International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 5, May-2014, pp: (413-421), Impact Factor: 1.252, Available online at: www.erpublications.com.

Data Vulnerabilities in the Saas Service Layer with Emphasis on Privacy, Trust and Informed Storage

Salman Hussain
Masters of Information Technology, Department of Information Technology, Deakin University

Abstract: The use of cloud computing is ever increasing because of its economical and operational benefits. But, one of the major issues hindering the growth of the cloud is its potential security issues. The data vulnerability in the SAAS layer of the cloud has been of primary concern and has created a fear amongst customers about privacy, trust and informed storage in the cloud and is resulting a decline in its popularity along with inefficient usage.
This paper would explain the importance of securing user privacy, gaining trust and providing informed data storage to the user in the cloud and subsequently would go on to propose a methodology of developing a standardised set of rules which would govern and regularise the service provided by cloud providers.

1. INTRODUCTION

Information technology has seen a huge rise in the past two decades, everything has become dependent upon the internet and computing devices. More and more bussinesses , schools , colleges, universities around the world are becoming extremly dependent on the information sector. The number of devices connected to internet has already surpassed the population of the whole world and this demand doesn't seem to come to an end . The increasing demand in the availabilty of computing is mostly attributed to the amount of data being streamed over the internet and the ease of device access being provided. With the development of smart operating systems like android, IOS etc computing has been made more easy and has connected billions of users to the human network. The trends in the internet network shows how rapidly the world is moving towards a second information revolution. It has been estimated that by 2020, 50 billion devices will be connected to the Internet(cisco.com,2013).This takes us to a question which has to be answered at the earliest.

"Are we ready to handle such huge amount of data, are we ready to generate the supporting hardware , the software for all the 50 billion devices which we are going to use in the future?"

Practicaly speaking this would burden us with a huge cost of manufacturing equipments seperately for the needs of every indivisual, the answer that researchers have come up with to tackle this situation is CLOUD COMPUTING.

Problem statement:
Cloud computing comes with its shares of problems one of the most important being the lack of service providers to guarantee the user:

- Privacy of user data.
- Informed storage of the data.

This has resulted in lack of user's trust in the concept of cloud computing. These three problems in cloud have resulted in stagnation in its growth and have to be answered so as to regain the user trust. Although many attempts have been made to secure user interests in the field of cloud computing by researchers nobody has been able to clearly address the problem of privacy, trust and informed storage.

A solution to this problem should comprise of the interests of following stakeholders:

- Cloud provider
- Customers
- Governments and international laws on privacy

Motivation of research:

Clouds are the answer that the world has towards a sustainable future of information technology. Many attempts are being made to draw a consensus and reach towards a solution to curb the data vulnerabilities in the cloud. Researchers have attributed SAAS as the most vulnerable layer of the cloud and have also tried answering data vulnerabilities in the SAAS layer. Many of the researchers have also concluded that privacy, trust and informed storage are the factors which are restricting users from being an active part of the cloud. The conclusion thereby derived is that the main block in the path of securing cloud computing is the reason that there has been no single standard set of regulations to govern the quality of service which is to be provided by the cloud providers to the customers.

Importance of the research:

If a common set of protocols is developed by keeping in mind the requirements of all the three major stakeholders of cloud computing i.e. cloud provider, customers and the governments which would rate the service being provided by the cloud providers keeping in mind various factors such as level of privacy, informed storage, user authentication etc. on a scale of one to five where increased number would mean increased quality of service then this would lead to a substantial regularization in the field of cloud computing and would help increasing the mutual trust among cloud providers , customers and governments. This establishment of the protocol would thereby lead to increased level of informed storage and privacy by interpreting the rating given to service being provided.

The solution to be presented in the further part of the research would basically aim at giving an unbiased rating to cloud service providers based upon the factors such as level of security being provided, Privacy being maintained , handling of data ,importance given to the user , level of informed storage being provided etc. These ratings would enable the user to be sure of while investing into a cloud provider's service i.e. if the rating of the cloud provider is high user will be assured of quality service and security of his data. These ratings would also encourage healthy competition amongst cloud providers and would streamline the competition in a direction wherein the user satisfaction would be the utter most priority.

