International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 6 Issue 11, November-2017, Impact Factor: 4.059

A Consumer Friendly, Security Based Cloud Service Rating System

Salman M Hussain

ABSTRACT

Cloud computing services are undoubtedly one of the fastest growing trends in the field of information technology. However there has been a lot of debate on the issue of security, data transparency, informed storage and trust in the field of cloud computing. This research focuses upon carving a method to rate the cloud service providers and their services on the above mentioned factors along with other parameters related to security in order to make it easier for a common user to rely upon cloud services.

INTRODUCTION

Cloud computing is being touted as one of the greatest revolution in the field of information technology, with many small sized and medium sized organisations moving on to the cloud and also many general users using cloud for one reason or the other it can very well be said that cloud has a bright future ahead. However, the speed at which the cloud is growing as per some of the critics is very slow when compared to what it should have been seeing all te positives and advantages that the cloud has to offer. The main reason for this steady growth according to many of the critics is the lack of trust, transparency, informed storage and data security. The very next prominent reason according to many critics that hinders the growth of the clod is said to be the lack of knowledge amongst the customers with respect to the cloud services and their exact advantages, they say that there is a lot of misconception related to the cloud which actually falls on its face when compared factually. The last but not the least and one of the most important issues of the cloud is the legal aspect of it or as some might call it the legal turmoil of the cloud. The very nature of cloud services to store data at data centres that might be in the user's country or might not be in the user's country lands cloud in a catch 22 position.

There is no second thought in the fact that software or information technology has become an essential part of one's life just as food, shelter and clothing. This can be remarked as a very laudable achievement, but what is more concerning is that all the providers of the rest of the basic amenities are held liable by the government of almost every nation when something goes wrong from their part, thereby it would not be wrong to say that software and software companies will soon be held liable for the mistakes on their part and this would mean that cloud will also come under the liability criteria , it would not be wrong to say that cloud might be the very first aspect which would make the world think upon making companies liable for their software commodities and services.

When one from the general netizencommunity thinks of the cloud, he generally tends to think that cloud is not too safe for his information to be stored and has many security concerns surrounding it, he would generally think that storing data on a physical device is much safer than on the cloud. This actually is a myth being propagated because if we see the number of breaches of the public cloud they tend to be almost negligible when compared to security breaches on physical devices. This wrong perception or the uninformed behaviour from the consumer perspective is one of the greatest blockage for the growth of the cloud.

Verily cloud computing has given the world a new perspective of efficient computing and it drastically reduces the infrastructure cost required for a particular task to be done, it has become a very prominent business concept amongst the major Information technology companies who now rent out their unused infrastructure to the ones who actually need it. This is a win-win situation for both the provider and the consumer as the provider is earning from what would otherwise be wasted and the consumer is saving by using the service being provided without actually having to purchase the whole infrastructure. As there are more and more number of user moving on the cloud, the attention of the illicit users of technology the hacker community is also increasing in the cloud. Due to this development the research community has now shifted its focus from security in the cloud to security of the cloud.

In order to have a holistic structured growth of the cloud there will have to be an active participation from the cloud consumer, the cloud provider and the federal government. The cloud consumer has to make it his responsibility to keep

himself informed about the cloud technologies and the advances in the cloud sector, the cloud provider should take responsibility to convey its users of how much effort is being put in to keep their information secure and also has to actively take reviews of the services from the user, the government should see to it that the data of its citizens is not compromised with and also there is not an hostile environment for the cloud providers meaning that the cloud providers should not feel that they are being burdened by the policy being made.

The proper analysis of the service level agreements is required from a customers and a government's perspective, this is because if a service level agreement is made solely in the interest of the cloud provider it will hush away the customers from accepting the cloud service, also the governmental policies should be analysed to see to it that the interest of both the customer and the provider are taken into account. The customer's interest also needs to be properly tapped because extraneous expectations can never be met by the provider and can also be damaging to the constructive growth of the cloud.

The service levels of the cloud are IAAS, PAAS and SAAS, of these service levels the one that garners maximum customers is undoubtedly the SAAS layer which gives software as a service for its users, and the SAAS layer also gives the least control to the user over the security policies and data storage. In order to garner increasing number of customers it is of prime importance that the issues of the customers of the SAAS layer are dealt with in a proper manner and a solution is carved out to make it easier for the customers of the SAAS layer to rely on cloud services being provide.

In general terms the users or consumers of IAAS and PAAS services are technologically aware users and are often the ones which are related to a collaboration of personnel related to the field of information technologies i.e. the consumers are mainly companies which run their business solely as an information technology firm or companies where information technology plays a major role in running the business. The SAAS layer consumer's generally are the wider heterogeneous community of general netizens of which there is more possible chance of them not being associated with the terms and terminologies of information technology at all. It is thereby a very hard path to convince these users to rely upon loud services as they are not technologically aware of the benefits of the cloud and also are the ones that generally get panicked when they hear that something is wrong with any new technology in market.

It is an evident fact that these people contribute and will contribute as the majority of the consumers of the cloud services and their holistic participation will only lead to the cloud achieving its due growth. There has to be a way in which the research community is able to carve out a solution which would help these consumers come on board with minimal doubts about the services and quality of the services.

There is an increasing need for a solution to address the real problem on ground and for the research and industry communities to understand the fact that in order to achieve success in the field of cloud computing the active participation of the general consumer is of prime importance.

While designing the path for this research, the main idea was to try to carve a middle way which would benefit all the three stakeholders without burdening one another. The literature reviewed for this research focused primarily on finding out what the existing concerns are surrounding the cloud that are hindering its growth are and also reviewing the concerns from all the three perspectives.

The research after carving out the possible parameters to rate a cloud provider on the basis of security and other aspects will move on to carving a fully developed methodology to take this approach and make it into a formalised rating method. The method then will be compared to existing solutions and also research supporting the effectiveness of the proposed method will be put forward. Critical analysis of the proposed solution will also be done and shortcoming if any will also be brought into light. Future research directives would then conclude the proposed research paper.

RESEARCH QUESTIONS

The research basically aims at listing don of security issues and general issues that are hindering the growth of cloud computing, the second important aspect of the research would be to find out what steps have been taken by the research community in the direction of making cloud computing a better space, furthermore the research will aim at finding out what actions have been taken by the governments of various countries to make the cloud a better and safer place, lastly the research will analyse the service level agreements of various cloud providers and will then try to carve out a framework to rate the cloud provider's services.

