Volume 3, No. 1, January 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW PAPER
Available Online at www.jgrcs.info

SECURITY PERSPECTIVE OF CLOUD COMPUTING WITH SURVEY OF SECURITY ISSUES

S.Thirukumaran*[1], M.Sanjay Ram[2] and A.Vijayraj[3]
*[1]Department of MCA, Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India
thirukumaran75@gmail.com
[2] Department of MCA, Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India
sanjayramm@gmail.com
[3]Department of IT, Saveetha Engineering College, Chennai, Tamil Nadu, India
satturvijay@yahoo.com

Abstract: Cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply, whilst reducing capital expenditure. It describes the advance of many existing IT technologies and separates application and information resources from the underlying infrastructure. However the opportunity cost of the successful implementation of Cloud computing is to effectively manage the security in the cloud applications. Security consciousness and concerns arise as soon as one begins to run applications beyond the designated firewall and move closer towards the public domain. Previous work security framework that has limitation of scalability for cloud computing. In this paper is to provide an overall security perspective of Cloud computing with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of Cloud computing. Cloud security issues are used to findings from the International Data Corporation enterprise panel survey based on cloud threats, will be discussed in this paper.

INTRODUCTION

Cloud computing is a new and emerging information technology that changes the way IT architectural solutions are put forward by means of moving towards the theme of virtualization: of data storage, of local networks (infrastructure) as well as software [1][2].The success of modern day technologies highly depends on its effectiveness of the world's norms, its ease of use by end users and most importantly its degree of information security and control. International Data Corporation (IDC) conducted a survey of IT executives and their line-business colleagues to gauge their opinions and understand their companies' use of IT cloud services. Security ranked first as the greatest challenge or issue of cloud computing.

Corporations and individuals are concerned about how security and compliance integrity can be maintained in this new environment. Even more concerning, though, is the corporations that are jumping to cloud computing while being oblivious to the implications of putting critical applications and data in the cloud. Moving critical applications and sensitive data to a public and shared cloud environment is a major concern for corporations that are moving beyond their data centre's network perimeter defence. To alleviate these concerns, a cloud solution provider must ensure that customers can continue to have the same security and privacy controls over their applications and services provide evidence to these customers that their organization and customers are secure and they can meet their service level agreements (SLA) to convince the customer on security issues.

The clouds have different architecture based on the services they provide. The data is stored on to centralized location called data centres having a large size of data storage. The data as well as processing is somewhere on servers. So, the clients have to trust the provider on the availability as well as data security. The SLA is the only legal agreement between the service provider and client. The only means the provider can gain trust of client is through the SLA, so it has to be standardize. In this paper, section two describes the service level agreement, section three explains present SLA's of cloud computing, and section four discusses how to standardize SLA's followed by the proposed data security issues. A service level agreement is a document which defines the relationship between two parties: the provider and the recipient. This is clearly an extremely important item of documentation for both parties. If used properly it should:

a. Identify and define the customer's needs
b. Provide a framework for understanding
c. Simplify complex issues
d. Reduce areas of conflict
e. Encourage dialog in the event of disputes
f. Eliminate unrealistic expectations

In this we proposed to provide an overall security perspective of Cloud computing with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of Cloud computing.

LITRATURE SURVEY

a. The world of computation has changed from centralized (client-server not web-based) to distributed systems and now we are getting back to the virtual centralization (Cloud Computing). Location of data and processes makes the difference in the realm of computation. On one hand, an individual has full control on data and processes in his/her computer. On the other hand, we have the cloud computing wherein, the service and data maintenance is provided by some vendor which leaves the client/customer unaware of

where the processes are running or where the data is stored. So, logically speaking, the client has no control over it. The cloud computing uses the internet as the communication media. In this approach in this paper, we put forward some security issues that have to be included in SLA are have slow process.

b. The Cloud computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure (CapEx) and operational expenditure (OpEx). In order for this to become reality, however, there are still some challenges to be solved. Amongst these are security and trust issues, since the user's data has to be released to the cloud and thus leaves the protection sphere of the data owner. Most of the discussions on this topic are mainly driven by arguments related to organizational means. This paper focuses on technical security issues arising from the usage of Cloud services and especially by the underlying technologies used to build these cross-domain Internet-connected collaborations. In this approach cloud computing offers less operation.