RELATED WORK

With the majority of the users getting added to the cloud being the users of the SAAS layer i.e. do not know much about security measures taken and are mostly exploited in terms of data confidentiality, privacy, trust and security. It is thereby becoming an increasing concern to secure personal information of subscribers of the SAAS layer of the cloud. The data vulnerabilities experienced in SAAS layer of cloud computing can be tabled down as follows (Subashini, S & Kavitha, 2011):

a) Data can be co-located with the data of unknown owners (competitors, or intruders) with a weak separation
b) Data may be located in different regions which have different laws
c) Incomplete data deletion – data cannot be completely removed
d) Data backup done by untrusted third-party providers
e) Information about the location of the data usually is unavailable or not disclosed to users
f) Data is often stored, processed, and transferred in clear plain text

Fig: Data Vulnerabilities in cloud computing

The issues of extreme concern at the stage of SAAS layer in terms of security are the location of data in different places; incomplete data deletion; no disclosure of information storage to customer and the lack of transparency. These are the concerns of a common man and there have been cases where in hackers have been able to hack into servers of IT giants like IBM and Microsoft. So the minimum security requirement for a customer to effectively come on to the cloud is the development of trust between cloud provider and the customer which can only be achieved if problems of data location , informed storage , complete deletion etc. can be solved. Many researchers have stated that data security issues such as privacy and trust mechanisms have not been answered time and over again. The article by (Chen & Zhao 2012) raises some

very good questions regarding problems that have been unresolved such as key management, data integrity, Data destruction, the authors state that issues such as weak identification policies, lack of key management protocols, incomplete data deletion etc. are of prime importance and need to be resolved so as to have a bright future for the cloud. The authors focus mainly upon lack of key management protocols and try to propose homomorphic keys as a solution to curb data security. The authors finally state that there is still a lot of research to be done in the field of securing user privacy and gaining user trust.

Authors in the like (Rong, Nguyen et al. 2013) have been advocating the establishment and need for a common standard for cloud services and have been talking talk about the standardization of Service level agreements along with accountability in the cloud so as to improve the trust criteria of a cloud user. Many authors such as (Cheung, Sun et al. 2013) explain how sensitive amount of data is being collected and is being breached without the knowledge of the owner by cloud providers thereby causing loss of trust. The article by chueng is divided into three parts namely privacy enhanced technology, trust and reputation, applications in cloud computing where he primarily focuses upon growing lack of trust and reputation among customer with regards to services being provided by the cloud providers. There are various existing international standards which guide the best practice for cloud providers in security area such as ISO/IEC 27001 and 27002 are being used by service providers to gain trust of cloud customers to an extent. But, these standards are still far from being able to cover the full complexity of the issue at hand. The requirements of these standards are generic and do not take user privacy as primary point of focus. Moreover, these standards are generic and do not consider the type, size and nature of the organization. The existing standards fail to address specific issues such as privacy, trust and informed storage and also do not involve the requirements of all the stakeholders in their standards. Privacy, trust and informed storage have been the primary focus points for many of the researchers because of the reason that it is due to these three issues that cloud is losing a lot of reputation and is facing a lot of problem. Many countries such as that of the European Union have taken actions against cloud providers to secure the interest of their citizens who are active on the cloud and have restricted providers to not violate the privacy and information security law concerning the data of their citizens. They have also gone to an extent of limiting the cloud providers to store the data of their citizens in their own country and nowhere else. In conclusion majority of the researchers have agreed that a solution to be proposed should comprise of a common standard set of rules which would govern the service being provided by the cloud providers.

