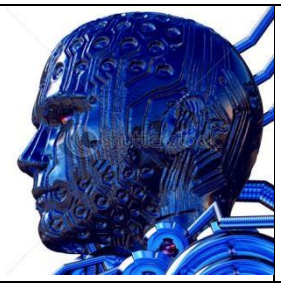

*TRS

Technology, Networks and Society

e-planning | **networks** | **e-learning** | **e-government**

Internal Report TRS 05/2017

Título

MSL Framework: (Minimum Service Level Framework) for Cloud Providers and Users

Author(s)

Sohail Khan, UFP

Luis Borges Gouveia, UFP

Month, Year

April, 2017

Web site *http://tecnologiaredesesociedade.wordpress.com*

Scientific Repository *trs *http://bdigital.ufp.pt/handle/10284/3787*

University Fernando Pessoa

Praça 9 de Abril, 349

4249-004 Porto, Portugal

ABSTRACT

Cloud Computing ensures parallel computing and emerged as an efficient technology to meet the challenges of rapid growth of data that we experienced in this internet age. Cloud computing is an emerging technology that offers subscription based services, and provide different models such as IaaS, PaaS and SaaS to cater the needs of different users groups. The technology has enormous benefits but there are serious concerns and challenges related to lack of uniform standards or nonexistence of minimum benchmark for level of services across the industry to provide an effective, uniform and reliable service to the cloud users.

As the cloud computing is gaining popularity organizations and users are having problems to adopt the service due to lack of minimum service level framework which can act as a benchmark in the selection of the cloud provider and provide quality of services according to the users expectations. The situation becomes more critical due to distributed nature of the service provider which can be offering service from any part of the world.

Due to lack of minimum service level framework that will act as a benchmark to provide a uniform service across the industry there are serious concerns raised recently in security and data privacy breaches, authentication & authorization, lack of third party audit and identity management, integrity and variable availability standards, confidentiality and no uniform incident response and monitoring standards.

This paper examines the impact of lack of minimum service level framework and proposes a conceptual model based on uniform minimum model that acts as benchmark for the industry to ensure quality of service to the cloud users. The framework act as a set of minimum standards to be provided by the cloud provider. The MSL framework, proposes a set of minimum and uniform standards in the key areas which are essential to the cloud users and provide a minimum quality benchmark that becomes a uniform standard across the industry.

Key Words

Minimum Service Level Framework, Service Level Agreement, MSLF, Utility Computing, Cloud Computing, General Data Protection Regulation, Data Security, CIAA (Confidentiality, Integrity, Availability, Authentication).

Introduction

The term “Cloud Computing” is defined by the National Institute of Standards and Technology (NIST) as “a model or enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, server, storage, applications, and services) that can be rapidly provisioned and released with minimal effort or service provider interaction” [16]. In the last many years, the computation has experienced enormous changes from centralized to distributed system and now moving back to the centralization as a structure. The benefit of the cloud computing services are many where the model significantly cut IT infrastructure costs and this saving can be used for operational expenses, also model provides on-demand access to vast IT resources that are available in the cloud [3].

The rapid growth of data which we have experienced in this internet age, the capacity of normal PC can’t meet the demand of large-scale massive data scientific computing [8]. The model with its benefits have lots of concerns which have been raised. This model leaves the client/customer not aware of where the data is stored or how it is maintained. Due to the design of the model the client or customers has lack of or no control over their data and where internet is used as a communication media to access data. The security and privacy of the data in the cloud computing is a major issue and the provider has to provide concrete assurance in Service Level Agreement (SLA) to assure the customer regarding the data protection and privacy issues [4].

The increase of public cloud providers, cloud consumers face various challenges such as data security and privacy issues, authorization and authentication breaches, poor availability standards, lack of interoperability and response time standards, methodology to allocate resources, weak or no third party audit mechanism and lack of monitoring and responses standards [4] [5] [10].

As you see from the following figure. Customers’ biggest concern; identifies major concerns while using cloud services. It is not possible to fulfil all the customers’ expectations where service providers are offering different quality of service and there is no framework to benchmark the services offered by these various cloud providers.

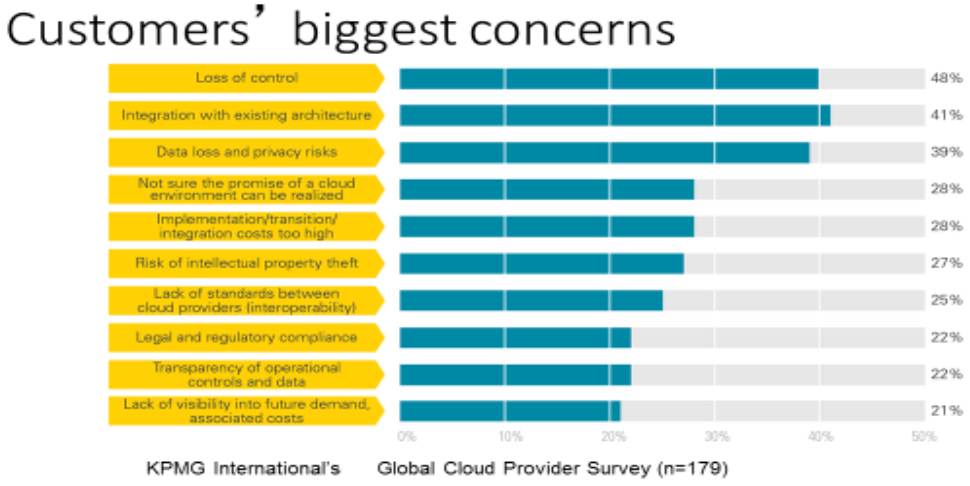

Figure 1 – Customers' biggest concerns

Source: KPMG International's Global Cloud Provider Survey.

Cloud computing is an emerging technology and facing a growing demand so hundreds of technology based companies such as Amazon, Salesforce, Google, Microsoft, IBM, Yahoo and many others are trying to capitalize on the emerging market [5]. More companies can bring better competition, deliver choices and meet customer's requirements but all these companies have variable level of services or no uniform standards so the selection process is based upon their own business models and different set of Quality of Services (QoS) [1].