RESEARCH METHODOLOGY

This research is a synthesis of qualitative and quantitative research, qualitative research will be used carves out a solution framework and quantitative research will then be used to check the validity of the solution.

As the solution to be proposed is a rating methodology the quantitative methods of surveys and interviews will be used to prove the validity of the proposed solution.

LITERATURE REVIEW

The research tried to find out what the existing community thinks about the possible threats that are hindering the growth of the cloud and how they propose to solve the given problem at hand, the existing literature was reviewed keeping in mind to find solutions to the question of security threats to the cloud, the importance of informed storage, trust and transparency, the flaws in the existing service level agreements and the current governmental policies at hand. This method of research helped in narrowing down the broad available research done by the community and allowed the research to be focused upon papers that talk about the security threats and their possible solutions, papers that try to take consumers (specially SAAS) perspective and give it a prime importance in their solution and papers that talk about the legal ways in which the problem of cloud has been addressed.

The very first conclusion made while going through the existing research was that the security issues in the cloud are a cluster of heterogeneous ones and this is mainly due to the fact that cloud computing in itself is a cluster of various driving factors or enabling technologies such as distributed computing, the internet, grid computing etc. which makes it the direct inheritor of the security problems being faced by all the technologies that drive its creation.

The first inference that was drawn out by the existing research was to limit the research to the fact that it is outside the scope of this research to actually address all the security issues being faced by the cloud at large. The rating mechanism thus would have security solutions as one criterion which is to be subdivided into many other criteria's based on the service under question and the threats it faces.

The second conclusion made from the existing research was that the research community mainly has focused itself on finding solutions to secure the cloud and has not given a due insight into the fact upon how to garner the support of the non IT consumers of the cloud who generally are a large chunk of consumers. The research's focused mainly on providing solutions to security threats and just a few of them actually focused on providing a mechanism to inculcate the idea of increasing the trust, informed storage, transparency.

Data Security was found to be the prima facia of many researches although almost all of them spoke about how there is a lack of trust between the providers and the consumers, how there is an increasing worry amongst the governments upon how the data of their citizens is to be used while stored on foreign land and how the user themselves feel that the whole process of data storage is least transparent.

The definition of data security in context of this research can be given as data security refers to the fact that the consumers data is secure and remains in the same form while it is stored, transferred over and the access of the data of the user is only restricted to the privileged user and not even to the ones who have the highest possible privileges at the provider side.

The definition of Transparency in context of this research can be given as the approach by the cloud provider to make the consumer aware of all possible facts that he needs to know about the services being used in simplest possible manner and to also state the consequences clearly in case of any possible breach by the user or any outsider into the cloud data.

The definition of informed storage can be derived as the criteria that enable the cloud consumer to know the geo graphical proximity of his data that is being stored on the cloud and also refers to the fact that consent is taken of the consumer before moving his data from one location to another.

The definition of trust is simple yet very important Trust refers to the amount of confidence the customer shares with the services being provided by the cloud provider and to what extent does he feel safe while using the possible services. Looking from the consumer's point of view as pointed out by Divyakant and Kumbharana (2015) have stressed upon the point that security in the SAAS layer is of utmost importance for the growth of cloud reiterating the point first made. They have very well summarised the security practices that should be used for the SAAS layer such as security architecture design, security management and governance, secure SDLC, policies, standards and guidelines, risk management and assessment, Security awareness and training, data privacy, data security, application security and data governance.

The authors very succinctly describe all the current requirements of security that are of prime importance for the user. They however have not been successful in supporting their research by material proof or statistical proof.

Having a look into the service level agreements of various cloud providers such as amazon, Microsoft etc. one can come to a fair conclusion that data storage, processing is solely done based upon how the provider wants it to be

without any interference from the client. The other issues such as problem management, responsibilities and liabilities of both the parties, warranties, security issues are almost rarely discussed and even if they are discussed they contribute towards only one aspect and interest i.e. the interest of the provider.

Many researchers such as the likes of Rong et al. (2013), Dwivedi et al. (2013) have given various insights into problems being faced by the cloud such as multi- tenancy, system monitoring and logs, resource location, authentication, trust of acquired information and cloud standards. The likes of Hashizume et al. (2013), Kumar et al. (2013) have stated that virtualisation, storage and networks are the primary points of concern for security in the cloud environment, whereas Chikkara (2013) has said that transparency, responsibility, assurance and remediation are primary concerns of cloud security.

The conclusion drafted out is that the areas of security concern are very vast and the problem specific solutions are even broader. Thereby the general aspects of security are to be taken into consideration such as authentication, authorization, Trust, Data Backup and restore, Data Integrity, Data Recovery, Data Safety while storage etc.
From the review of Service level Agreements the qualities on which the systems are to be rated would be drafted as Consumer concerned SLA, Clarity, Simple and understandable, Consumer Trust, Transparency, Informed Storage, Uptime, Down Time, Disaster recovery mechanisms etc.

While going through the legal aspects and turmoil's faced by cloud computing one interesting point that came forward was in regards with the issue of legal liability many countries like that of China and DPRK have seen to it that the data of their citizens is retained within their geographical limit and do not allow it to be stored or transferred anywhere else, the policies have been formulated in such a way that even cloud computing is to be done within the country and data centres and other infrastructure present in the country only is to be used, this however is one extreme of policy making where the provider is burdened and is restricted.

On the other hand there is a moderate policy formed by the European Union where the data is to be stored within the member nations and not anywhere outside that, what can be inferred from this is that the government of other countries could sign an official treaty with one another so that if a breach of data of a consumer of country A occurs and the data is stored in the country B still the provider could be held liable in the jurisdiction of Country A.

Critical infrastructure industries such as banks, healthcare, governmental agencies also are a bit afraid of the cloud and do not tend to use the service for sensitive information. If a safer environment is made and better policies formulated then there would be enormous realization of the potentials of cloud computing and concepts such as e governance could really come into picture even for economically backward nations.