PROPOSED SOLUTION

Research Questions

The main research question which has to be answered so as to structure the research and come to a consensus is:
What are the factors that have to be taken into consideration while designing a standard set of rules for cloud services?
Furthermore to simplify the research the question can be sub divided as:

- What all areas have to be taken into consideration while designing a solution?
- Service level agreements of which cloud providers are to be taken into consideration while forming a base study.
- What customer level should be interviewed so as to know the customer requirements?
- What all survey questions are to be included in the survey?
- What all international laws are to be kept in mind while designing the standard?
- Data protection laws of which countries are to be studied and summarised while forming the solution.

The solution:

This paper aims at proposing a standard set of rules that would set rating criteria for cloud services being provided. The ratings would be based upon factors such as security mechanisms being used, privacy of user data, level of transparency, informed storage and authentication mechanisms being applied. These ratings would enable users to be sure of what quality of service they are being provided by the service provider and this would even help increase a healthy competition amongst cloud providers to deliver quality service to its users which will thereby increase the overall mutual trust between provider and the customer.

Methodology

Step 1:

The research would begin with doing a qualitative study of the service level agreements of all major cloud service providing companies. The data so collected will be summarised and a common consensus of similarities between companies is jotted down alongside with the major differences.
A draft of the common service agreement is to be made such that all the cloud providers agree to it to an extent of at least 80%.

Step 2:

The next step in the research would involve creating a survey questionnaire for major cloud customer in all the leading countries in information technology. A list of top 10 customers of cloud service providers would be made and a detailed questionnaire would be made which would ask them to include their expectations, fears, thoughts on the standard solution and the future advances that they would like to see in the arena of cloud services. The data collected by this step would be analysed thoroughly and a detailed point wise report of people agreeing to the thought of a standard solution would be made. The data then would be subjected to quantitative analysis and percentage of customers agreeing to a specification will be made. This would give a detailed report of customer expectations.

Step3:

Finally the international and national laws in respect to privacy and data security are to be studied to complete the view of all stakeholders and all aspects influencing the privacy, trust and transparency in cloud services.
The data collected from these three steps would be collaborated and a draft set of rules would be made which would incorporate a consensus between all three stakeholders of the cloud service arena.

Step4:

The data drafted would set the basic precedent for generating the rating criteria which would include the following factors:

- Security mechanisms
- User privacy
- Authentication mechanisms
- Level of transparency
- Compliance with international and national laws of privacy and secrecy

These factors would then be used to rate the cloud providers. The maximum compliance of the provider with the above factors would mean that the rating of the provider is more and the least compliance would mean that the rating of the provider is less. The rating would be calculated as follows: Each of the factors would be rated on a scale of 1 to 10 and then the average of all the factors is taken out. After the average is known then it is converted to a scale of 5 and the answer obtained would be the rating

For example let us assume a cloud provider got the following ratings for the factors considered:

- Security mechanisms- 7/10
- User privacy- 6/10
- Authentication mechanisms – 7/10
- Level of transparency – 5/10
- Compliance with international and national laws of privacy and secrecy 5/10

Then rating would be calculated as(7+6+7+5+5)/5= 6

Then this average is converted to the scale of 5 which results in the rating being 3/5 for the provider.

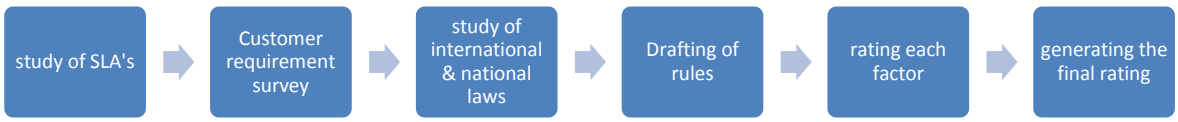
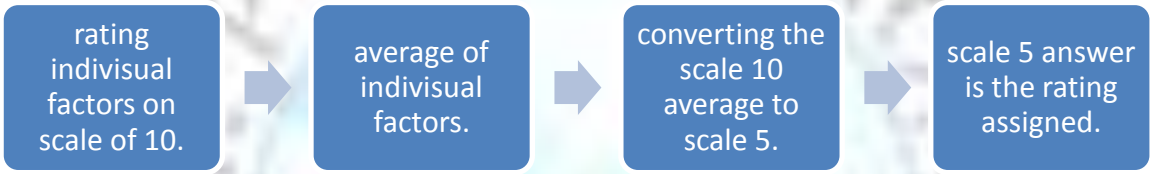


Fig: Flow diagram of the solution.