Due to the reason it is confusing for the cloud users to differentiate and select the cloud provider as there is no minimum set standards. There is an increasing number of Cloud providers but the concern that is raised by the users is the selection of the provider according to their set requirements it is a difficult job due to lack of uniform standards or a benchmark that is agreeable to all the providers.

The selection of the cloud services is a completely different from any online services. As cloud services are different in nature such as SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), IaaS (Infrastructure-as-a-Service). When we have to select a provider for SaaS services then providers such as Salesforce, Google Apps will have different requirements than any other model. These cloud services have different quality of services such as security, privacy, integrity, authentication and authorization [6].

The cloud users and providers will have different interpretation and the level of expectation will be different for the cloud services. The situation becomes very difficult if there is no standards or benchmark to measure the quality of service of the cloud services [6].

At the start of selection of the cloud provider, the negotiation process between the potential users and the cloud provider takes place in which they agree on set standards known as Service Level Agreement (SLAs) [2]. SLAs consist of Quality of Services (QoS), these are different rules which are contractual bounded to be followed both the parties [1].

SLA parameters are scalability, privacy, security, availability which increases the level of confidence to the cloud users. The main purpose of SLA is to define the each QoS and identify the responsibility [3]. It enables the end-users to agree on the type of services are offered, who will be responsible for the service execution [9]. If there is SLA breach the cloud provider is subject to pay for the SLA breach as the contract shall describe what will be the consequences if the quality of service is not meet [2].

Due to lack of standards SLA in cloud computing; the providers are not legally obliged to provide any template or a benchmark or pay back for any losses [1]. This is due to lack of standards in the industry. The cloud providers will provide the uptime as the main indicators whereas other services are not clear and situation becomes more difficult when identical services is given different price, quality of services and customer experience [3].

There is a critical need to have a mechanism to provide minimum service level framework that acts as a quality of services benchmark to the customers who are using or planning to use the cloud computing services regardless of their location, size of the business and business needs. A mechanism or a framework that provides comprehensive set of services that are crucial and helps the selection of the cloud provider and acts as uniform standard that guarantees the quality of set of services to the cloud users.

The educational institution can be the biggest beneficiary of using the cloud computing infrastructure with major savings. As the educational institutions are trying to reduce cost, cloud model will provide benefits as they don’t have to invest heavily on or to maintain their computing infrastructure. With increased number of educational institutions opting for cloud services; this raises many questions and the one which needs urgent attention is lack of minimum standards across the providers or what type of minimum service level should students, staff and employees of the educational organizations should expect from the cloud providers.

The situation becomes more critical due to distributed nature of the service provider which can be offering service from any part of the world. Here the question should be raised how the students and staff at educational institutions should be satisfied with the security and privacy of their data where a provider can be operating across the world with different standards of security requirements and different set of laws & policy.

The issues for various educational institution; relates to the data security and privacy, authorization and authentication, availability and third part audit mechanism to ensure that provider have compressive framework to meet the quality of services requirements of the cloud users which can provide better services with set assurance of a quality of services .

A framework or guidelines that are provides minimum service level standards across the industry that can enable cloud users to choose the provider based on reliable and universally agreed mechanism is required to allow more organizations to use the service and reduce uncertainty that exists.

Setting the Work:

Research Question

The Research question to be investigated is as follows:

> Main question: *Is it possible to implement a Minimum Service Level framework for educational institution's users (students, staff and employees); offering a uniform standards of service clearly defining a benchmark for all the cloud providers across the industry regardless of their locations.*

The main question to be investigated in this research is the implementation of Minimum Service Level Agreement for educational institution's users (students, staff and employees) so that there is a uniform standards of services across the industry regardless of their hosting location. The above research questions will resolve critical issues faced by students, staff at different educational institutions using cloud services on daily basis.

The research will provide a framework to enforce and comply a minimum service level standards on all the cloud providers. The minimum service level standard will act as a benchmark for all

the providers across the industry and also users can select a provider based on the standard which will act as a performance indicator according to the services offered by the providers.

Research Aims and Objectives

There is a very important need to have a MSLF Minimum Service Level Framework that clearly defines a universal benchmark standards for all the providers to follow and implement regardless to their location. The universal minimum service level standards will act as a performance indicator which will enable the customers to choose a provider easily and compare the quality of service.

Aim of the Research

To implement a Minimum Service Level Agreement; for educational institution's users (students, staff and employees); offering a uniform standards of service clearly defining a benchmark for all the cloud providers across the industry regardless of their locations.

Objectives

- To identify different flaws and weaknesses in the current Service Level agreement offered by the cloud providers.
- To investigate the requirements of the educational institution's users and challenges they face in the adoption and usage of cloud computing as a service.
- To propose a Conceptual framework; which will act as a Minimum Service Level framework for the educational institution.
- To design, develop and implement a test-bed using a private cloud platform to perform tests on SLAs.

A Brief Literature Review

Cloud Computing is emerging market and its growing at an exponential rate. The selection process of a cloud provider is a daunting task as it entails very complex details that has to be considered by the potential cloud users [4].

The selection process is more complex then proposed multi-objective optimization [5], that overcomes some of the limitation in the selection of the cloud provider but the provision of Pareto front of optimal solutions creates the selection of the final solution more problematic.

In the existing literature there are proposed models such as Wang [6], where the entire selection of the service is according to the consumer's perception and their experiences. In the real world web or cloud services can't be assessed just on the basis of the consumers' experiences as there should be a multi-factor included in the final decision.

In order to rank the best cloud services SMICloud [7] has introduced a model that only considers quantifiable SLA attributes according to Cloud Service Measurement Index Consortium (CSMIC) [8] and there is no mention of qualitative attributes. Some proposed frameworks compare the performances of different cloud services as Amazon EC2, Windows Azure and Rackspace CloudCmp [10], but the limitation in these model is it only compares the low-level performance metric such as CPU utilization and network throughput.

