International Journal of Computer Science and Informatics

Volume 3 | Issue 4 Article 14

April 2014

CLOUD COMPUTING APPLICATIONS AND SECURITY ISSUES: AN ANALYTICAL SURVEY

ARATI KOTHARI
Vivekanand Institute of Management, Gulbarga, Karnataka, India, aratikothari@rediffmail.com

CLOUD COMPUTING APPLICATIONS AND SECURITY ISSUES: AN ANALYTICAL SURVEY

ARATI KOTHARI

Vivekanand Institute of Management, Gulbarga, Karnataka, India
Email:aratikothari@rediffmail.com
Cell: +919916366508

Abstract - Cloud computing, a rapidly developing information technology has becoming a well-known the whole world. Cloud computing is Internet-based computing, whereby shared resources, software and information, are provided to computers and devices on-demand, like the electricity grid. Cloud computing is the product of the fusion of traditional computing technology and network technology like grid computing, distributed computing parallel computing and so on. Companies, such as Amazon, Google, Microsoft and so on, accelerate their paces in developing Cloud Computing systems and enhancing their services to provide for a larger amount of users. However, security and privacy issues present a strong barrier for users to adapt into Cloud Computing systems. It is a new technology that satisfies a user's requirement for computing resources like networks, storage, servers, services and applications, without physically acquiring them. It reduces the overhead of the organization of marinating the large system but it has associated risks and threats also which include – security, data leakage, insecure interface and sharing of resources and inside attacks.

Keywords*: Cloud Computing, on demand, pay per use, threats, data leakage, CSP*

1. INTRODUCTION

Cloud Computing has more attention nowadays. The government agencies, enterprises, and more companies started to use Cloud Computing. The next revolution in IT and the big switch in IT is shifting the paradigm of classical computing to cloud environment. In Classical computing buying and owning the system software, hardware, application software to meet the peak needs. The system configuration, testing, verification and evaluation raise the demand of using resources. The cost of using the resource utilization is higher in order to meet the demands. In Cloud computing environment the storage of data and faster evaluation of CPU utilization and provides subscription of the data storage and pay per use of service as per the quality of services. Cloud computing is different from other technological trends but related with grid computing, utility computing and transparent computing. Grid computing is a base form of distributed computing whereby a super and virtual computing composed of clusters of network, loosely coupled computers acts to perform extreme tasks. Utility computing is the packaging of computing resources, such as computation and storage, as a metered service similar to a traditional public utility such as electricity, water, gas and telephone services. Transparent computing is a complex back-end services that are transparent to users which is simple and easy-to use provides front-end interface.

The term *cloud* has been used historically as a metaphor for the Internet. This usage was originally derived from its common depiction in network diagrams as an outline of a cloud, used to represent the transport of data across carrier backbones (which owned the cloud) to an endpoint location on the other side of the cloud. However, since the turn of the millennium, the concept has been revitalized. It was during this time of revitalization that the term *cloud computing* began to emerge in technology circles.

Definition of cloud computing:

- Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications, services etc, that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- Cloud Computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes. Examples of such nodes include end user computers, data centers, and Cloud Services. We term such a network of nodes as a Cloud.
- A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and **virtualized** computers that are **dynamically provisioned** and presented as one or more unified computing resources based on **service-level agreements** established through **negotiation** between the service provider and consumers."- Rajkumar Buyya, University of Melbourne.

The characteristics of a cloud server that includes the following:

- Ease of use-Includes simplified deployment and maintenance and portability.

- Instant availability- provides access to the server via a direct cabling that are connected over the Local Area networks and the internet.
- Subset of functionality
- Privacy in nature- we own our data and control over the data.
- Overall controlling power of software resources.

Cloud Architecture

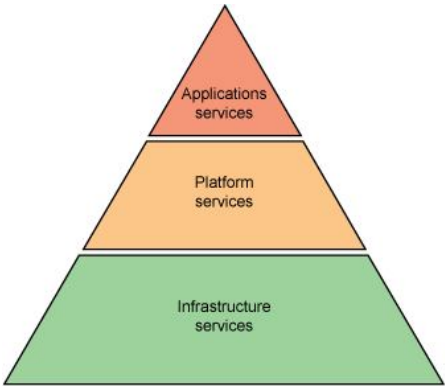

Figure 1: ***Architecture of Cloud***

Architecture

- Application Services (services on demand)
  - Gmail, GoogleCalender
- Platform Services (resources on demand)
  - Google Appengine
- Infrastructure as services (physical assets as services)
  - IBM Blue house, Amazon EC2, Microsoft Azure Platform, Sun Parascale etc.