The solution would be a recursive process for each company to be rated and would take into account the company's service level agreements and the national privacy laws of the country where the company is located. Taking this into account the company would be rated upon the earlier stated factors.

The process of calculating the rating can be represented as follows:



Potential Outcomes and Limitations

This research would yield a standardised version of rules which would rate and govern the level of service provided by cloud service providers. This set of rules would benefit both the customer and the cloud provider in the long run by increasing the trust of the customer in the cloud service thereby by increasing the number of customers using cloud services to the maximum extent. This would be a path setter for further researches in the field of cloud data security and would potentially narrow the gap between the customer and the provider.

Ethical issues &Limitations:

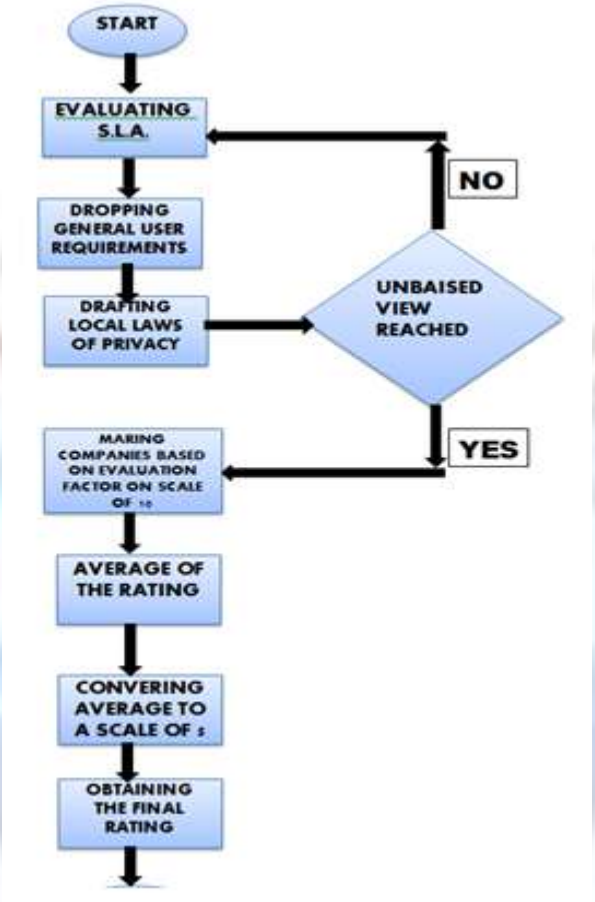
- The research conducted would be done without any kind of ethical bias and accurate data interpretation and analysis will be done.
- Government permissions are required and method is to be accepted by the governments of the host nation of the company to carry out rating of the company.
- These ratings will not apply to the same company operating outside the nation in which it was rated. Different ratings will be done to the same company in operating in different regions keeping local laws in mind.

This research would be a game changer for all the data security issues being faced by the cloud and would enable cloud services to reach heights of success.

EVALUATION CRITERIA

The proposed solution will now be evaluated against existing standards such as ISO 27001 and ISO 27006. The criteria which will be used to showcase the efficiency of the proposed solution over the existing standards will be the scope of the standards at hand and what all they include in their criteria of giving a certification.