The model can be further developed to incorporate indicators such as high-level system properties focus around power consumption [11]. The model propose by Hoi Chan [12], is based on few applications; as model lacks on weighting mechanism of cloud services that are linked to the cloud provider. CloudRank [14], proposes a cloud ranking algorithm that revolves around a ranking algorithm based on functional parameters and fail to incorporate the delivered services in their framework. The model such as Qu [15], based around consumers experience and involves a third party to monitor and oversee the entire process but lacks in the performance measurements and evaluation framework. The following figure 2 explains the cloud infrastructure.

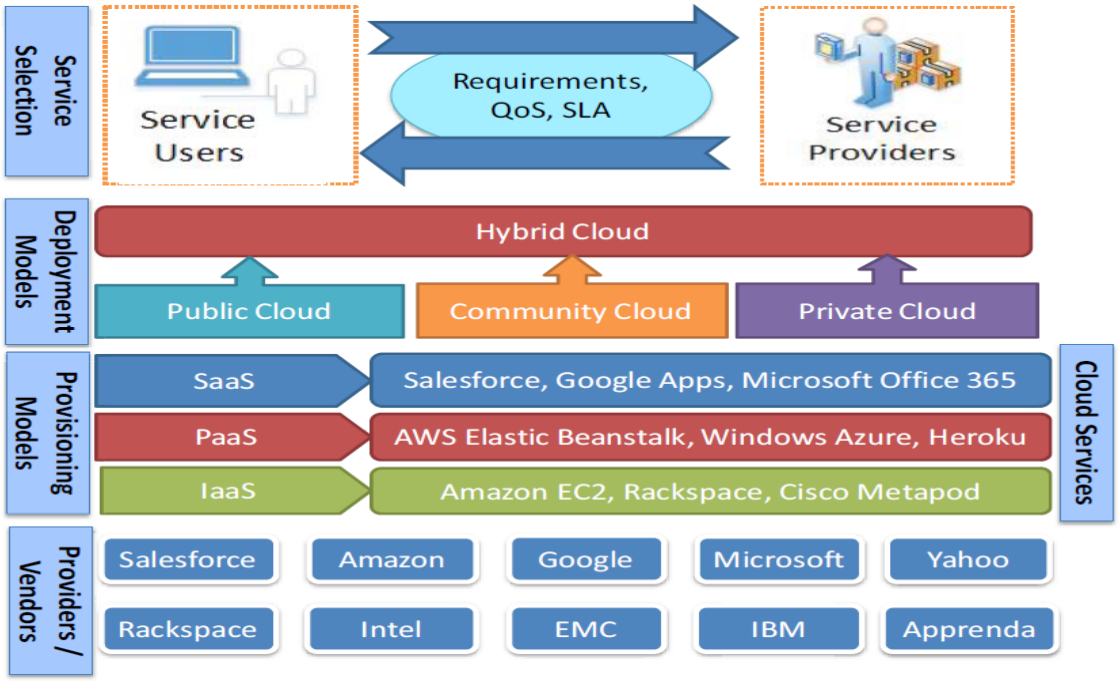

Figure 2 – The Cloud Service Infrastructure

Source: Taken from [9]

Different models and frameworks were proposed that will enable the selection of the cloud providers. One of the major trends is Service-Oriented Architecture (SOA) in which the delivery of services is done, by using the web service over the Internet [11].

The services can be tailored according to the user's requirements and quality of services required [12]. According to Sun [2] cloud service selection process can be divided into two main sections such as Multi-Criteria Decision Making (MCDM) and Multi-Criteria Optimization Method (MCOM). These models went under detail analysis and findings show that there is a lack of advanced measurements of user preferences. Whereas Manvi [11], address this issue by providing metrics to quantify each of the schemes.

The authors tried to justify that the challenge of resources management depends on the demand of each application and resources are allocated accordingly. The study helped to understand the management of resources and its impact on the service selection and optimization. Baranwal [16], proposed a new approach for cloud service selection that is based in ranked voting. The highest normalized preference score will indicate the preferred cloud provider.

Quality of Service (QoS) is the most important factor in-terms of selecting the cloud provider. According to Burkon [12], QoS plays a key role in the service selection process especially for SaaS model. In [7], CSMIC introduced the Service Measurement Index (SMI) that indicates various categories defined by various key entities.

The model provides a Key Performance Indicators (KPI) for measuring and comparing the services. However, there is no standardized SLA framework that sets as a benchmark across the industry. As there is no standardized SLA framework and different providers are using their own proprietary SLAs this makes it nearly impossible to compare the services offered by different providers.

Due to lack of standards the selection of cloud provider becomes a difficult task for the end-users who don't have so much of technical knowledge. The study further elaborates that this selection technique is a complex process for ordinary users who have limited or no technical knowledge of cloud technologies. A standardized SLA can be an effective way to monitor the performance and make the cloud provider accountable whereas enable the cloud user to easily select the provider and demand a certain level of quality of service from the provider.

SLA has multiple stages to develop and implement the life cycle management. The five stages are Service Development, Negotiation and Marketing, Implementation and evaluation as shown from the following figure. SLA management provides different types of services such as pre-run time and runtime [14]. In the pre-run time contains details that before the service runtime is started. In this phase SLA registration, Service Inquiry & Contract and negotiation has to be completed.

The Service provider has to register the types of service in the management system, which is available for the client to be searched. After this there is a direct contact between the service provider and service client to negotiate the SLA contract to assure that client can pay according to their requirements according to SLA metrics and penalty rules. As per the agreement the client should follow the rules and same, applies to the service provider [13]. In the next stage known as Run Time where the focus is to monitor and observe all the SLA metrics and identify any violation that has occurred.

The main focus is that all SLA metrics should meet the agreed requirements and if the requirements are not met then violation decision has to be made based on the rule that is violated. The main purpose of cloud computing contracts is to define the SLA and ensure that all SLA

conditions are met. These SLAs are around data protection legislation, security of data, data protection, location of data, licensing and retention of data.

