International Journal For Research In Advanced Computer Science And Engineering
ISSN: 2208-2107

Analysis of Different Security Issues in Cloud Computing

Namita Jhende[1], Raghvendra Kumar[2], Naazish Rahim Khan[3]
[12,3]Dept. of Computer Science & Engineering, LNCT Group of College, Jabalpur, MP, India
jhendenamita@gmail.com, raghvendraagrawal7@gmail.com, naazish.rahim786@gmail.com

Abstract: Cloud computing is envisioned as the next generation technology. Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. In a cloud computing environment, the entire data resides over a set of networked resources, enabling the data to be accessed through virtual machines. Since these data-centers may be located in any part of the world beyond the reach and control of users, there are multifarious security and privacy challenges that need to be understood and addressed. There are a number of algorithms and methodologies available for achieving data security in cloud computing. In this paper we look at the current researches related to data security issues like integrity, Reliability and Confidentiality. in this particulars we will discuss how to secure client's data on remote cloud Servers.
Keywords: Reliability, Integrity, confidentiality, Trusted Storage. Software as a Service (SAAS), Platform as a Service (PAAS), Infrastructure as a Service (IAAS).

1. **Introduction**

Cloud computing [1] [2] is not an innovation per se, but a means to constructing IT services that use advanced computational power and improved storage capabilities. The main focus of cloud computing from the provider's view as extraneous hardware connected to support downtime on any device in the network, without a change in the users' perspective. Also, the users' software image should be easily transferable from one cloud to another. Balding proposes that a layering mechanism should occur between the front-end software, middle-ware networking and back-end servers and storage, so that each part can be designed, implemented, tested and ran independent from subsequent layers. This paper introduces the current state of cloud computing, with its development challenges, academia and industry research efforts. Further, it describes cloud computing security problems and benefits and showcases a model of secure architecture for cloud computing implementation.

Critics argue that cloud computing is not secure enough because data leaves companies [3] [4] [5] local area networks. It is up to the clients to decide the vendors, depending on how willing they are to implement secure policies and be subject to 3rd party verifications. Sales force, Amazon and Google are currently providing such services, charging clients using an on-demand policy. References statistics that suggest one third of breaches are due to laptops falling in the wrong hands and about 16% due to stolen items by employees. Storing the data in the cloud can prevent these issues altogether. Moreover, vendors can update application/OS/middleware security patches faster because of higher availability of staff and resources. According to cloud vendors, most thefts occur when users with authorized access do not handle data appropriately. Upon a logout from the cloud session, the browser may be configured to delete data automatically and log files on the vendor side indicate which user accessed what data. This approach may be deemed safer that storing data on the client side. There are some applications for which cloud computing is the best option. One example is the New York Times using Amazon's cloud service to generate PDF documents of several-decade old articles. The estimated time for doing the task on the Times' servers was 14years, whereas the cloud provided the answer in one day for a couple hundred dollars. However, the profile of the companies that currently use the cloud technology includes Web 2.0 start-ups that want to minimize material cost, application developers that want to enable their software as a service or enterprises that are exploring the cloud with trivial applications. The fact that cloud computing is not used for all of its

potential is due to a variety of concerns [6] [7] [8]. The following surveys the market in terms of continuous innovation, academia and industry research efforts and cloud computing challenges.

Nevertheless, there numerous ways in which cloud computing can expand on the issue of security. For example, Qualys Guard is a compilation of products that are used to discover network weaknesses. It is used by over 200 companies in Forbes Global 2000, so it acquired significant acceptance in the marketplace. Qualys Guard main idea is to place an appliance behind the firewall that would monitor various security issues. The box encrypts all its data and has no access to client stored data; however, it does contain a back porch by allowing a certain IP address and admin to modify scripts and credentials. In this fashion, it proposes a new type of security to the cloud, so that whenever an attack is made on a certain service, it may be monitored by a 3rd party and cut off before it disrupts proper access or attempts to falsely validate itself to the cloud.