c. Cloud computing is an emerging paradigm for large scale infrastructures. It has the advantage of reducing cost by sharing computing and storage resources, combined with an on-demand provisioning mechanism relying on a pay-per-use business model. These new features have a direct impact on the budgeting of IT budgeting but also affect traditional security, trust and privacy mechanisms. Many of these mechanisms are no longer adequate, but need to be rethought to fit this new paradigm. In this paper we assess how security, trust and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed in this approach used for business models.

d. This paper aims to present a model for malware detection, uCLAVS (University of Caldas' AntiVirus Service), a multiple engine service that follows the set of defined protocols and standards for Web Services technologies; in addition Ontology for Malware and Intrusion Detection is described. uCLAVS is based on the idea that the files analysis commonly carried by applications residing on the client can improve their performance if they are moved to the network, where instead of running complex software on every host, it gives each process a receiving the light entering the system files, send them to the network to be analyzed by multiple engines, and then to decide whether or not they are executed according to the report of threat delivered. As a result of the tests with the prototype can be uCLAVS arguing, among other things, that offers the possibility of increasing the rate of the assertion characterization harmful files, allows the construction of thin clients, facilitates zero-day updates, and provides a forensic capabilities enhancement.

e. Cloud computing is an evolving term these days. It describes the advance of many existing IT technologies and separates application and information resources from the underlying infrastructure. Personal Cloud is the hybrid deployment model that is combined private cloud and public cloud. By and large, cloud orchestration does not exist today. Current cloud service is provided by web browser or host installed application directly. According to the ITU-T draft, we might consider cloud orchestration environment in collaboration with other cloud providers. Previous work proposed security framework that has limitation of scalability for cloud orchestration. In this paper, we analyze security threats and requirements for previous researches and propose service model and security framework which include related technology for implementation and are possible to provide resource mobility.

f. The term "cloud computing" has emerged as a major ICT trend and has been acknowledged by respected industry survey organizations as a key technology and market development theme for the industry and ICT users in 2010. However, one of the major challenges that face the cloud computing concept and its global acceptance is how to secure and protect the data and processes that are the property of the user. The security of the cloud computing environment is a new research area requiring further development by both the academic and industrial research communities. Today, there are many diverse and uncoordinated efforts underway to address security issues in cloud computing and, especially, the identity management issues. This paper introduces architecture for a new approach to necessary "mutual protection" in the cloud computing environment, based upon a concept of mutual trust and the specification of definable profiles in vector matrix form. The architecture aims to achieve better, more generic and flexible authentication, authorization and control, based on a concept of mutuality, within that cloud computing environment.

g. In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is. This paper discusses security issues, requirements and challenges that cloud service providers (CSP) face during cloud engineering. Recommended security standards and management models to address these are suggested for technical and business community.

CLOUD COMPUTING MODULES

Cloud computing types:

Cloud computing have a major decision is to decide on the type of cloud to be implemented. Currently there are three types of cloud deployment models offered, namely, a hybrid, private and public cloud. These, together with their security implications will be discussed below. Within this paper vendors are referred to as cloud providers, or companies specializing in providing a tailor made cloud solution. These entities have established cloud infrastructure including virtual servers for storage matching required

processing power. Organizations are entities, including business managers, executives and end-users, entering into an agreement with cloud vendors to utilize their cloud capabilities for personal and/or private use.

Hybrid Cloud: A hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Clouds provide more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. The cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand. In deciding which type of Cloud to deploy, business managers' needs to holistically assess the security considerations from an enterprise architectural point of view, taking into account the information security differences of each Cloud deployment.

Public Cloud: A public cloud is a model which allows users' access to the cloud via interfaces using mainstream web browsers. It's typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. This helps cloud clients to better match their IT expenditure at an operational level by decreasing its capital expenditure on IT infrastructure. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks. Therefore trust and privacy concerns are rife when dealing with Public clouds with the Cloud SLA at its core. A key management consideration, which needs to be answered within the SLA deals with ensuring that ample security controls are put in place. One option is for both the cloud vendor and client mutually agree in sharing joint responsibility in enforcing cloud checks and validation are performed across their own systems. The alternative option will be for each party to set out individual roles and responsibilities in dealing with cloud computing security within their utilization boundaries.