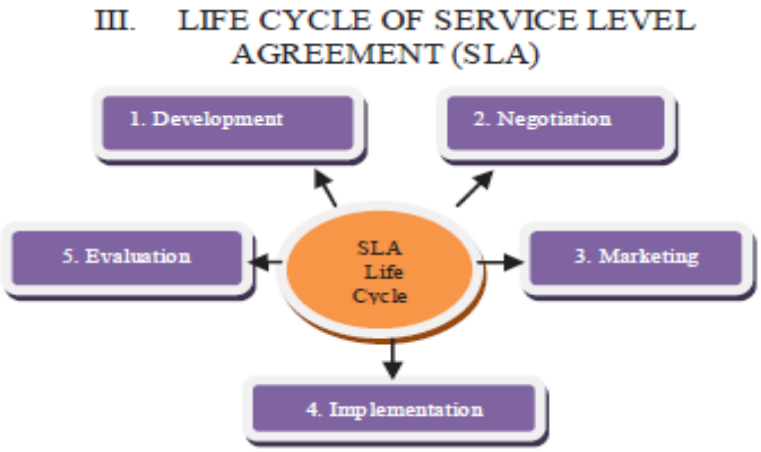

Figure 3 – SLA Life Cycle

Service Level Agreement is a negotiated formal contract, that exist between the cloud users and the provider and both parties have to abide by all the terms that were agreed. As mentioned [19], SLA is defined as a legal document that stipulates a set of terms such as usage or services, service data, delivery mode, quality of services, cost/price of service and condition for penalty in the case of SLA violation [17].

SLA should specify the Quality of Services (QoS) related to specific role [18]. The specification of service level agreement provides to ensure the services are delivered with availability, security, reliability and performance [19]. Cloud services are associated with various QoS entities such what type of performance is provided by the provider, how reliable is the system, the layer of defense that is provided to protect the security and privacy of the client's data. Further QoS attributes are usability factor, comparison of prices and incident response mechanism that is in place by the cloud provider [21].

There can be different expectation from the cloud user and provider for QoS delivered, as there is a lack of standard benchmark to measure the QoS [4]. SMI is a major step to standardized the cloud QoS but it is not a holistic approach and doesn't cater all the necessary requirements for the cloud users.

In cloud computing service level agreement violations do occur because of multiple factors such as unexpected interruption in the Internet connection, hardware, software and network failures [18]. Failure as a Service (FaaS) is model that deals with cloud service and disruption. As more and more users are opting for cloud computing; many recent events have be highlighted of disruption and interruption of services. Cloud computing is a distributed in its setting that has resulted in high unstable platform facing massive scale failure in real deployment.

Cloud Computing with each day pass has an increased number of resources any failure affects the application which are hosting the service [11]. There are an increased number of services hosted by cloud and there is a possibility of failure to be occurred in the cloud. In order to protect the users a string set of service level agreement need to be designed to cater all these needs.

Cloud Computing Challenges

The major security challenge faced by cloud computing is security and privacy of data. The concern related to security and privacy of data is raised due to the decrease in the rate of reliability and efficiency. Security in cloud computing has become the most important topic which needs urgent attention [9].

According to the following table use authentication and access control is one of the serious challenges faced by the cloud, based environment for both the service providers and end-users [18]. In the past many studies and researcher have tried to propose solution to improve efficiency and reliability of managing access and ensure authentication but still there are many cases reported of the breach [3].

TABLE I: SECURITY CONCERNS IN CLOUD COMPUTING ENVIRONMENTS

Service Provider	*Infrastructure*	*End-User*
Identity and User Authentication	Data-Storages	Data Protection
Privacy and Access Control	Network Hardware	Loss of Governance
Data Transmission	Other Hardware	Managing Accesses
Possible Attacks		Reliable Authentication
Unpredictable Events		Browser Security
Supporting Processes		Visibility of Data
Third-Party Applications		

Table 1 – Cloud Computing Security Challenges

Source: Taken from [17]

In order to protect and provide privacy to the data the new privacy framework has been recently initiated known as GDPR (General Data Protection Regulation) that provides a new policy to deal with the challenges of privacy of the data in the information society [21].

The regulation (EU) 2016/679, provides protection to process the personal data and provides safeguards to the movement of such data within EU members [22]. If GDPR regulation doesn't explicitly states about cloud computing, about the regulation is designed with cloud computing as a central focus of attention [24].

The law will be enforced in 2018 (25^{th}, May), so the cloud providers should place systems to be prepared for the new rules and avoid any major issues [21]. In order to meet these new challenges and provide better security for cloud users the authentication and authorization need to be enhanced to provide a safe cloud environment. Forensic tasks are very difficult since the investigators are not able to access system hardware physically [19].

Different studies have identified that data related to critical applications and sensitive in nature to be hosted over the cloud has always raised serious concerns as the data is continuously moved between the data centre network and the client setup. The system is considered to be secure when we reduced all the threat to a minimum level that is acceptable to the organization.

To provide better user authentication and access control some model are applying various solution such as Applying agent-based authentication system [17] and multi-factor authentication process [20] both these solutions can increase reliability of authentication process but still there is no uniform solution that can be followed across the industry to provide privacy and security to the data.

Threat	Description
Data Breaches	Release of protected data in an untrusted environment
Data Loss	Information is lost due to improper storage, transmission or processing
Account or Service Traffic Hijacking	Attack methods such as fraud and exploitation of services
Insecure APIs	Attack on code-signing keys used by web and cloud for identification
Denial of Service	Refusing user access to their data or applications
Malicious Insider	Any insider misusing their authority to harm the cloud system
Abuse of cloud services	Using the cloud servers and services for malicious activities
Insufficient Due Diligence	Risk due to incomplete understanding of the cloud infrastructure
Shared Technology	Attacks due to multi-tenant architecture, re-deployable platforms and shared resources

Table 2 – The Notorious Nine: Cloud Computing Threats

Source: Taken from [11]

The non-functional requirements such as availability, confidentiality, integrity, scalability, response time, reliability, and monitoring and response mechanism are crucial to the cloud consumers to ensure better quality of service. The availability is the probability that the cloud infrastructure or service are up and running in the specific time of utilities of the service provided for in the SLA [11].