The research resulted in the concept of extradition treaties that allow a criminal from one nation to be transferred to another. There have been debates in the United Nations general assembly to mark E- criminals for proceedings via the international criminal court in cases of extreme damage done to a nation. The research would aim at formulating a solution along these lines and also make propositions for future directives required for a complete and detailed solution. Ethical responsibility, adherence to local and international laws, inline security measures and deployment of least vulnerable systems are also the factors on which the rating system will be based.

Another rating criterion of primary importance is the seriousness of the cloud provider towards the research and development of security measures for the technologies being deployed in his cloud service being provided and the awareness amongst the employees about current security trends and issues. These are of primary importance as this would quantify the amount of time and resources the company is spending upon the development of solutions to existing problems. This criterion will also show the amount of awareness the company and its employees have about the current security trends and issues being faced.

The last criteria are the interest shown by the provider to educate its customers about the latest security practices for the consumer to make computing environment even safer.

EXISTING SOLUTIONS

The researches have focused their research on making cloud computing environment a neutral one , a solution proposed by Lombardi, Pietro (2012) called advanced cloud protection system, this system is able to observe both the middleware and guest integrity and could possibly prevent the user from many attacks. The interesting feature is that the system is transparent to the user and doesn't interfere with his activities. The system perform well when applied locally however there has been no details given as to how they expect the system to be globally accepted and also how platform independent the system would be. The researchers have concentrated only upon making an upgraded version of intrusion detection firewall and have not addressed basic issues of cloud security such as that of data security while transmission and storage and also have not addressed the issues of improving trust and transparency amongst users of the cloud.

Zissis and Lekkas (2012) have proposed trusted third party system to ensure necessary trust level and preserve confidentiality, integrity and authenticity.

The authors state that the introduction of the third party would help reduce the loss of traditional security boundaries by producing trusted security domains. The TTP is responsible to conduct and review all critical transactions ad communications between the parties on the basis of ease of creating fraudulent content. The basic idea of the authors is to establish a certification authority that would ensure that the integrity of transactions is maintained, the other issues addressed is the use of single sign on being used along with the PKI thereby improving authentication, and authorization process.

The trusted third party can be relied upon for server and client authentication, low and high level confidentiality, separation of data, certificate based authorization and creation of security domains. The research finely advocates thee use of PKI and SSO by moulding it into a third party, this solves the problems of authentication, authorization and till a certain level increases trust, but the authors fail to address the issues of informed storage and do not rightly prove how this system would bring back security domains and hand over the control of data to the user, the authors concentrate on providing solution for IAAS customers and to an extent for the PAAS customers who have a say in policy making but do not cater to the emerging needs of the largest base SAAS.

Some researchers such as Mathew (2012) argue that a secure cloud based environment can be achieved only when security solutions have been proposed for each and every issue and all are in tandem with each other. The authors argue that secure VPN would ensure a secured environment which every client has to go through to reach the desired cloud provider, the framework proposed by the authors makes use of this technique and propose that the provider check the authentication of the user and also check whether the clients are genuine and authorised. The technique which should be used to do so is not made mention of by the authors. Moreover the issues pertaining to authentication and authorisation are very vast in nature and cannot be addressed using this approach.

The approach of anonymous authentication and authorization is made use of as a protocol by Khalid et al. (2013), they employ a public key certificate with normal strong authentication and XAMCL servers. By doing so their protocol ensures complete anonymity and prevents identity theft by employing anonymous identities. They have deployed their framework with more than one certification authority to make it more platforms independent and widely acceptable, their solution given if combined with identity management systems could very well provide anonymity as a cloud service.

In the field of cloud storage security authors like A. Kumar et al. (2013) have proposed a methodology that exploits the elliptic curve cryptographic encryption technique to preserve data, the suggested model is made up of two parts included private data section and shared data section, they have done so to attain storage and secure reach of data. The technique specified is successful in safeguarding the data stored on cloud and they have also run tests to check whether the solution works against such as denial of service, cross virtual machine, malicious insider etc. the tests conducted were however based on local database of attacks created and the method still needs to be tested for applicability on a larger scale against attacks for which it has not been tested.

RESEARCH GAPS

There is no second thought in the fact that there is a growing urge amongst the research community to identify and address the issues of security in the cloud. Security issue driven research is being done by the community in large volumes and possible solutions are also being put forward.

Research in the field of service level agreements and governmental policies has not been tapped by the research community, the community has talked about the service level agreements of various companies and what is missing about it but has not been able to propose a probable solution that could guide the formulation of service level agreements in simplest possible manner.

The legal aspect of the cloud has also not been taken into consideration by the community while providing solutions towards the development of a safer cloud computing environment. While one might argue that the proposition of solutions to tackle security threats in the cloud are a way in which the legality can be addressed and will ensure that the trust of governments would increase. Legal propositions of the cloud can be addressed by using international bodies such as the United Nations and also by urging countries to sign a memorandum of understanding to extradite and prosecute companies and users under different laws.

The research community has focused its research upon presenting solutions to security issues of the cloud, the problem here is that almost every researcher recognises the fact that the issues hindering the growth of cloud are trust, transparency, informed storage and lack of knowledge about cloud technologies amongst the users still almost none of them try to focus their research upon carving a solution out for these problems.

The community focuses mainly upon a practical solution driven research of a small practical problem but doesn't work to create a framework that would drive research in the cloud community in various directions. Majority of the researchers base their research from a provider's point of view and do not take into consideration views of the consumer community and the government. There is an emerging need for research to be done keeping the consumer perspective in mind as majority of the problems faced by the cloud are from the consumer's perspective and not from the provider's perspective.

Proposed Solution:

In order to deploy a constructive research in the field of cloud computing we propose the use of a universal consumer friendly security based cloud services rating system. This solution would propose a framework for cloud services to be rated upon various parameters so as to make the companies strive harder to achieve the higher rating as it would bolster their image in front of the consumer and would also develop a competitive atmosphere in the field of cloud services.

Motivation:

The motivation for this solution came from the fact that the electronic industry has come up with the same sort of rating mechanism for electrical appliances, the rating mechanism used by the industry is based on the electricity consumption, and this has made the industry a much more competitive and had made them to develop appliances that consume less electricity to get more ratings, thereby helping them to garner more customers for highly efficient appliances.

This rating method has also made it easy for the customers to judge between the products. This has made the customers much more aware and reliant upon the method of rating making it easy for them to understand the issues of an electrical appliance which are of prime importance leaving out the other unnecessary requirements.