2. Cloud Computing Challenges

Challenges that cloud computing currently faces in being deployed on a large enterprise scale [9] [10]:

1. Self-healing - in case of application/network/data storage failure, there will always be a backup running without major delays, making the resource switch appear seamless to the user.
2. SLA-driven - cloud is administrated by service level agreements that allow several instances of one application to be replicated on multiple servers if need arises; dependent on a priority scheme, the cloud may minimize or shut down a lower level application.
3. Multi-tenancy - the cloud permits multiple clients to use the same hardware at the same time, without them knowing it, possibly causing conflicts of interest among customers.
4. Service-oriented - cloud allows one client to use multiple applications in creating its own.
5. Virtualized - applications are not hardware specific; various programs may run on one machine using virtualization or many machines may run one program.
6. Linearly scalable - cloud should handle an increase in data processing linearly; if "n" times more users need a resource, the time to complete the request with "n" more resources should be roughly the same.
7. Data management - Distribution, Partitioning, Security and Synchronization of data.

3. Cloud Security Challenges [11] [12]

Start-up companies often lack the protection measures to weather off an attack on their servers due to the scarcity of resources - poor programming that explores software vulnerabilities (PHP, JavaScript, etc) open ports to firewalls or inexistent load-balance algorithms susceptible to denial of service attacks. For this reason, new companies are encouraged to pursue cloud computing as the alternative to supporting their own hardware backbone. However cloud computing does not come without its pitfalls. For starters, a cloud is a single point of failure for multiple resources. Even though network carriers such as AT&T believe a distributed cloud structure is the right implementation, it faces major challenges in finding the optimal approach for low power transmission and high network availability [Croll08]; some people believe that major corporations will shy away from implementing cloud solutions in the near future due to ineffective security policies. One problem comes from the fact that different cloud providers have different ways to store data, so creating a distributed cloud implies more challenges to be solved between vendors.

1. Linearly scalable - cloud should handle an increase in data processing linearly; if "n" times more users need a resource, the time to complete the request with "n" more resources should be roughly the same.
2. Data management - distribution, partitioning, security and synchronization of data.

4. Cloud Data Security [13] [14]

Cloud security refers to confidentiality, integrity and availability, which pose major issues for cloud vendors. Confidentiality refers to who stores the encryption keys - data from company A, stored in an encrypted format at company B must be kept secure from employees of B; thus, the client company should own the encryption keys. Integrity refers to the face that no common policies exist for approved data exchanges; the industry has various protocols used to push different software images or jobs. One way to maintain data security on the client side is the use of thin clients that run with as few resources as possible and do not store any user data, so passwords cannot be stolen. The concept seems to be impervious to attacks based on capturing this data. However, companies have implemented systems with unpublished APIs, claiming that it improves security; unfortunately, this can be reversed engineered; also, using DHCP and FTP to perform tasks such as firmware upgrades has long been rendered as insecure. Nevertheless, products from Wyse are marketed with their thin client as one of the safest, by using those exact features.

4.1 Cloud Computing Security Issues [15]

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

1. 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.
2. 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.
3. Data location - depending on contracts, some clients might never know what country or what jurisdiction their data is located.
4. 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.
5. Recovery - every provider should have a disaster recovery protocol to protect user data
6. Investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursued an investigation.
7. 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.

4.2 Security and Privacy [16]

Identity management every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using federation or SSO technology, or a biometric-based identification system, or provide an identity management solution of their own. Cloud ID, for instance, provides a privacy-preserving cloud-based and cross-enterprise biometric identification solution for this problem. It links the confidential information of the users to their biometrics and stores it in an encrypted fashion. Making use of a searchable encryption technique, biometric identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries.

4.2.1. Physical security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

4.2.2. Personnel security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre, Para and post employment activities such as security screening potential recruits, security awareness and training programs, proactive security monitoring and supervision, disciplinary procedures and contractual obligations embedded in employment contracts, service level agreements, codes of conduct, policies etc.

4.2.3. Availability

Cloud providers help ensure that customers can rely on access to their data and applications; at least in part (failures at any point - not just within the cloud service providers' domains - may disrupt the communications chains between users and applications).

4.2.4. Application Security [16]

Cloud providers ensure that applications available as a service via the cloud (SAAS) are secure by specifying, designing, implementing, testing and maintaining appropriate application security measures in the production environment. Note that - as with any commercial software - the controls they implement may not necessarily fully mitigate all the risks they have identified, and that they may not necessarily have identified all the risks that are of concern to customers. Consequently, customers may also need to assure themselves that cloud applications are adequately secured for their specific purposes, including their compliance obligations.