Flow Diagram Of The Proposed System:



Drawbacks of ISO 27001&27006:

The problem with the ISO 27001 scope is that the Information Security Management System (ISMS) must have interfaces to the "outside" world i.e. the outside world is not the only client or supplier but even the companies departments that are not defined within the scope are also considered to be an external supplier. This creates an overhead burden for the company to make its departments which are not in the scope sign legal documents of data being transferred by them. For example if only the department of information technology is placed within the scope of the company and this department uses services of other departments to carry out business, then the IT department is to perform a risk assessment of other departments and has to sign a document of terms and conditions between the department for the information being used. This means that IT department must certify that within your scope you are able to handle the information in a secure way, while it cannot be held liable for information being given to other departments and the certification cannot guarantee the security of the data.

This is not where the trouble stops. Sometimes, a narrow scope is simply not possible, because there is no interface with the outside world. For instance, if employees from both within the scope and outside the scope are sitting in the same room, such a scope is hardly feasible; if both the employees within and outside the scope use the same local network (with no segregation) and have the access to various network services, such a scope is definitely not possible – there is no way you

would be able to control the information flow only inside the scope. The standard does not allow the user to be sure of what will happen if the data of the user is used outside the department which is not in the scope thereby reducing the trust between the cloud provider and the cloud customer.

Even when organization have complied with the standard there have been a lot of high profile security breaches in the past few years that brings us to a question

If ISO27001 is so good, why are we still seeing security breaches?

The answer is that the standard is a management standard, not necessarily a security standard. Let's take an example an organisation might decide that its risk appetite is high risk. Thereby the organization might take an offhand approach and expose itself to a high risk but still complying with the standard. In practice I don't think that is what is happening. I think most organisations have a problem defining what their information security management system (ISMS) should protect, what risks they face and how they mitigate those risks, through the use of controls or other techniques. That means that a significant number of organisations are not properly protected from a security point of view. If either your risk assessment or your controls are fundamentally flawed then you are at risk of a breach occurring. There are many reasons why businesses are not adequately involved, committed, and effectively contributing to IS:

- Basic professional IS concepts are difficult, complicated and strange to practical business people.
- Organizational overall IS performance depends on many detailed aspects in a complicated way.
- IS is a multidisciplinary issue and difficult to cope with simple managerial practices. E.g. it is very difficult to get effective links between business-managerial and technical solutions of the IS.
- Communication between business leaders and IS (and other related) experts is ineffective and uncreative in general and within organizations.
- Business leaders are very busy, subjective, authoritative, and holistic generalists and very different from IS experts.
- External third party audits and certifications undermine business leaders' active responsibility.
- Business information is greatly based on tacit (implicit) knowledge, and management of the security of tacit knowledge is a sophisticated issue.

The current certification process appears to be a desktop exercise. That is it might be an appropriate approach to certification and is a very cost effective approach. On the other side it means that the certification process provides certification against the standard, but limited assurance over the overall risk and control framework. These standards even fail to actively engage the criteria for engaging the requirements of stakeholders' i.e. Cloud providers, customers and government laws. This has resulted in lack of interest in all the three stakeholders to believe in the standard when it comes to cloud computing. These standards moreover are not cloud specific and fail to address issues specific with that of cloud computing such as informed storage and customer privacy. Implementation of these standards by cloud providers has done only a little good to the cloud society and has not really answered the questions at hand. The lack of the standards to give a precise scope definition has made them more vulnerable to interpretation by companies who get the certification but fail to actually protect the data as seen in the cases of amazon and Microsoft in the recent past.

POSITIVES OF THE PROPOSED SOLUTION

The current solution actively engages all the three major stakeholders in providing a rating to the cloud provider's quality of service. The proposed solution includes the following factors before rating the provider:

- Requirements of all stakeholders.
- Analysis of actual security policies in place by the provider.
- Involves governmental permission to rate the companies in the country.
- Analysis of compliance with governmental policies of privacy and security.
- Level of transparency being provided is included.
- Authentication mechanisms of the company are evaluated thoroughly.
- Data separation and deletion policies are taken into consideration.

- Compliance of provider with general user requirements such as extent of privacy and secrecy provided is taken into consideration.
- Amount of Risk liability provided is also taken as criteria for rating.