The other non-functional requirement is scalability; the cloud provider should facilitate the specific resources for ease of scaling up and down that will maximize revenue and cloud providers are able to optimise resource effectively [8]. The limitation is the existing work is there is no set standards that are required for non-functional requirements such as availability of

services, response time and scalability; and what would be the consequences if the cloud provider can't offer services up to acceptable level.

The resource location is a major concern for the end-users, as most of the users don't know exactly where the resources for such services are located [19]. This can lead to serious dispute that can happen which is not in control to the cloud providers.

To save cost large amount of cloud providers are storing data across the world where data protection and privacy safeguards are not considered as rigors and comprehensive. This is a serious risk to the security and privacy of data as according to the data compliance and privacy laws states that locality of data has an importance for each enterprise [15].

The European Union issued a Directive 95/46/EC that prohibits transfer of personal data to countries, which do not ensure the adequate level of protection of data. There are many examples such as Dropbox users have agreed in the "Terms of Services" which grants the provider the right to right to disclose the personal users information with the compliance to law enforcement request [19]. This raises serious privacy risk to the user data.

Data availability and timely access to the cloud data is another serious security challenges for the cloud providers and users. The availability of the cloud provider is becoming a serious challenge as cloud services are disrupted and the best example is Amazon cloud services in year 2011 got affected resulting in no service for various website such as Reddit, Foursquare and Quora [16].

Services hosted on SaaS application provider are required to ensure effective services around the clock which means infrastructural changes to add scalability and high availability and resiliency in the hardware/software failure to protect against the denial of service attacks and appropriate business continuity and disaster recovery plan [5].

This can play a vital role by ensuring the safety of the data and maintaining a minimal downtime for any enterprise. In the case of Amazon [7], Amazon Web Services (AWS), to protect against these threats are using various mitigation techniques such as synchronous cookies, connection limiting, extra internal bandwidth and a world-class infrastructure but these procedure and standards are different for each provider.

The confidentiality and information security is another concern of the existing and the potential cloud users. There are serious questions raised about the intentional or unintentional unauthorized disclosure of information. The data can be stored remotely it is accessed while

using Internet connection [14]. The entire user's data can be stored at the same platform as other user's data, which can lead to serious concern on data confidentiality and information security.

As the data is stored outside the enterprise boundary, the SaaS vendor must adopt additional layers of security to protect and prevent any breach of data. The cloud vendors such as Amazon (EC2), administrators don't have access to customer instances and cant log into the guest OS [17].

One administrator with business needs is required to use individual cryptographically strong secure shell to gain access to the hot [8]. All accessed are logged and audited routinely. In terms of audit it's not clear whether a third party is allowed to carry out the audit and what procedures are followed. The data owner will not have a physical access to the data and traditional cryptographic primitives for the purpose of data security protection can't be directly adopted [27].

In this scenario, there is a need of third-party auditor (TPA) [28] that provides efficiency, transparency and fairness in performing the required audit and closes the gap between the cloud provider and users. This mechanism provides realistic security solution where cloud users achieve majority of the cloud benefits at a very minor cost, the auditing of TPA is required. Currently this is a not a required standard and there is a legitimate concern for the security of data and confidentiality raised by the cloud users.

There is lack of uniform standards across the cloud providers in the industry. Due to lack of uniform standards, interoperability can't be achieved across the cloud providers [19]. The existing storage specification by a provider can be completely incompatible with the storage specification of the different cloud provider that can lead to interoperability issues. For e.g. if the cloud user want to move data from one provider to another there can be a situation that it is not possible due to lack of uniform standards.

Data stored in Amazon's S3 is totally incompatible with IBM's Blue cloud or Google storage. There are serious implications for the cloud users as there are no uniform standards across the industry for cloud providers, which can lead to less users opting for cloud option. As reinforced by [25], many general computing standards may be re-used in the cloud but for the moment there are to our knowledge no dedicated minimal standards that provide a uniform service to the cloud users and acts as a benchmark to the quality of service offered by the providers.

As cloud provides a model that is based on multi-tenancy to reduce cost and improve the efficiency to host multi-users data in the same platform [3]. In these circumstances the data that belongs to different users will reside at the same storage location. This environment can lead to intrusion of data from one user to another by exploiting vulnerabilities at the application level or by infecting the code at the SaaS system [7].

There is a need to be a mechanism that can define a clear boundary not at the physical level but at the application level to stop any intrusion. There is a need to have compatible solution that segregate data from the users and this solution followed by all the providers across the industry. Currently there is no uniform standard to ensure that data segregation doesn't take place and different providers provide different solution to this problem.

The standards vary while making storing backups as well. For example in the case of Amazon the data at rest in S3 is not encrypted by default [12]. The cloud users have to encrypt the entire data and define a backup strategy so that it can't be accessed by the unauthorized person, and confidentiality, integrity and availability is maintained. This is another example of different standards and no minimum benchmark that provides a uniformity of services to be offered by the cloud providers.

The limitation in the existing academic work is there is no minimum framework of standards of services that should be adapted by the cloud providers to provide a uniform set of services to the cloud users. The proposed research; sets a minimum service level framework that will define a uniform guideline for all the clouds providers to provide a set of services that is comparable and act as a benchmark to measure the performance of the providers. The proposed model will allow the selection of cloud provider easier and cloud users can expect better quality of services with the implementation of the framework.

The Proposal: MSL Framework (*Minimum Service Level Framework*)

Cloud Computing ensures parallel computing and emerged as an efficient technology to meet the challenges of rapid growth of data that we experienced in this internet age. The technology has enormous benefits but there are serious concerns and challenges related to lack of uniform standards or nonexistence of minimum benchmark for level of services across the industry to provide an effective, uniform and reliable service to the cloud users.