Multi-tenancy refers to the ability to run multiple customers on a single software instance installed on multiple servers. This is done to increase resource utilization by allowing load balancing among tenants, and to reduce operational complexity and cost in managing the software to deliver the service.

Advantages of Cloud Computing.

Cloud computing offers lots of advantages:

- Cost- As in the clouds the user needs not own the resources, it just needs to pay as per the usage in terns of time, storage and services. This feature educes the cost of owning the infrastructure.
- Performance-the performance is improved because the cloud is not a single computer but a large network of powerful computers resulting in high processing power.
- Freedom from up gradation and maintenance- the cloud infrastructure is maintained and upgraded by the cloud service provider.
- Scalability- The user is can request to increase the resources if the area of application grows or new functionality is added. On the other hand if requirement shrinks the user can request to reduce the resources as well.
- Speedy Implementation- Time of Implementation of cloud for an application may be in days or sometimes in hours. You just need a valid credit card and need to fulfill some online registration formalities.
- Mobility- We don't need to carry our personal computer, because we can access our documents anytime anywhere.
- Increase Storage Capacity- in Cloud computing we have extreme resources for storing data because our storage consists of many bases in the Cloud. Another thing about storing data in the Cloud is that, because of our data in the Cloud can automatically duplicated, they will be more safety.

Disadvantages of Cloud Computing

There are certain security threats and issues of implementing Cloud computing:

- Data Loss-Customers are responsible for the security of their data, thus in any case if data is lost the customer is in deep trouble.
- Account Hijacking-Since No native APIs are used for login and anyone can easily register himself as cloud service user chances of hijacking ones account are very high.
- Control over the process – in cloud computing the user have very less or no control over the services.
- Insider attacks by Cloud Service Provider-It may possible that a fraudulent employee may do the fishing and steal the data.
- Legal aspects-In case of Data loss the user may suffer if there is no Service Level Agreement (SLA), the loss will be of user, because he is not able to put claims against the cloud service provider.

II. SERVICES IN CLOUD

There are three types of cloud providers that you can subscribe to: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These three types differ in the amount of control that you have over your information, and conversely, how much you can expect your provider to do for you. Briefly, here is what you can expect from each type.

1. ***Software as a Service*** - A SaaS provider gives subscribers access to both resources and applications. SaaS makes it unnecessary for you to have a physical copy of software to install on your devices. SaaS also makes it easier to have the same software on all of your devices at once by accessing it on the cloud. In a SaaS agreement, you have the least control over the cloud.

2. ***Platform as a Service*** - A PaaS system goes a level above the Software as a Service setup. A PaaS provider gives subscribers access to the components that they require to develop and operate applications over the internet.
3. ***Infrastructure as a Service*** - An IaaS agreement, as the name states, deals primarily with computational infrastructure. In an IaaS agreement, the subscriber completely outsources the storage and resources, such as hardware and software that they need.

As you go down the list from number one to number three, the subscriber gains more control over what they can do within the space of the cloud. The cloud provider has less control in an IaaS system than with a SaaS agreement.

III. TYPES OF CLOUDS

There are different types of clouds that you can subscribe to depending on your needs. As a home user or small business owner, you will most likely use public cloud services.

1. Public Cloud - A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.
2. Private Cloud - A private cloud is established for a specific group or organization and limits access to just that group.
3. Community Cloud - A community cloud is shared among two or more organizations that have similar cloud requirements.
4. Hybrid Cloud - A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