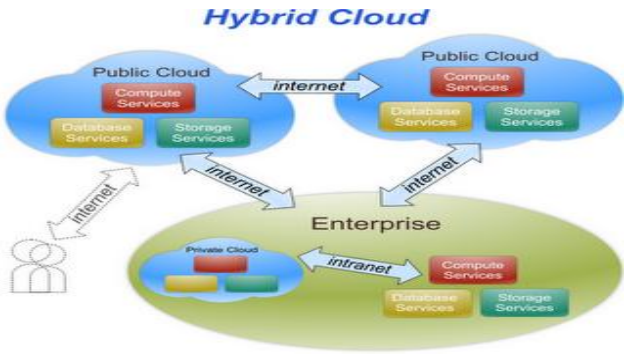

Figure. 1 Cloud Computing Modules

Private Cloud: Private cloud is infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally [8]. It is easier to align with security, compliance, and regulatory requirements, and provides more enterprise control over deployment and use. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific private cloud.

Cloud computing services:

Securing Infrastructure-as-a-Service: This model lets users lease compute, storage, network, and other resources in a virtualized environment. The user doesn't manage or control the underlying cloud infrastructure but has control over the OS, storage, deployed applications, and possibly certain networking components. Amazon's Elastic Compute Cloud (EC2) is a good example of IaaS. At the cloud infrastructure level, CSPs can enforce network security with intrusion-detection systems (IDSs), firewalls, antivirus programs, distributed denial-of-service (DDoS) defenses, and so on.

Securing Platform-as-a-Service: Cloud platforms are built on top of infrastructure service with system integration and virtualization middleware support. Such platforms let users deploy user-built software applications onto the cloud infrastructure using provider-supported programming languages and software tools (such as Java, Python, or .NET). The user doesn't manage the underlying cloud infrastructure.

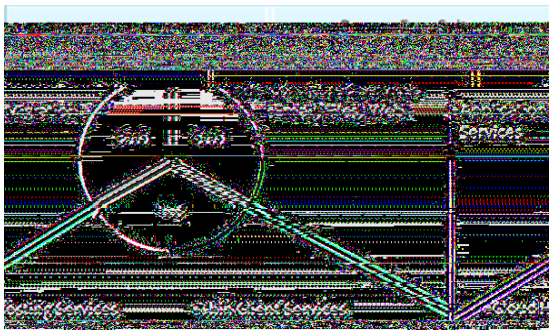

Figure. 2 Cloud Computing Services

Popular platforms include the Google App Engine (GAE) or Microsoft Windows Azure. This level requires securing the provisioned VMs, enforcing security compliance, managing potential risk, and establishing trust among all cloud users and providers.

Securing Software-as-a-Service: This service employs browser-initiated application software to serve thousands of cloud customers, who make no upfront investment in servers or software licensing. From the provider's perspective, costs are rather low compared with conventional application hosting. Software service as heavily pushed by Google, Microsoft, Salesforce.com, and so on — requires that data be protected from loss, distortion, or theft. Transactional security and copyright compliance are designed to protect all intellectual property rights at this level. Data encryption and coloring offer options for upholding data integrity and user privacy.

Security issues:

Cloud computing security issues identified seven issues that need to be addressed before enterprises consider switching to the cloud computing model. They are as follows:

a. ***Privileged user access*** **-** information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water.
b. ***Regulatory compliance*** **-** clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't.
c. ***Data location*** **-** depending on contracts, some clients might never know what country or what jurisdiction their data is located.
d. ***Data segregation*** **-** encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider.
e. ***Recovery*** **-** every provider should have a disaster recovery protocol to protect user data.
f. ***Investigative support*** **-** if a client suspects faulty activity from the provider, it may not have many legal ways pursued an investigation.
g. ***Long-term viability*** **-** refers to the ability to retract a contract and all data if the current provider is bought out by another firm.

Given that not all of the above need to be improved depending on the application at hand, it is still paramount that consensus is reached on the issues regarding standardization.