As the cloud computing is gaining popularity organizations and users are having problems to adopt the service due to lack of minimum service level framework which can act as a benchmark in the selection of the cloud provider and provide quality of services according to the users expectations.

Due to lack of minimum service level framework that will act as a benchmark to provide a uniform service across the industry there are serious concerns raised recently in security and data privacy breaches, authentication & authorization, lack of third party audit and identity management, integrity and variable availability standards, confidentiality and no uniform incident response and monitoring standards.

This research examines the impact of lack of minimum service level framework and proposes a conceptual model based on uniform minimum model that acts as benchmark for the industry to ensure quality of service to the cloud users.

The main contribution of the research is to investigate and implement a MSL (Minimum Service Level) Framework for educational institutions offering a universal agreed standards of set services that will act as a benchmark for all the providers across the industry regardless of their hosting location.

The research will play a vital contribution in the field of cloud computing as we are experiencing increase number of users using the service which is raising many questions and the most important that needs urgent attention is lack of minimum standards across the providers or what type of minimum service level should we as users expect from the cloud providers.

Thus, resulting the research to address concerns of users about the providers hosting services from different parts of the world where security standards are not very rigorous as compared to the standards we experience in western countries. The Minimum Service Framework will provide an uniform universal standards for all multinational and medium sized organization; where security and privacy of their data is a major concern and this will allow more users to use the service which will reduce their infrastructure cost.

The research will make major contribution to provide minimum service level framework that will act as a benchmark to provide a uniform service across the industry there are serious concerns raised recently in security and data privacy breaches, authentication & authorization, lack of third party audit and identity management, integrity and variable availability standards, confidentiality and no uniform incident response and monitoring standards.

The educational institution can be the biggest beneficiary of this research. The cloud model will provide benefits to the educational institutions because they don't have to invest heavily on or to maintain their computing infrastructure and it provides a greater flexibility to choose any provider.

With increased number of educational institutions opting for cloud services; this raises many questions and the one which needs urgent attention is lack of minimum standards across the providers or what type of minimum service level should students and employees of the educational organisations should expect from the cloud providers.

The model provides uniformity across the industry setting a guideline for all the manufacturers to follow regardless of their location around the world. As the number of cloud users are increasing it is crucial to have universal agreed minimum service level agreement that all providers have to follow and implement that becomes minimum standards across the industry.

The research will remove hurdles and challenges that are faced by the cloud users to find out what provider they should trust their data with as there no benchmark or universal minimum service level standards across the service providers which can ease the selection of the cloud provider and improve the overall QoS.

The research will play a vital role to the users to find out which providers is better in-terms of offering service as there is no Minimum indicator that define the quality of service being offered. So it becomes really difficult to choose a provider with no universal standards or minimum service level that these customers can expects from the provider. A detailed framework is required to enforce and comply to a minimum service level standards on all the cloud providers.

The minimum service level standard will act as a benchmark for all the providers across the industry and also users can select a provider based on the universal standard which will act as a performance indicator according to the services offered by the providers.

The Proposed Model

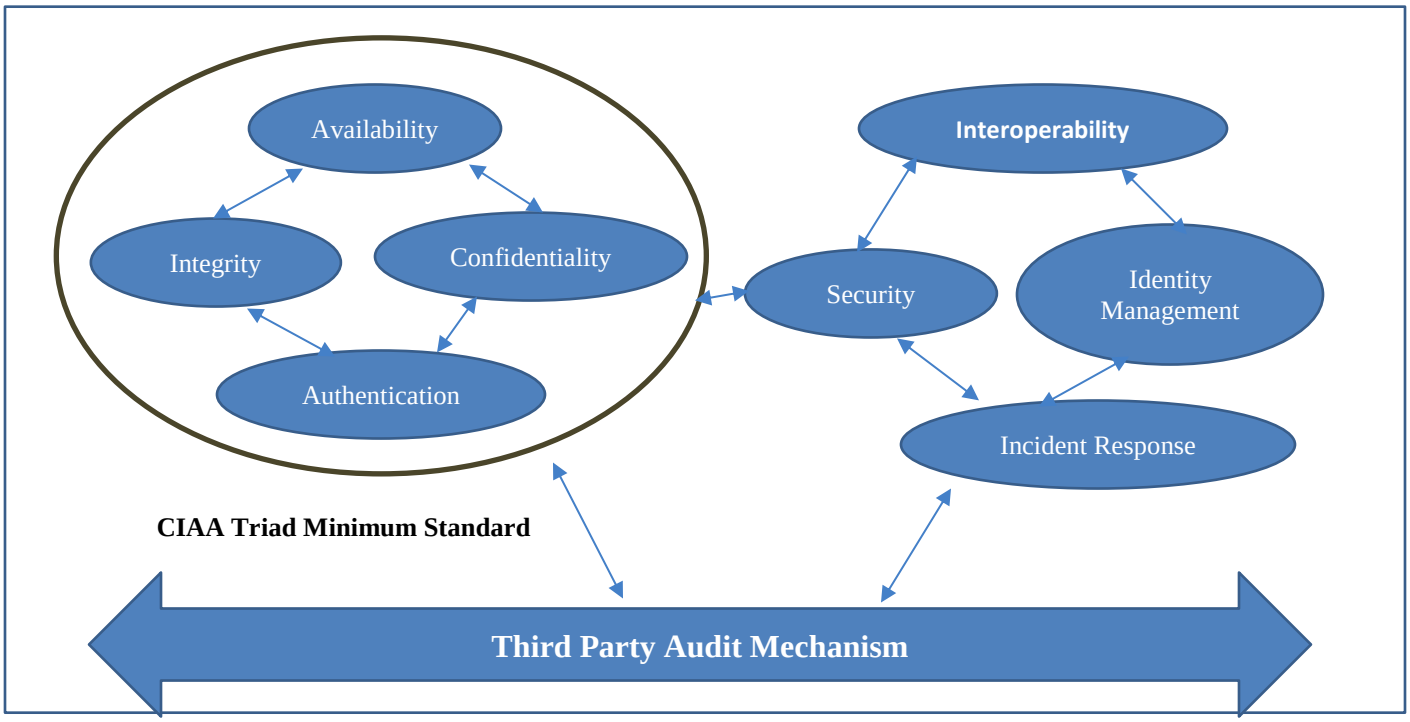

Figure 4 – Proposed MSL Framework

Methodology

For this research the methodology that will be deployed in order to collect qualitative data is Grounded Theory. The methodology best suites this research as it will collect data from people who have experienced the issues faced by the educational institutions. As reinforced by Fortin, Grounded theory provides mechanism to collect data from a particular area from those individuals who have relevant experience in that field. Semi-structure interviews and questionnaire will be used to collect data.