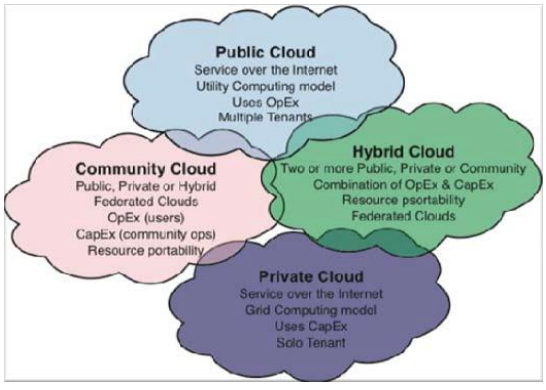

Figure 2: Types of Cloud Computing

IV. CLOUD SECURITY ISSUES

Security issues come under many guises both technical and socio-technical in origin. To cover all the security issues possible within the cloud, and in-depth, would not be possible. Existing efforts look to provide taxonomy over the issues seen. The Cloud Security Alliance is a non-profit organization that seeks to promote the best practices for providing security assurance within the cloud computing landscape. The Cloud Security Alliance identify seven threats to cloud computing that can be interpreted as a classification of security issues found within the cloud. They are:

1. Abuse and Nefarious Use of Cloud Computing

Legitimate CSPs can be abused for nefarious purposes, supporting criminal or other untoward activities towards consumers. The emphasis is that legitimate services are used with malicious intent in mind. Other issues seen include the provision of purposefully insecure services used for data capture. Commonly asked information includes the consumers name, email/postal address, D.O.B or even credit card details. Users are essentially being goaded to part with more information than required as a prerequisite for service use. Malicious entities can then use this information for nefarious purposes, most notably identity theft. Even if the entities are not malicious the disclosure of information to the CSP can also be said to be an abuse of service by the CSP themselves. CSPs may collect this information, or any other information provided at later stages, and markets this information to third parties for data mining purposes. Another security issue found is the provision of legitimate maliciously-oriented services. This service provision also known as (In) Security-as-a-Service, offers users the same security guarantees as existing services yet their use is malicious. By using a cloud based service it is claimed that a process that would take around five plus days now takes on average twenty minutes.

2. Insecure Interfaces and Application Programming Interfaces

Data placed in the Cloud will be accessed through Application Programming Interfaces (APIs) and other interfaces. Malfunctions and errors in the interface software, and also the software used to run the Cloud, can lead to the unwanted exposure of user's data and impugn upon the data's integrity. A HTTP server can allow an attacker to gain complete control over the web server. Data exposure can also occur when a software malfunction affects the access policies governing user's data. This has been seen in several Cloud based services in which a software malfunction resulted in which a users privacy settings shall be overwritten and the user data is exposed to non-authorized entities. Threats can also exist as a result of poorly designed or implemented security measures. If these measures can be bypassed, or are non-existent, the software can be easily abused by malicious entities. Regardless of the threat origin, APIs and other interfaces need to be made secure

against accidental and malicious attempts to circumvent the APIs and their security measures.

3. Malicious Insiders

Although a CSP can be seen as being honest their employees may not be. A malicious insider may be an employee of the CSP who abuses their position for information gain or for other nefarious purposes. Regardless, of the employee's motivation the worrying aspect is that a surreptitious employee will have access to consumer's data for legitimate purposes but will abuse this power for their own means. Another more subtle form of the malicious insider problem is through PaaS based services. If the service provider offers a platform that allows developers the ability to interact with user's data i.e. Social Networking Applications, users may unknowingly allow these developers access to all their data. Use of this platform may be unchecked. For example, it is well known on the Social Networking Web Sites.

Platform that once a user adds an application the application will have the ability to access the entire user's information, if allowed to do so, regardless of the applications function. Even if the application developers are not malicious this does not mean that the application cannot be hacked.

4. Shared Technology Issues

A more interesting form of confidentiality issue relates to the construction of a cloud and the services themselves.

4.1. Virtualization Issues

The underlying virtualization architecture allows IaaS service providers the ability to host several machine images on a single server. Practical attacks on such services are: First, the authors showed that they could map the internal structure of the cloud, allowing them to determine if two virtual machines were co-resident with each other i.e. were running on the same physical machine. Secondly, they demonstrated that they were able to, purposefully; add a virtual machine to the cloud so that it was co-resident with another machine. Finally, the authors were able to show that once a machine was co-resident, they would be able to launch several attacks that would allow them to learn information regarding CPU cache use, network traffic rates and keystroke timings.

