Computing and Data Science, Vol.1, pp.1–48.

[44] Rana, A. and Mohammad, A. (2016). Risk Management Framework for Cloud Computing: A critical Review. International Journal of Computer Science and Information Technology. Vol. 8, No. 4.

[45] Ren, K., Wang, C and Wang, Q. (2012). Security Challenges for the Public Cloud. IEEE Internet Computing, Vol. 16, No.1, pp. 69-73.

[46] Sah, S.K., Shakya, S. and Dhungana, H. (2014). A security management for cloud based applications and services with diameter-AAA. In Proceeding of IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT). pp. 6–11.

[47] Scott, P., Paul, T. J and Susan, C.W. 2010. Identifying the Security Risks Associated with Governmental Use of Cloud Computing. Journal of Government Information, Quarterly 27, pp. 245-253.

[48] Shukla, S. (2014). Public Cloud Security Challenges and Solution. International Journal of Scientific Engineering and Research. Vol. 2, Issue 4, pp. 111-117.

[49] Siddiqui, S.; Darbari, M and Yagyasen, D. (2019). A Comprehensive Study of Challenges and Issues in Cloud Computing. In Soft Computing and Signal Processing; Springer: Singapore, 2019; pp. 325–344.

[50] Singh, J. (2017). Study on Challenges, Opportunities and Predictions in Cloud Computing. International Journal of Modern Education and Computer Science, Vol. 3, pp. 17-27.

[51] Sivasubramanian, Y.; Ahmed, S. Z and Mishra, P. V. (2017). Risk Assessment for Cloud Computing. International Research Journal of Electronics & Computer Engineering. Vol. 3, No. 2. Pp. 7-9.

[52] Srivastava, P and Khan, R. (2018). A Review Paper on Cloud Computing. International Journals of

Advanced Research in Computer Science and Software Engineering. Vol. 8, Issue 6, pp .17-20.

[53] Stoneburner, G., Goguen, A. and Feringa, A. (2002). NIST SP 800-30 Risk Management Guide for Information Technology Systems. NIST, pp. 8-26.

[54] Tabrizchi, H and Rafsanjani, M.K. (2020). A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions. Journal of Supercomputers. Vol. 76, pp. 9493–9532.

[55] Uri, B. (2013). Enterprise Cloud Strategy: Lessons learned from recent cloud outages. https://www.rightscale.com/blog/enterprise-cloud-strategies/lessons-learned-recent-cloud-outages. (Accessed: 23 January, 2019)

[56] Velliangiri, S.; Karthikeyan, P and Kumar, V.V. (2020). Detection of Distributed Denial of Service Attack in Cloud Computing Using the Optimization-Based Deep Networks. Journal of Experimental and Theoretical Artificial Intelligence Vol. 33, Issue3, Pp.405-424.

[57] Verma, D. K and Sharma, T. (2019). Issues and Challenges in Cloud Computing. International Journal of Advanced Research in Computer and Communication Engineering. Vol. 8, Issue 4, pp. 188-195.

[58] Wu, Y., Lyu, Y and Shi, Y. (2019). Cloud Storage Security Assessment through Equilibrium Analysis. Tinshhua Journal of Science and Technology. Vol. 26, No. 6. pp. 738-749.

[59] Xu, J., Liang, C., Jain, H. K and Gu, D. (2019). Openness and Security in Cloud Computing Services: Assessment Methods and Investment Strategies Analysis. IEEE Access, Vol. 7, pp. 29038-29050.

[60] Yang, C.; Tan, L.; Shi, N.; Xu, B.; Cao, Y and Yu, K. (2020). AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud. IEEE Access Vol. 8, pp. 70604–70615.

[61] Yogeshwaran, S., Syed, Z. A and Ved, P. M. (2017). Risk Assessment for Cloud Computing. International Research Journal of Electronics and Computer Engineering. Vol. 3, No 2. pp. 7-9.

[62] Yunchuan, S., Junsheng, Z., Yongping, X., et al. (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks. Volume 2014, http://dx.doi.org/10.1155/2014/190903. (Accessed on 17 January, 2022).