This method has also been applied to water appliances even to show the consumption of water by the appliance and the lesser the consumption the more rating is given to it. This rating system has been made mandatory by the governments of various countries such as Australia, India, China, and United States etc.

The same method can be applied to cloud services and as such a big industry was able to comply with such a system in such a less period of time, it shows that proper efforts and a well-designed framework will help the cloud services to also be rated in the same manner.

The prime players in the formulation and deployment of this method will be the governments and the cloud providers. The government will be responsible for framing policies to govern the rating mechanism, take user and provider interests into account while doing so and also for overlooking the proper implementation of the mechanism by the providers.

The provider will be responsible for maintaining the practices of providing service in accordance with the guidelines issued by the government, making its policies in accordance with the rating mechanism and will also be responsible for proposing changes in the mechanism while being formulated and in the future.

The provider and the government will both be responsible to make the rating mechanism available to the general community at large, making the mechanism understandable and easy for the public to use, make the mechanism in compliance with user expectations and making the mechanism a household name and integrate it into the life's of the user in a way that it becomes a part and parcel of their life.

SOLUTION FRAMEWORK

The framework of the proposed solution of rating system will be based on marking the services being provided by the cloud provided o criteria's relating to data security, transparency, trust and informed storage. The solution will mainly focus upon catering the needs of the largest group of cloud consumers i.e. the users of SAAS services. This solution will also have impact on the other services provided up in the IAAS and PAAS layers, which will be gradually effected in appositive manner from this framework.

The rating system will take the following criteria's into consideration while marking a cloud service being provided:
Authentication mechanisms will play a primary role in determining the amount of initial security being provided by the cloud provider to the user, this criteria will be marked by the government based upon what techniques are being used by the provider and how safe and secure these techniques are when compared to the current techniques being used in the cloud community. A score of 5 is given to a provider who uses highly regarded authentication mechanisms to authenticate the users on the cloud.

Authorization controls is another important criteria of initial data security and immunity provided to the user by the cloud service provider, it is of utmost importance that the rating mechanism incorporates this criteria as many of the researchers have pointed out that weak authentication and authorization mechanism are the most probable loopholes for almost every attack. The cloud provider will be rated upon the types of controls being applied for proper authorization of the user and if the controls applied are in tandem with the latest control measures then the rating given would be 5.
Data Backup and restore will be another important factor in the rating system this factor aims at checking the capability of the provider to efficiently back up data of the user and also the efficiency of the provider to recover the data in a situation of manmade or natural crisis.

One of the important factors checked here would be the providers willingness to take the consent of the user prior to any relocation and backup of data being done and also the willingness of the provider to provide remuneration to the users in case of a manmade disaster such as a security breach to the user. The provider will be rated upon these criteria by checking the RAID level of data redundancy applied by it for backing up and restoring data. The frequency of back up provided depending upon the activity cycle of the user will also be taken into consideration, i.e. if there is a company using cloud services then it would like its data to be automatically backed up almost at a very high frequency that might sometimes be a day or even hours in fast paced companies.

Data Integrity refers to the feature of preserving data in the format in which it was last accessed by the user while it is being stored, transferred or even if it is accidentally deleted, integrity means that data should not be tampered with at any cost whatsoever the situation might be, the rating will be given based on how well the provider is able to protect the integrity of data, this would include rating based upon the mechanisms being applied by the provider and if they are in line with latest techniques then provider will be given a rating of 5.

Data safety while storage is another important criteria on which a provider will be rated based upon the capability of the provider to secure store data and also upon his capability to deny access to unauthorised users, another apex measure would be the criteria where in the provider himself employs mechanisms which do not allow his own employees even with highest privilege even to interpret the information, meaning the data should be stored in cryptographic from thereby creating a control domain for the user. This criteria is important as this is one of the most concerning issue for both companies and general users as they do not trust the provider with more sensitive data. If the provider employs exquisite techniques to ensure the safety of data while storage then it would be given a higher rating, the best practice currently being used will be given a rating of 5.

Data safety while transmission is another important issue to be addressed while rating a cloud provider, this however is also a very complex one due to the fact that it is not completely in the hands of the provider to ensure the safety of data while transmission as cloud computing uses the internet to provide service to its users and internet in itself has many complex issues when it comes to data safety. However in this rating mechanism the cloud provider will be rated upon the techniques that he employs in his control circle to protect the data transmission and also upon the ways in which he tries to make the data transmission in the safest possible manner by use of techniques such as cryptography and firewalls.

Identity and access control management this is an important issue as cloud services are generally provided in parallel to many users and this is an important quality of the cloud. The fact that the changes made by a single user doesn't affect the other user using the same service has made cloud highly multi tenable. This however comes with a disadvantage or as we can simply put it an issue which is that how well the provider is able to create separation boundaries and is able to provide access to multiple user of the same service, another issue is that a user is allowed to access multiple services in the cloud and thus a log in for every service being used if required will make the cloud service heavy to use for the users, due to this the concept of single sign on is used which allows users to access various services by signing in just once. The rating criteria here would be how well the identity and access control policies are framed by the company and how much they are in compliance with the best practices of the day. Higher the ability of the provider to address the issue of identity and access control management the higher the rating would be.

In line approach towards security is used as a criteria to rate the cloud service being provided, the issues discussed till now are just a little part of the security problems faced by the cloud community, but the ones mentioned above are common almost to any cloud service provided, this criteria is included in the rating mechanism as it is very well understood that there are many more security threats to the cloud such as denial of service, out-dated accounts etc. that vary from service to service and cannot be categorised easily if done so then this would make the research very prolonged and it will not be just to rate providers of one service who may not face such attacks for their service to be marked upon it as a criteria.

This criteria is very critical and is to be subdivided into various threats faced by a service based upon the current knowledge of attacks present in the industry, it is upon the government and the expertise hired by them to categorise various attacks and their protection mechanism so that a service could be checked as to whether it is in line with the best practises present in the industry.

Informed Storage refers to the feature of the cloud where the user knows the approximate geographical location of his data. The feature of cloud is that it combines various data centres into one and gives the users the functionality of being able to perform various operations on the computing capacity provided. The fact is that the data centre might almost all the time not be present in the country of the user and the user's data will be stored at a datacentre elsewhere outside his geographical proximity. This criteria rates the cloud provider based on his interest in telling the user the geographical proximity of where his data is being stored, thereby gaining his trust.