Cloud governance:

Cloud computing policies and procedures should be put in place in an effort to protect the cloud from potential of threats, hacks and the loss of information. We must understand that it is necessary to design privacy within the Cloud right from the outset. The privacy challenge for software engineers is to design cloud services in such a way so as to decrease privacy risks and to ensure legal compliance. There are threats associated with the data being stored, processed remotely and an increased usage of virtualization and sharing of platforms between users. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties. This lack of control leads to suspicion and ultimately distrust. The protection of data in the cloud is a key consumer concern particularly for committing fraudulent activities and financial exploitation. With governance and security in place, Cloud computing can be used safely and with confidence.

Cloud transparent:

Transparent security would entail cloud providers disclosing adequate information about their security policies, design, and practices, including disclosing relevant security measures in daily operations. Public clouds are more likely to be seen as having a greater degree of transparency as compared to the Hybrid or Private Cloud models. This is due to public cloud vendors having a "standardized" cloud offering thereby targeting a wider client base. Private clouds are usually built for specific organizations having more attention focused on offering customization and personalization cloud functionality. One of the most important protocols in ensuring transparency within Cloud computing is the SLA. The SLA is the only legal agreement between the service provider and client and its importance is greatly discussed in the article titled "Cloud Security Issues". The only means that the cloud provider can gain the trust of clients is through the SLA; therefore the SLA has to be standardized.

Impact cloud computing security:

As computer manufacturers, employers and universities deploy cloud based tools on desktops, many users may fail to realize that they are in fact using an Internet based service. This risk of confusion will likely increase when cloud based applications lack any recognizable browser branding, and continue to function when the user is not connected to the Internet. The use of HTTPS together with WS Security should be a bare minimum when logging on to access data using Cloud computing. But providing a HTTPS encrypted connection takes significantly more processing power and memory for a Web server to provide than a normal web connection. WS-Security assists with SOAP messages by defining the header that carries the WS-Security extensions. Additionally, it defines how existing XML security standards like XML Signature and XML Encryption are applied to SOAP messages. Thus far there has been four service failures identified between Amazon and Google in 2008, ranging from 1.5 to 8 hours downtime. Organizations must decide whether proper security measures are in place (to secure their data and applications) or do they share a joint responsibility with service providers when engaging in the cloud environment.

The shift to Cloud computing moved much of a user's normal activity to the Web browser. Web browsers generally store all of a user's saved passwords, browsing history and other sensitive information in a single place. As such it is possible for malicious websites to exploit browser vulnerabilities in order to steal information associated with other existing or previous browsing sessions, such as a logged in email account or online banking session. It is for this reason that some security experts recommend that consumers use one web browser for general surfing, and another for more sensitive tasks, such as online banking. Often, usernames and passwords are transmitted to remote servers via unencrypted network connections. In cases where encryption is used, it is typically only used to transmit the initial login information, while all other subsequent data is sent in the clear. This data can easily be snooped on by hackers.

This exposes users to significant risks when they connect to the services using public wireless networks to any Cloud Service. In the book titled "The Tower and the Cloud", Richard Katz focuses on many areas where the cloud may impinge on education. He advocates that because companies might be storing documents which should not be made public, there are reasons for concern about what can happen to the information. Potential Cloud organizations and vendors need to be aware that it may become easier for

attackers to threaten clouds by moving towards a single cloud interface.

Users desire a cloud software environment that provides many useful tools for building cloud applications over large datasets. Let's look at some security and privacy features these users desire:

a. Cloud resources they can access with security protocols such as HTTPS or Secure Sockets Layer (SSL), as well as security auditing and compliance checking;

b. Fine-grained access control to protect data integrity and deter intruders or hackers, as well as single sign-on or sign-off;

c. Shared datasets that are protected from malicious alteration, deletion, or copyright violations;

d. A method to prevent ISPs or CSPs from invading user privacy;

e. CSPs that fight against spyware and Web bugs; and

f. Personal firewalls and shared datasets protected from Java, JavaScript, and ActiveX Applets, as well as established VPN channels between resource sites and cloud clients.

We can enhance some of these features with cloud reputation systems and more efficient identity management systems, which we discuss in subsequent sections.