As [29], grounded theory is a comprehensive technique for data collection by using semi-structure interviews, key stakeholders, observation, focus groups and questionnaires can generate data for grounded theory. The theory is flexible [30] as it provides a systemic way of clearly

defined analytic steps but at the same time provides flexibility for the researcher to make adjustments to meet the research requirements.

The theory allows the researcher [30], to collect data from the participants, provide a mechanism to identify the data by using open coding and provide relationships between different key areas and entities.

The participants in the research are selected according to the job designation or title from different areas so that different opinions are gathered in the research [29]. The theory is a systematic methodology in the social sciences involving in the detail analysis of the data and tries to establish relationships between set of data.

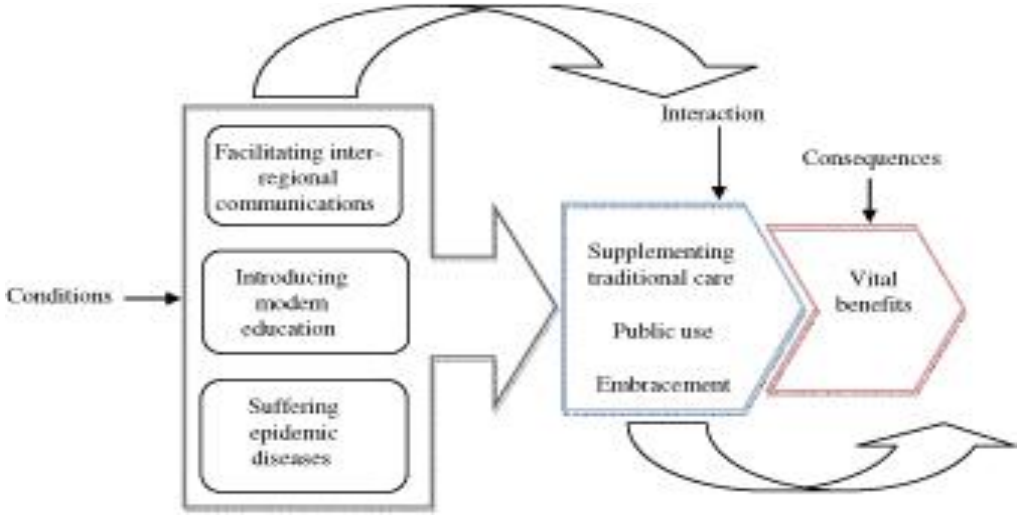

Figure 5 – The Grounded Theory Methodology approach

For the research initial the permission from the case study (the educational institution) will be taken in order to conduct the qualitative research from students, staff and employees working at the institution. After the approval, then emails will be sent to the students and staff to voluntarily become the part of the research.

Participants will be divided into different groups based on their position at the workplace and series of semi-structure interviews with questionnaires will be conducted. In order to triangulate the data personal observation will be conducted as well to ensure that data gathered through the interviews and questionnaire is reliable and authentic.

The participants to answer the interviews and questionnaire will be presented with the informed consent form that will state the data usage and previously approved by the University and the case study management Ethics committee approval.

Research Contributions

As the cloud computing is gaining popularity organizations and users are having problems to adopt the service due to lack of minimum service level framework which can act as a benchmark in the selection of the cloud provider and provide quality of services according to the users expectations.

The research will contribute by investigating the impact of lack of minimum service level framework and what problems the existing and the new cloud users for e.g. students, staff and employees at an educational institution are facing while trying to adopt or use the cloud service.

The main contribution of the research is to investigate and implement a MSL (Minimum Service Level) Framework for educational institutions offering an universal agreed standards of set services that will act as a benchmark for all the providers across the industry regardless of their hosting location. The framework provides minimum standards for set of key services, which are very crucial to the cloud users and provide better quality of services.

The uniform universal standards across the industry will provide mechanism to the potential new cloud customers to choose the cloud provider regardless of their hosting location; expecting minimum uniform international standards of security and privacy for their data. The framework will remove any ambiguity and confusion and allow more cloud usage.

The framework will acts as a benchmark for minimum expectable standards in-terms of Quality of Service (QoS), for data authorization and authentication, data privacy & integrity, data availability and confidentiality and minimum standards for interoperability, identity management and provide comprehensive auditing mechanism.

The framework will ensure trustworthiness of a service provider, removing ambiguity of implementation of law and data protection and uniform performance indicators to choose the provider easily based on set standards regardless of their hosting location. Following, are some more contributions from the undergoing research:

1. To investigate the existing Service Level Agreements offered by the cloud providers to educational institution's users such as students and employees; to identify the challenges faced due to lack of Minimum Service Level Framework;
2. Identify the most critical requirements and problems for the existing and new cloud users at an educational institution. Investigate the key threats faced to the data of the users at the educational institutions;
3. To investigate and implement a Minimum Service Level Agreement; for educational institution's users (students, staff and employees); offering a uniform standards of service clearly defining a benchmark for all the cloud providers across the industry regardless of their locations;
4. To implement a uniform standards across the industry that will provide mechanism to the students, staff and employees of the educational institutions to choose the cloud provider regardless of their hosting location; expecting minimum uniform recognised standards on all key set of services such as security and privacy of data;
5. Defining and implement a SLA mechanism for educational institution users (students and employees) that provides a uniform standards on availability of service, data security and privacy, integrity, data interoperability, response time, a defined mechanism for resource allocation, trustworthiness of service provider and remove ambiguity of implementation of law and data protection;
6. To implement Performance Indicators that will help educational institutions to choose the best cloud providers and make them accountable for the quality of service offered according to the MSL framework.