Data Centre Selection is another criteria which can be told to be a continuation of the previous criteria of informed storage, this means that the cloud provider gives the user a choice of datacentres where in his data could be stored and also that the user ids given the choice to select the datacentre where his data is to backed up. This facility is currently being provided by only amazon web services, amazon gives this option to its users and thereby along with its service this has played a major role in increasing its customer base. This step when taken by amazon was very well received from the users and they were all very happy to hear that at least a step has been taken in the direction of giving the user the ability and control of his data back. This can be seen as a ray of hope and the urge even among the providers to try and provide customers with what they want so as to make the efficient use of technology both by the user and the company.

Ethical responsibility is a very wide term with various implications n cloud security, as the customer puts his complete trust within the provider for the handling of his data, it now becomes the responsibility of the provider to see to it that the data is only used for purposes intended and consented by the user, there have been many theories stating that the data stored in the cloud is being used by the providers to improve upon business and make intelligent advertising by keeping a track of the users activities etc. this should only be done by the provider if at all he has a prior consent of the consumer. Furthermore the data when stored on foreign soil might give the access of the data to the government of the country, this has to be made clear to the user about how the local laws of the country where data is being stored will affect his data and also prior consent is to be taken if any government asks for data of a user except in the cases of national threats to sovereignty.

The consumer is very much interested in seeing the cloud provider being rated on criteria's which make the data of the consumer safe from every possible aspect. Legal liability of the cloud provider and the user is another major criteria upon which a service is to be rated, often in service level agreements the provider tries to hush away from accepting any sort of legal liability due to which the trust of the consumer keeps on diminishing, the very fact that the service level agreements are so large in size that often it is very tough for the customer to read through each and every statement made, it would be very wrong on the part of the government to not help its citizens in this part. With almost everyone from every walk of life having access to the internet, it is not fair to expect the person with the least knowledge about the laws to understand the terms and conditions, it is on the government to take this responsibility and rate the provider on this aspect so that the citizens can rely upon.

Legal adherence to local laws this criteria is of primary importance, the cloud provider is to be rated upon the adherence of the local privacy laws and legal barriers of the consumer/ users country even if the data is not being stored at the users homeland, this sounds a bit confusing and impossible to achieve but with due course of action taken by both government and the provider it is quite achievable. Many more steps have to be taken in this direction such as the one taken by the European union, it is a collaboration of 22 countries and they have passed the law stating that the data of their citizens is to be stored in the geographical reach of the European union itself and the cloud providers have happily complied with them as it also gives them the freedom to choose from 22 nations and they are not restricted to store data within a particular nation. The primary take away from this is that if countries step forward and sign memorandum of understanding amongst each other then this solution is quite achievable.

Transparency is defined as the willingness of the cloud provider to be able to inform the consumer of every possible action being taken by the provider which involves the user and his data or resources, in a way that is clear and is understandable by even thee least knowledgeable user of the service. Least Vulnerable systems is used as a criteria to analyse the extent to which the company is up to date with the best practices of hardware and software, this is important because the more the company upgrades to latest version of both hardware and software, the less are the chances of it being vulnerable to threats. Disinterest of the companies to upgrade can lead to a catastrophe as was in the case of the vulnerability of heart bleed, even after an updated version was released till date there are companies that have not patched their SSL. A governmental tap on this will ensure that the companies are inline and willing to move towards a better growth environment.

The other criteria's to rate the cloud provider based on the service level agreement can be the extent to which a Service level agreement is consumer friendly which means that the extent to which the service level agreement is easy to understand, simple, short and to the point. This is an important criteria as when the service level agreements for different categories of users is made on a different scale it would help the company broader its spectrum of customers and will also improve the consumer provider trust.

The criteria's of performance of cloud provider should also be taken into account while rating their service one of these criteria's is the response time, response time is defined as the amount of time taken by the cloud service to respond to a request made under normal operational conditions. The lower the response time the faster the service is , however while considering the response time the rating should also be based upon the response time of the service under heavy operational conditions or peak times as this will be a total assessment of the service being provided.

Up time also is regarded as an important performance criteria for cloud services, uptime is described as the total amount of time the service is made available to the user without any interruptions, the higher the uptime the more reliable the service is said to be. Thereby this criterion has to be taken into consideration while rating services of cloud providers.

Down Time is defined to be the total time the service is unavailable to the user either due to a planned outage or due to an unplanned condition, this has to be taken into account as a performance metric and services should be rated on these criteria as well. The higher the downtime, the lesser the ratings. There should be serious repercussion's placed on the company if it is not able to meet the specified performance measurement criteria's as stated in its service level agreement.

The last aspect of rating the company would be based upon the awareness and willingness of the company to contribute towards development of a safer computing space for its users, this part involves the criteria of up to date security policy, policy making is a very important aspect for assuring the security of a company, its employees and also the customers. Out-dated policies generally put both the company and its users at great risk. It is thereby important for the government to rate the cloud service providers on this criteria.

The other criteria to rate the cloud provider in terms of awareness and willingness to secure computing will be the amount of workforce and capital being put in by the company in order to research and develop new techniques to make cyberspace a better ad safe place.

The willingness of the company to educate its clients in a simple and subtle way about secure practices while accessing their services is also to be considered as an important criteria as this is one of the major loopholes in security "an ill-informed user", this will not completely or overwhelmingly reduce the number of attacks or make the system less vulnerable but it will gradually help educate the people about various cyber warfare's being used and will help them learn how to deal with them significantly reducing the probability of being a victim to a known attack.

The last criteria will be the willingness of the company to train and teach its employees about the latest security trends and mechanism in market thereby making them even technologically aware and ever ready to face threats from the outside world.

STRUCTURE OF THE RATING SYSTEM

The rating system would be comprised of three bodies one representing the government, the other representing a consortium of software cloud service providers, the last being a representative body of cloud consumers. The governmental body would comprise of legal department, Information technological experts, and experts of foreign relationship and policy managers. The team from the government will be responsible for rating the cloud service providers on the above mentioned criteria's and also to discuss and come to a consensus with the consortium of industries. The governmental body after formulating the rating mechanism is also responsible for opening it to comments from the general public and make any appropriate changes if required.