CONCLUSION

Cloud providers need to safeguard the privacy and security of personal data that they hold on behalf of organizations and users. In particular, it is essential for the adoption of public cloud systems that consumers and citizens are reassured that privacy and security is not compromised. Responsible management of personal data is a central part of creating the trust that underpins adoption of cloud based services – without trust, customers will be reluctant to use cloud-based services. Privacy protection builds trust between service providers and users: accountability and privacy by design provide mechanisms to achieve the desired end effects and create this trust. This management can span a number of type: hybrid, private and public.

The advantages of cloud computing – its ability to scale rapidly (through subcontractors), store data remotely (in unknown places), and share services in a dynamic environment can become disadvantages in maintaining a level of assurance sufficient to sustain confidence in potential customers.
In this paper key security considerations and challenges which are currently faced in the Cloud computing industry are highlighted. While current offerings explore trail-and error control methods, a great deal of investment must be made in the managing security around this evolving technology. The Cloud Security Alliance is one such organization. It is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud computing, and provide education on the uses of Cloud computing to help secure all other forms of computing. By following guiding principles discussed in this paper, a great deal of insecurities may be easily expelled, saving business owners' valuable time and investment. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution and future work and progress lies in standardizing Cloud computing security protocols.

REFERENCES

[1] Balachandra Reddy Kandukuri, Ramakrishna Paturi V,and Dr. Atanu Rakshit 'Cloud Security Issues', vol.3, pp.517-520, 2009.

[2] Meiko Jensen, J¨org Schwenk, and Nils Gruschka, Luigi Lo Iacono'On Technical Security Issues in Cloud Computing', vol.3, pp.109-116, 2009.

[3] Siani Pearson and Azzedine Benameur 'Privacy, Security and Trust Issues Arising from Cloud Computing', vol.32, pp. 693-702, 2010.

[4] Cristian Adrián Martínez, Gustavo Isaza Echeverri, and Andrés G.Castillo Sanz 'Malware Detection based on Cloud Computing integrating Intrusion Ontology representation', vol.35, pp.101-106, 2010.

[5] Sang-Ho Na, Jun-Young Park, and Eui-Nam Huh 'Personal Cloud Computing Security Framework', vol.48, pp.671-675, 2010.

[6] Aiiad Albeshri, and William Caelli 'Mutual Protection in a Cloud Computing Environment', vol.44, pp.641-646, 2010,

[7] Kresimir Popovic, and Zeljko Hocenski 'Cloud computing security issues and challenges', vol.46, pp.344-349, 2010.

[8] "The NIST Definition of Cloud Computing (Draft)". National Institute of Science and Technology. Retrieved 24 July 2011.

[9] Michael Miller, "Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online", Pearson Education, August 2008.

[10] Haley Beard, "Cloud Computing Best Practices for Managing and Measuring Processes for On-demand Computing, Applications and Data Centers in the Cloud with SLAs", Emereo Pty Limited, July 2008.

[11] Michael Miller, "Cloud Computing", Pearson Education, New Delhi, 2009.

Short BioData for the Author

S.Thirukumaran is an Assistant Professor in Department of Computer Applications at Adhiyamaan college of Engineering, Hosur, He received his Master of Computer Applications in Madras University in 2000 and he is continuing his research in Data Mining in Anna University of Technology Coimbatore. He has published two papers in International Journals under mining concept and his area of interest is Data Mining Content Retrieval and Cloud Computing.

Sanjay Ram M is an Assistant Professor in Department of Computer Applications at Adhiyamaan College of Engineering, Hosur. He received his Master of Computer Applications in Annamalai University in 2000. He has 11 years of teaching experience from various Engineering Colleges. He is a Member of CSI. He has Published 1 International Journal and 7 papers in National and International Conferences. His area of interest includes Cloud Computing, Network Security, Operating Systems

A.Vijayaraj is an Associate Professor in Department of Information Technology at Saveetha Engineering College. He received his Master of Computer Application in Bharathidhasan University, in 1997 and his Master of Engineering in Computer Science and Engineering from Sathyabama University at 2005. He has 12 years of teaching experience from various Engineering Colleges during tenure he was Awarded **Best Teacher Award** twice. He is a Member of, CSI and ISTE. He has Published 2 papers in International journal and 11 Papers in International and 10 National Level conferences. His area of interest includes Operating Systems, Data Structures, Networks and Communication.