5. Security Benefits

There are definitely plenty of concerns regarding the inability to trust cloud computing due to its security issues. However, cloud computing comes with several benefits that address data security. The following sections looks into addressing concepts such as centralized data, incident response or logging. Centralized Data refers to the approach of placing all eggs in one basket. It might be dangerous to think that if the cloud goes down, so does the service they provide, but at the same time, it is easier to monitor. Storing data in the cloud voids many issues related to losing laptops or flash drives, which has been the most common way of loosing data for large enterprises or government organizations. The laptop would only store a small cache to interface with the thin client, but the authentication is done through the network, in the cloud. In addition to this, when a laptop is known to be stolen, administrators can block its attempted access based on its identifier or MAC address. Moreover, it is easier and cheaper to store data encrypted in the cloud that to perform disk encryption on every piece of hardware or backup tape.

6. Conclusion

Cloud computing is still struggling in its infancy, with positive and negative comments made on its possible implementation for a large-sized enterprise. IT technicians are spearheading the challenge, while academia is bit slower to react. Several groups have recently been formed, such as the Cloud Security Alliance or the Open Cloud Consortium, with the goal of exploring the possibilities offered by cloud computing and to establish a common language among different providers. In this boiling pot, cloud computing is facing several issues in gaining recognition for its merits. Its security deficiencies and benefits need to be carefully weighed before making a decision to implement it.

However, the future looks less cloudy as far as more people being attracted by the topic and pursuing research to improve on its drawbacks.

References

[1].M. Jensen, J. Schwenk, N. Gruschka, And L. Lo Iacono, On Technical Security Issues In Cloud Computing. Ieee, 2009.
[2]. Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, "Cloud Computing", Http://Www.Ibm.Com/Developerswork/Websphere/Zones/Hip Ods/Library.Html, October 2007, Pp. 4-4
[3]G. Frankova, Service Level Agreements: Web Services And Security, Ser. Lecture Notes In Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, Vol. 4607.
[4]. "Service Level Agreement And Master Service Agreement", Http://Www.Softlayer.Com/Sla.Html, Accessed On April 05, 2009.
[5]. S. Berger, R. Caceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, W. Schildhauer, And D. Srinivasan, "Security For The Cloud Infrastrcture: Trusted Virtual Data Center (Tvdc)." [Online]. Available: Www.Kiskeya.Net/Ramon/Work/Pubs/Ibmjrd09.Pdf
[6]. Http://Www.Cloudsecurity.Org, Accessed On April 10, 2009.
[7]. "Sampling Issues We Are Addressing", Http://Cloudsecurityalliance.Org/Issues.Html#15, Accessed On April 09, 2009.
[8]. Mikekavis,"Real Time Transactions In The Cloud", Http://Www.Kavistechnology.Com/ Blog/?P=789, Accessed On April 12, 2009.
[9]. "Secure Group Addresses Cloud Computing Risks", Http://Www.Secpoint.Com/Security-Group-Addresses-Cloudcomputing- Risks.Html, April 25, 2009. [10]. "Service Level Agreement Definition And Contents", Http://Www.Service-Level-Agreement.Net, Accessed On March 10, 2009.
[10] Sun Microsystems, Introduction To Cloud Computing Architecture, 2009
[11] Fellows, W.2008. Partly Cloudy, Blue-Sky Thinking About Cloud Computing. 451 Group.
[12] Varia, J.2009. Cloud Architectures. Amazon Web Services.
[13] Chappell, D.2009. Introducing The Azure Services Platform. David Chappell & Associates.
[14] Rayport, J. F. And Heyward, A.2009. Envisioning The Cloud: The Next Computing Paradigm. Marketspace.
[15] Pastaki Rad, M., Sajedi Badashian, A., Meydanipour, G., Ashurzad Delcheh, M., Alipour, M. And Afzali, H. 2009. A Survey Of Cloud Platforms And Their Future.
[16] Khajeh-Hosseini, A., Sommerville, I. And Sriram, I. "Research Challenges For Enterprise Cloud Computing," (Unpublished).(Submitted To 1st Acm Symposium On Cloud Computing, Indianapolis, Indiana, Usa, June 2010, Under Paper Id 54)