The consortium of software companies would effectively comprise of corporate bodies that represent the information technology industry and education sector in the respective country. If for example in Australia if rating mechanism is to be implemented then groups such as the Australian information industry association, The Australian Computer society and other eminent heads of multi-national cloud services companies will be a part of this group. The major responsibility of this group will be to represent the cloud provider community at large and their interests, they will be responsible to propose the terms and conditions of what they would like the rating system to be in front of the government and then the two parties are to come to a consensus upon what is to be done and taken into account.
The representative body of cloud consumers could essentially comprise of organisations that represent the majority of industries that use cloud services and this can also include the general public at large by asking them for their inputs via online surveys and feedbacks.

The rules of rating and the detailed process

The rating of the services will be done by the governmental body after the formulation of the detailed rating mechanism, some suggestions as to the validity and the process of rating can be as follows:

The rating mechanism is subject to change annually, this is because of the fact that there is a lot of instability in the information technology community and this field is growing at a very fast pace. The rating mechanism is to be made anonyms i.e. the member body rating the service should not be given access to details that would hint at the name or the status of the company thereby reducing any chances of partiality. The panel heads of expertise is to be selected by the respective parliaments and the co members are to be selected on a rotational basis, based on their experience and proven expertise in the field of operation.

The provider is to submit a report demonstrating the various mechanism deployed in just brief and it is not a compulsion to go into details. A practical inspection is to be run by the governmental body where so ever possible and possible test runs have to be done by the technical expertise. The legal experts and the policy makers are to have a keen look upon the service level agreements presented and also take the responsibility of urging the government to carve ways where in data and services can be legally received from other sister countries. These are just a small number of suggestions made and it is upon the expertise of the panel and the industry to mould this prototype into a universally approachable one.

Supporting Research Conducted:

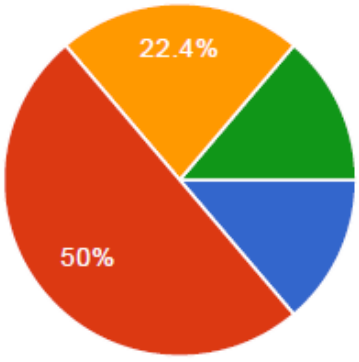
In order to test the proposed solution interviews were carried out over the internet and also a notable number of members of the information technology community were met to give their insights about the proposed solutions.
The survey conducted has a response from 60 people who were carefully picked and were analysed, the reason for doing so was that to ensure that people for all walks of life are involved in the survey. The survey had responses from countries like Australia, India, The United States of America, China, Saudi Arabia etc.

The survey saw the responses coming from people of various fields such as IT, Medicine, Accounting, Law, Engineering, and Teaching and even from students of college in their 12th grade.

The responses received were made to be one per person by making signing in compulsory before being able to fill out the form, this way the survey was made to have the criteria that there are no repetitions of results.

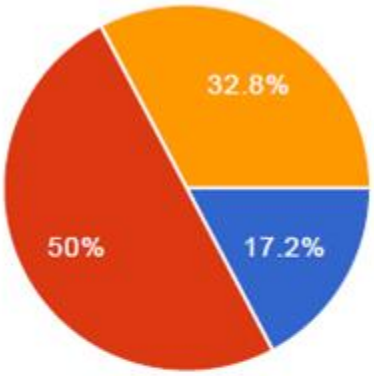
The reason for the survey to be conducted was to see how the people will react in regards with the cloud security issues and what they feel is the biggest threat to the cloud, it was also conducted to check how much people rely upon cloud computing services and what they think about the current solution being proposed.

The following is the summary of responses that were carefully shortlisted, please do note that responses received from school children were not taken into account.



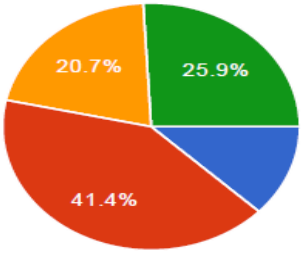
Completely	8	13.8%
Moderate	29	50%
Not very much	13	22.4%
Not at All	8	13.8%

Fig. 1: Result for the question of the trust the consumer has on cloud based services.



Completely understand	10	17.2%
partially understand	29	50%
don't really know what is being talked about	19	32.8%

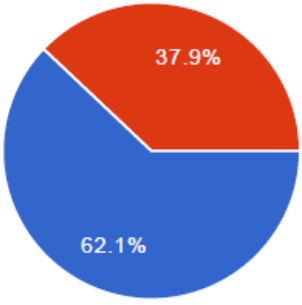
Fig. 2: Response summary of the question asked whether the user understands the terms and conditions put forward by the cloud provider.



Completely	7	12.1%
Moderately	24	41.4%
Not at all for extremely important information	12	20.7%
to an extent to store less relevant information	15	25.9%

Fig. 3: Response pie of the reliance of user upon cloud based services such as storage etc.

Would you like to choose the geographical position where you information is being stored.



Yes	36	62.1%
No	22	37.9%

Fig. 4: Response pie of the question on being able to select geographical location of the data storage.

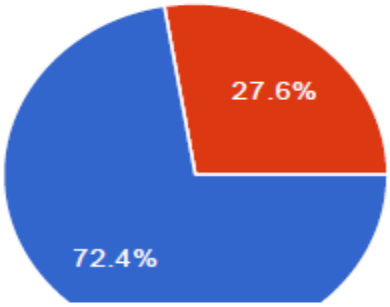
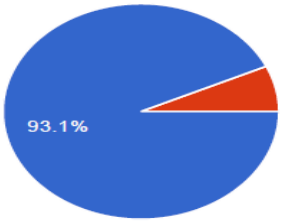


Fig. 5: Response pie of the question would you like the government to interfere and form policies to protect your data.

yes	58	100%
no	0	0%

Fig. 6: Response pie of the question asked whether the user would like to know the measures being taken by the company to safeguard his data.

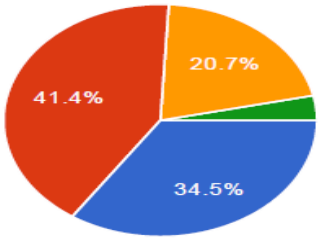
Do you want cloud service providers to be rated on security, trust and transparency just like government issues energy and water ratings to various electrical appliances.



yes	54	93.1%
no	4	6.9%

Fig. 7: Response on whether the user would like to see the cloud service being rated.