Table: Comparison of solution based on evaluation factors

Evaluation criteria	Proposed solution	Existing solution
Solution exclusively for cloud systems.	Yes	No
Stakeholder requirements.	Complete involvement of all stakeholders' requirements.	Very shallow involvement.
Consideration of local privacy laws.	Yes	No
Evaluation done on case to case basis (different evaluation for same companies in different geographical regions).	Yes	No
Rating based on Company security policies.	Yes	No
Authentication mechanisms considered as a criteria	Yes	No
Full liability of risks as criteria.	Yes	Partially
Data separation and deletion policies	Yes	Partially
Level of transparency between user and provider	Yes	No
Data co location policies	Yes	No
Informed storage to government and customer as criteria.	Yes	No
Informed data relocation	Yes	No

The proposed solution clearly would be the answer to bridge the gap between user and cloud arena. This solution has a maximum probability of acceptance from all three major stakeholders the user, the provider and the government. This solution would effectively increase healthier competition between providers and would also improve the overall cloud quality of service by making it more users centric.

CONCLUSION

This proposed solution would lead cloud towards a bright future and would increase the amount of trust users have in cloud computing. This solution would enable a healthy competition between cloud providers so as to provide quality service to people. The important aspect of this solution to keep in mind the requirements of users, governments and providers so as to agree upon the rating gives a bright indication of this being acceptable easily by all the three stakeholders. The rating criteria of this solution see to it that all aspects with regards to user data protection and secrecy are taken into consideration along with governmental policies this implies that the solution is a fool proof solution and would even help to streamline the on-going research in the subject. This research would also make it easier to answer questions with respect to data vulnerabilities with respect to cloud computing by giving researchers a direction to research with. Cloud computing needs to have a universally acceptable standard set of rules and this solution would set a precedent in formulation of the standard.

REFERENCES

[1]. Subashini, S & Kavitha, V 2011, 'A survey on security issues in service delivery models of cloud computing', Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11.
[2]. Chen, D & Zhao, H 2012, 'Data security and privacy protection issues in cloud computing', in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 1, pp. 647-51.
[3]. Rong, C, Nguyen, ST&Jaatun, MG 2013, 'Beyond lightning: A survey on security challenges in cloud computing', Computers & Electrical Engineering, vol. 39, no. 1, pp. 47-54.
[4]. Cheung, S, Sun, Y, Aberer, K, Haritsa, J, Horne, B & Hwang, K 2013, 'Guest Editorial< newline/> Special Issue on Privacy and Trust Management in Cloud and Distributed Systems', Information Forensics and Security, IEEE Transactions on, vol. 8, no. 6, pp. 835-7.
[5]. CISCO,2013.Internet Of Things[Online],available at:www.cisco.com.
[6]. MICROSOFT Information Security Management System for Microsoft Cloud Infrastructure,
[7]. (2010),http://www.globalfoundationservices.com/security/documents/InformationSecurityMang
[8]. SysforMSCloudInfrastructure.pdf, Accessed in September 2011.
[9]. CLOUD SECURITY ALLIANCE Top Threats to Cloud Computing V1.0,
[10]. http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.
[11]. NIST Risk Management Guide for Information Technology Systems (2002),
[12]. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, Accessed in September 2011.
[13]. AICPA SSAE 16. Accessed in September 2011.
[14]. http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx.
[15]. PCI DSS v2.0. Accessed in September 2011.
[16]. https://www.pcisecuritystandards.org/security_standards/.
[17]. HIPAA https://www.cms.gov/HIPAAGenInfo/. Accessed in September 2011.
[18]. D. CATTEDDU, G. HOGBEN (2009) Cloud computing risk assessment. European Network.
[19]. Whittaker, Z (2011), “Microsoft Admits US PatriotAct Can Access EU Based Cloud Data”, ZDNet 28 June 2011. Online at: http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-accesseu- Based-cloud-data/11225.