References

[1] AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-Health cloud: opportunities and challenges," Future Internet, vol. 4, no. 3, pp. 621–645, July 2012.

[2] Solanas et al., "Smart health: a context-aware health paradigm within smart cities," Communications Magazine, IEEE, vol. 52, no. 8, pp. 74– 81, August 2014.

[3] Holzinger, C. Röcker, and M. Ziefle, “From smart health to smart hospitals,” in Smart Health Open Problems and Future Challenges, A. Holzinger, C. Röcker, and M. Ziefle, Eds. Berlin: Springer, 2015, pp. 1–20.

[4] Burkon, Lukas, “Quality of Service Attributes for Software as a Service”, Journal of System Integration, vol. 4 issue 3, pp. 38,September 2013

[5] Baranwal, G. and Vidyarthi, D. P. (2016) ‘A cloud service selection model using improved ranked voting method’, Concurrency and Computation: Practice and Experience, , p. n/a–n/a. doi: 10.1002/cpe.3740.

[6] Communication from the Commission to the European Parliament, the Council, the EESC and the Committee of the Regions, “Unleashing the Potential of Cloud Computing in Europe,” COM/2012/0529 final.

[7] Kotsokalis, J. Rueda, S. Gmez, and A. Chimeno, “Penalty management in the sla@soi project,” in Service Level Agreements for Cloud Computing, 2011.

[8] Duan Q (2011) Modeling and Performance Analysis on Network Virtualization for Composite Network-Cloud Service Provisioning. 2011 IEEE World Congress on Services.

[9] Elsenpeter RC, Velte TJ and Velte AT (2009) Cloud Computing: A Practical Approach (1st edition). New York: McGraw-Hill Professional Publishing

[10] Garg, S.K.; Versteeg, S.; Buyya, R., "SMICloud: A Framework for Comparing and Ranking Cloud Services," in Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on , vol., no., pp.210-218, 5-8 Dec. 2011. doi: 10.1109/UCC.2011.36

[11] Han and J. Xing, “Ensuring Data Storage Security through a novel Third Party Auditor Scheme in Cloud Computing,” Proc. 2011 IEEE

[12] International Conference on Cloud Computing and Intelligence Systems (CCIS), 2011, pp. 264-268.

[13] Judith Hurwitz, Robin Bloor, Marcia Kaufman, Cloud Computing for dummies, HP Special edition.

[14] K. Pande Joshi and C. Pearce (2015) "Automating Cloud Service Level Agreements using Semantic Technologies", Proc. of the 2015 IEEE International Conference on Cloud Engineering (IC2E), 9-13 March 2015, Tempe, AZ, USA, pp.416-421

[15] Intel Corporation (2012) Intel® Cloud Finder - Cloud Service Providers Search Tool. [Online] Available at: http://www.intelcloudfinder.com/ (accessed 03/06/15).

[16] Khalil, A. Khreishah, and M. Azeem, “Cloud Computing Security: A Survey,” MDPI Computers, vol.3, no.1, 2014, pp. 1-35.

[17] Manvi SS and Shyam GK (2014) Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey. Journal of Network and Computer Applications. 41, 424–440

[18] M. Guzek, A. Gniewek, P. Bouvry, J. Musial, and J. Blazewicz, “Cloud brokering: Current practices and upcoming challenges,” IEEE Cloud Computing, vol. 2, no. 2, pp. 40–47, Mar 2015.

[19] M. Guzek, P. Bouvry, and E.-G. Talbi, “A survey of evolutionary computation for resource management of processing in cloud computing [review article],” IEEE Computational Intelligence Magazine, vol. 10, no. 2, pp. 53–67, May 2015.

[20] M. Guzek, J. E. Pecero, B. Dorronsoro, and P. Bouvry, “Multi-objective evolutionary algorithms for energy-aware scheduling on distributed computing systems,” Applied Soft Computing, vol. 24, pp. 432–446, 2014.

[21] Mell, P. and Grance, T. (2012) The NIST definition of cloud computing recommendations of the national institute of standards and technology special publication 800-145. Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (Accessed: 8 February 2016).

[22] NIST, National Institute of Standards and Technology, US Department of Commerce, Special Publication 500-291, Version 2.

[23] Peter Mell, Timothy Grance,”NIST Definition of Cloud Computing”, Special Publication 800-145.

[24] “Service Measurement Index Framework Version 2.1”, July 2014, Carnegie Mellon University Silicon Valley

[25] S. Mei, C. Liu, C. Yong, W. Jiangjiang, and W. Zhiying, “TETPA: A Case for Trusted Third Party Auditor in Cloud Environment,” Proc. IEEE Conference Anthology, 2013, pp. 1-4.

[26] Sun, L., Dong, H., Hussain, F. K., Hussain, O. K. and Chang, E. (2014) ‘Cloud service selection: State-of-the-art and future research directions’, Journal of Network and Computer Applications, 45, pp. 134–150. doi: 10.1016/j.jnca.2014.07.019

[27] Velte, A.T., Velte, T.J. and Elsenpeter, R.C. (2009) Cloud computing: A practical approach. New York: McGraw-Hill Professional Publishing.

[28] Yu R, Yang X, Huang J, Duan Q, Yan and Tanaka Y (2012) QoS-aware service selection in virtualization-based Cloud computing. 2012 14th

[29] Zibin Zheng; Xinmiao Wu; Yilei Zhang; Lyu, M.R.; Jianmin Wang, "QoS Ranking Prediction for Cloud Services," in Parallel and Distributed Systems, IEEE Transactions on , vol.24, no.6, pp.1213-1222, June 2013. doi: 10.1109/TPDS.2012.285