How effective you think the rating would be to attract more customers towards the cloud.



Very Effective	20	34.5%
Effective	24	41.4%
Cant Say	12	20.7%
Least Effective	2	3.4%

Fig. 8: Response pie on how effective the user thinks the rating system would be.

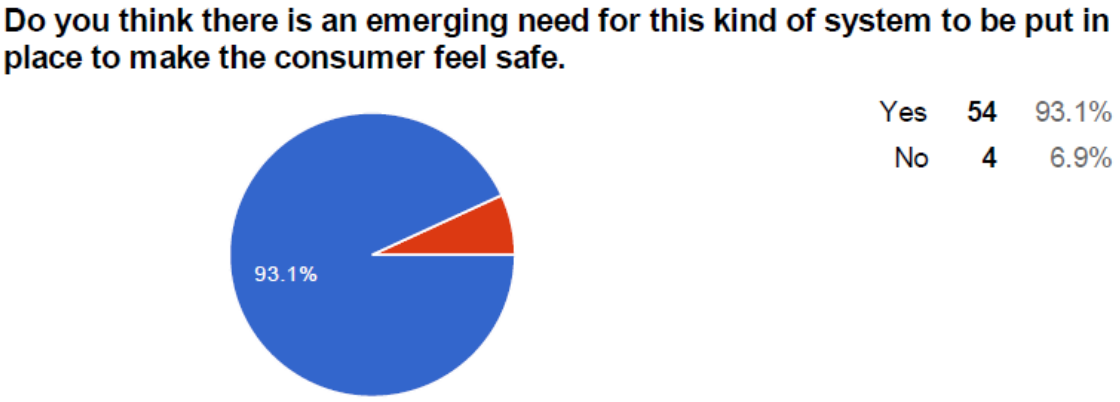


Fig. 9: Response pie on if there is emerging need for this system to be brought into effect.

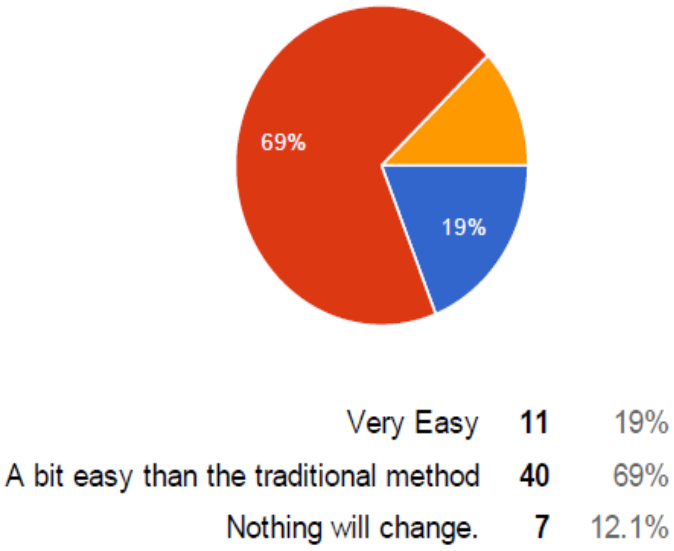


Fig. 10: Response pie on how the user thinks the rating system will help in choosing cloud services.

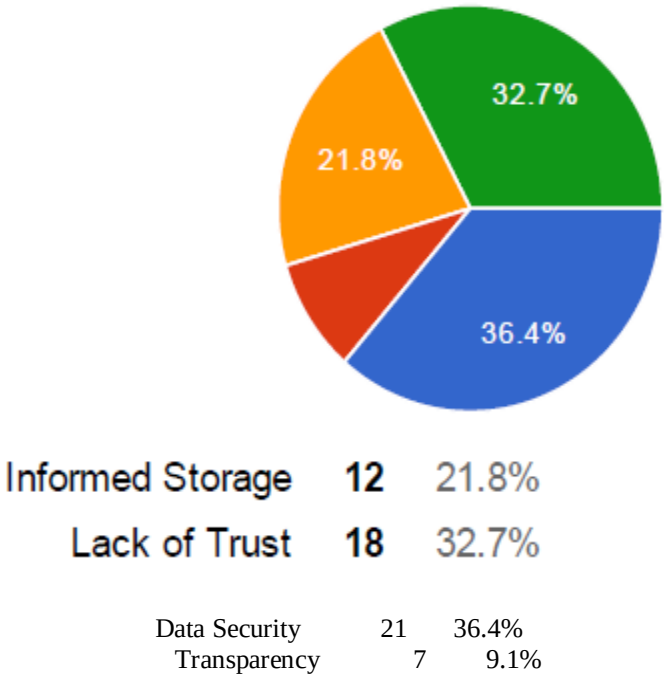


Fig. 11: Response pie of what is the biggest threat that is hindering the growth of cloud computing.

As it can be seen from the responses of the survey there is an emerging need for such kind of system to be put into place so that the trust of the consumer is regained and cloud flourishes leaps and bounds. What's interesting is that almost everyone not related to the field of information technology wanted this system in place, and also majority of personnel from the IT field also were in support of the system.

The Survey is an indication of the current mood of the consumer and how much he puts his trust in the cloud service provider and how much he thinks his data is safe with a third party. The interesting response came from one to one interview that was conducted with company personnel. Cloud service providers such as Infosys, Aramco (K.S.A) were interviewed over Skype, cloud consumers such as Asset link, Citywide, Metro wide, Bank Of America and Ask4Tech were interviewed the last two were on Skype while the others were face to face.

The responses from the cloud providers was that the solution would be possible to execute only after a rigorous effort is made from the governments side and from the company's side, they were also worried about how much time it will take to form a consensus amongst the two parties on how they are to be rated. The framework proposed was appreciated and on a personal note they both thought that the solution will work if more research is put into its development. The personnel questioned here were Mr Khalid Bin Abdul, CIO, Aramco, Kingdom of Saudi Arabia and Ms. Tahera, Regional Manager, Infosys, South India region.