4.2. Service Aggregation

Aggregated services offer services based upon the functionality offered by existing services. Often aggregated services offer the combined functionality of existing services allowing for rapid service construction. However, service aggregation presents consumers with several interesting problems. Data is now being shared across multiple service providers whose privacy policies will also subject to change. Under whose privacy policy is the data governed by, how to combine the two policies? Furthermore, service aggregation can occur in an ad-hoc and rapid manner implying that less stringent controls could have been applied to the protection of data, increasing the likelihood of a problem.

5. Data Loss or Leakage

Although insecure APIs can lead to data loss or the unwanted exposure of information, consumers can also lose their information through other means.

5.1. Availability Issues

Availability issues are when user's data is made inaccessible to the consumer. The data has been made unavailable. Such a lack of availability can be a result of access privilege revocation, data deletion or restricting physical access to the data itself. Availability issues can be attributed to an attacker using ooding based attacks. A monetary effect can also be seen with availability issues. Monetary issues affect not only the consumer but also the CSP.

Flooding attacks will have an effect upon resource utilization and will result in increases to power consumption, network usage and hardware maintenance. Ultimately this will also increase the amount of money the consumer will be charged for resource usage. Moreover, these monetary increases will also increase the operational expenditure of the service provider. Fault tolerance protocols are used to combat the issue of node failure within the Cloud. Fault tolerance protocols replicate data across machines, and data centers, ensuring that if part of the cloud does fail a version of the data will still be available to the user. Part of the cloud will be redundant though for good measure. Data replication also requires that the data state of the data be synchronized across multiple nodes. However, poorly designed protocols can also lead to availability issues. Furthermore, the existence of multiple copies of data can also introduce confidentiality problems. The increased number of data instances also increases the likelihood that an attacker will be able to access the data.

5.2. Data Leakage

Another form of data leakage stems from the disclosure of information that, though hidden, is deduced from freely available information. When users interact with a service they can leave a public trail, be it from status/update messages or through new postings. Unwelcome linkage occurs when new information is discerned about an individual through analysis of the individuals public trail i.e. links. This unwelcome linkage could be accidental or the result of the individual not covering their tracks. Social graph merging is similar to unwelcome linkage however the links formed occur through the aggregation of social graphs. A social graph is a

graph describing a person's social information such as friends, groups and interests.
Through combination of a person's social graphs from separate social networking sites, or the social graphs of people from the same social network site, new information can be deduced.

6. Account or Service Hijacking

When communicating with the CSP malicious entities may seek to affect the integrity and authenticity of the user's communication with the CSP and vice versa. There are several ways in which the integrity and authenticity of a user's session can be impugned. Browser based interfaces and authentication are used by consumers to establish a session with their service provider. A malicious entity can attempt to capture or hijack this session or steal the user's credentials to access or inuence the user's data, from within the browser. Most browsers operate on a Same Origin Policy where client scripts are allowed to access resources if they share the same origin. However, attacks such as Cross Site Scripting and Cross Site Request Forgery, as well as DNS Poisoning can be used to undermine this security feature. Other issues found include the manipulation of the data being sent within the sessions. The effects of breaking session integrity are two-fold, for one the attacker will be able to steal the identity of their victim, and secondly impugn the reputation of the victim through falsified data. Such man-in-the-middle attacks will have lasting repercussions such as violation of the services terms of use, or criminal. For instance, the hacking of many a celebrity on social networking account.

7. Unknown Risk Profile

Risk Management is a business process that users can use to identify and mitigate threats.
It allows users to determine their current stance towards the security of their data. Auditing information such as software version, code updates current security practices, intrusion attempt are used as a basis for determining this stance. CSPs may not be so forthcoming with this information. Consumers, when adopting a service, must also accept the Terms and
Conditions (including privacy policy) of the service, together with any Service Level Agreements made. Consumers and providers need to comply with existing laws and regulations. However the degree to which service providers adhere to current security practices and legislation, or implement them may not be clear. This leaves the consumers with an unknown risk profile. Users are unable to determine the risk to their data as they do not have sufficient information to do so.