The response from the consumer companies was interesting and the common point amongst them was the iteration of the fact that they do not trust cloud services with sensitive information of their companies and keep it with themselves under their guidance and protection. When asked about the solution proposed all of them agreed that this would definitely increase the consumer trust in the cloud services and they were also equivocal about the fact that this might lead towards a much safer cloud computing environment. The personnel contacted were Mr Irfan M Ahsan, Data Manager, Bank of America, Hyderabad. Ms. Catherine, Business development Manager, Citywide, Melbourne. Mr Clyde Harding, Regional Manager, Vic and Tas, Asset Links.

CRITICAL EVALUATION AND COMPARISON OF THE SOLUTION

The current proposed solution incorporates the views of all the three major participants in the growth of the cloud, the cloud provider, the cloud consumer (corporate) and the cloud consumer (general).

When compared to other frameworks proposed towards the security of the cloud, this framework is a much broader one and tries to incorporate all the various aspects of cloud security and concerns.

The solution proposed is in a very beginning stage and needs to be extraneously developed by expertise from all aspects of information technology and communication technology. The solution incorporates the need of merging various people who do not belong to the field of information technology to generate a workable solution to an information technology problem.

The proposed solution is almost one of a kind one in the current field of research, the researchers till date have advocate only for a third party to govern the transactions between the user and provider but this solution has made the third party even more trustworthy for both the user and the provider by making it the government. The government's role is an important one and needs to be emphasized properly, this research projects the important role what a government can play in the successful implementation of this solution.

The survey methodology used in the research had a very short sample size, but still this sample size was used to just establish the fact that there is a need amongst the people for a solution of this calibre and approach.

LIMITATIONS OF THE SOLUTION

The solution is in a very nascent stage and is just a prototype or a framework. The implications of this solution will definitely vary from country to country as the laws of different countries are different and the definition of data privacy and privacy laws also vary to a large extent.

The same company or provider can get a different rating from this prototype in two different countries and it completely depends on the way at which the country and its panel of experts look at the scenario of cloud computing and the issues of security.

The solution and its success amongst the masses depends upon how much serious the government and the industry is in promoting this idea among the masses and it is highly possible that developed countries would actually very easily embrace this method when compared to developing and under developed ones. The success of the solution also depends upon the way in which the United Nations looks at the cyber criminals and whether or not resolutions are passed by the Security Council to prosecute cyber criminals who have caused extensive damage in terms of loss of data

to a nation while hailing from another one. The more the number of sister nations or friendly nations a country has the more is the probability of the industrial community agreeing to this solution. If a country wants it data to be stored only on its sovereign soil then still this solution can be carried out but will create a hostile investment environment for the software industry. The way in which the solution or rating criteria will be framed might not unanimous and the reason behind this will be that the perception and seriousness of the countries government about the solution proposed.

Future Directives

The author acknowledges the fact that there is a lot of more research that has to be put in to achieve a successful and safe atmosphere for cloud based computing. The fact of the hour is that there is a diminishing or marginal amount of trust within the people with respect to cloud based services which is hindering or blocking the growth of the cloud extensively.

The research community has to acknowledge the fact that the only way to make the cloud a better and secure place is not by solving security issues of the cloud from a technical perspective rather it would be achieved only when the community takes an extra step to collaborate with various stakeholders from various walks of life to develop a solution. Cloud is a heterogeneous cluster of technologies and this is what makes it complex and solutions to its problem even more difficult, there has to be a continual effort made from the governments, research institutes and IT industries to continually fund and direct constructive research in this direction.

Immense amount of concentration is to be done by the research community to blend the user requirements in their proposed solutions, also there has to be a whole hearted initiative from the various countries to bring to justice cyber criminals even when present on foreign soil. Countries like Australia, United States of America, and Great Britain all have laws that deter their citizens from trying activities of cybercrime even on services of other countries and they take a notable step to bring the criminals to justice. There are however a large number of countries that have a very loosely coupled law against cybercrime.

There is also an enormous gap between the international extradition and tracing of cyber criminals and international laws framed by the United Nations also have to be revised, this is being done on a serious note from the past 3 years and more has to be done to achieve what is required. The countries and its governments are required to sign as many memorandums of understanding with their sister nations so as to help the cloud become a safer space by increasing collaboration against cybercrimes and deterring cyber criminals.

ACKNOWLEDGEMENTS

The author acknowledges the efforts and time put in by all the participants in filling out the survey form. The author acknowledges the time and efforts put in by the representatives of various companies and thank them for providing time from their busy schedules. The author finally acknowledges the immense amount of effort put in by my Guide and mentors Professor JemalAbwajy; it is all due to his guidance that this research was done.

BIBLIOGRAPHY

[1]. Chhikara, S. (2013): Analysing Security Solutions in Cloud Computing. International Journal Of Computer Application. 68(25).17– 21.
[2]. Hashizume, K., Rosado, D. G., Fernándezmedina, E., & Fernandez, E. B, 2013, An analysis of security issues for cloud computing, Journal Of Internet Services And Applications, 4(1), 5. Doi: 10.1186/1869-0238- 4-5.
[3]. KHALID, U., GHAFOOR, A., IRUM, M., & SHIBLI, M. A. (2013): Cloud Based Secure and Privacy Enhanced Authentication & Authorization Protocol. Procedia Computer Science, 22, 680–688. doi:10.1016/j.procs.2013.09.149.
[4]. Kumar, S., Pal, S., Kumar, A., & Ali, J. (2013): Virtualization, The Great Thing And Issues In Cloud Computing. International Journal Of Current Engineering And Technology. 338–341.
[5]. Lombardi, F., & Di Pietro, R. (2011): Secure Virtualization For Cloud Computing. Journal Of Network And Computer Applications, 34(4), 1113–1122. Doi:10.1016/J.Jnca.2010.06.008.
[6]. Dwivedi, S.K, Kushwaha, D.S, Maurya, A . (2013): Security Issues And Resource Planning In Cloud Computing. International Journal Of Engineering And Computer Science, 2(2).
[7]. Mathew, A. (2012): Security and Privacy Issues of Cloud Storage Systems . University Of British Coloumbia, 2(4).
[8]. Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013): Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 39(1), 47–54. doi:10.1016/j.compeleceng.2012.04.015
[9]. Zissis, D., & Lekkas, D. (2012): Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583– 592. doi:10.1016/j.future.2010.12.006.
[10]. Prof. Divyakant Meva. Dr. C. K. Kumbharana. (2015): Issues and Challenges of Security in Cloud Computing Environment, International Journal Of Advanced Networking Application.