V. CONCLUSIONS

Cloud computing is still struggling in its accuracy, with positive and negative comments made on its possible implementation for a large-sized enterprise. IT technicians are spearheading the challenges. Cloud provides many options for the everyday computer user as well as large and small businesses. It opens up the world of computing to a broader range of uses and increases the ease of use by giving access through any internet connection. However, with this increased ease also come drawbacks. You have less control over who has access to your information and little to no knowledge of where it is stored. You also must be aware of the security risks of having data stored on the cloud. The cloud is a big target for malicious individuals and may have disadvantages because it can be accessed through an unsecured internet connection.
If you are considering using the cloud, be certain that you identify what information you will be putting out in the cloud, which will have access to that information, and what you will need to make sure it is protected. Additionally, know your options in terms of what type of cloud will be best for your needs, what type of provider will be most useful to you, and what the reputation and responsibilities of the providers you are considering are before you sign up.

REFERENCES

[1] http://www.cloudsecurityalliance.org/

[2] David S. Linthicum, Cloud Computing and SOA Convergence in your Enterprise, Pearson, 2010.

[3] Mehrdad Mahdavi Boroujerdi, Soheil Nazem, Cloud Computing: Changing Cogitation about Computing, World Academy of Science, Engineering and Technology 58 2009.

[4] R. Buyya, C. S. Yeo, and S. Venugopa, "Marketoriented Cloud Computing: Vision, hype, and reality for delivering it services as computing utilities", in Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08, IEEE CS Press, Los Alamitos,CA, USA) 2008.

[5] Top Threats to Cloud Computing V1.0, Cloud Security Alliance, March 2010.

[6] Amazon web service, [Online]. Available: http://aws.amazon.com/

[7] Armbrust, M., Fox, A., Griffith, R. et al. Above the Clouds: A Berkeley View of Cloud Computing. UCB/EECS-2009-28, EECS, Department, University of California, Berkeley, 2009.

[8] Brodkin, Jon. (2008, 07):Seven Cloud-Computing security risks, available online, http://www.infoworld.com/d/securitycentral/gartnerseven-cloud-computing-security-risks-853.

[9] Controlling Data in the Cloud: Outsourcing computation without Outsourcing Control, Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina Elaine Shi, Jessica Staddon Parc, CCSW'09, November 13, 2009, Chicago, Illinois, USA.

[10] Dan Hubbard, Michael Sutton et al. Top Threats to Cloud Computing v1.0. Tech. rep. v1.0. Cloud Security Alliance, Mar. 2010.

[11] Flavin Cristian. `Understanding fault-tolerant distributed systems'. In:Commun. ACM 34.2 (1991). issn: 0001-0782.

[12] Meiko Jensen, Jorg Schwenk et al. `On Technical Security Issues in Cloud Computing'. I: Cloud Computing, IEEE International Conference on 0 (2009).

[13] Siani Pearson `Taking account of privacy when designing cloud computing services'. In: CLOUD '09: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. Washington, DC, USA: IEEE Computer Society, 2009.

[14] The Cross-Site Request Forgery (CSRF/XSRF) FAQ. English. CGI Security. Apr. 2010.

[15] Robert Lemos. Alliance forms to _x DNS poisoning aw. English. Security Focus. July 08.

[16] Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 2010 1st International Conference on Parallel, Distributed and Grid Computing 2010.

[17] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, "Security and Privacy in Cloud Computing: A Survey", 2010 Sixth International Conference on Semantics, Knowledge and Grids.

[18] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, April-June 2010.

[19] Jianfeng Yang, Zhibin Chen, "Cloud Computing Research and Security Issues", International Conference on Computational Intelligence and Software Engineering(CiSE), Wuhan, Dec. 2010.

[20] Shuai Zhang, Shufen Zhang, "Cloud Computing Research and Development Trend", 2010 Second International Conference on Future Networks,ICFN'10 , 2010.

[21] Dan Hubbard, Michael Sutton et al. Top Threats to Cloud Computing v1.0. Tech. rep. v1.0. Cloud Security Alliance, Mar. 2010.

[22] Siani Pearson `Taking account of privacy when designing cloud computing services'. In: CLOUD '09: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. Washington, DC,USA: IEEE Computer Society, 2009, pp. 44

[23] Meiko Jensen and Jorg Schwenk. `The Accountability Problem of Flooding Attacks in Service-Oriented Architectures'. In: Availability, Reliability and Security, International Conference on 0 (2009)