ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

Study of Security Concerns in Cloud Computing

Satinder Singh
Dept. of Computer Science and I.T, Lyallpur Khalsa College, Jalandhar, Punjab, India

Abstract
From the past few years, cloud computing is one of the fastest growing segment in I.T industry. Cloud computing is sharing of resources on large scale which is cost effective and location independent. Resources in cloud computing can be installed by seller and used by client. In this paper, I will study the security concerns in cloud computing, which needs to be resolve. These security issues have greater impact on the cloud computing. I would also discuss services provided by cloud computing, cloud computing deployment and delivery model etc.

Keywords
Cloud Computing, Securing Clouds, Cloud Computing Deployment and Delivery Model

I. Introduction

Cloud Computing has been defined in many ways by analyst firms, academics, industry practitioners, and IT companies [1]. Cloud computing is an emerging IT development, deployment and delivery model, enabling real time delivery of products, services and solutions over the Internet (i.e., enabling cloud services) [3]. It can also be viewed as a style of computing in which massively scalable IT-related capabilities are provided "as a service" using Internet technologies to multiple external customers [2]. Cloud computing is based on four pillars such as applications, platforms, infrastructure, and enabling services [8]. The services provided by cloud computing are used either via web browser or via a defined API [1].

II. Cloud Computing Deployment and Delivery Model

Fig. 1, shows cloud computing deployment and delivery model [12]. It consists of five cloud delivery models such as hybrid cloud, private cloud, agency cloud, community cloud and external cloud. The model also contains three service methods namely SaaS (cloud software compuing), PaaS(cloud plateform computing) and IaaS(cloud infrastructure computing).

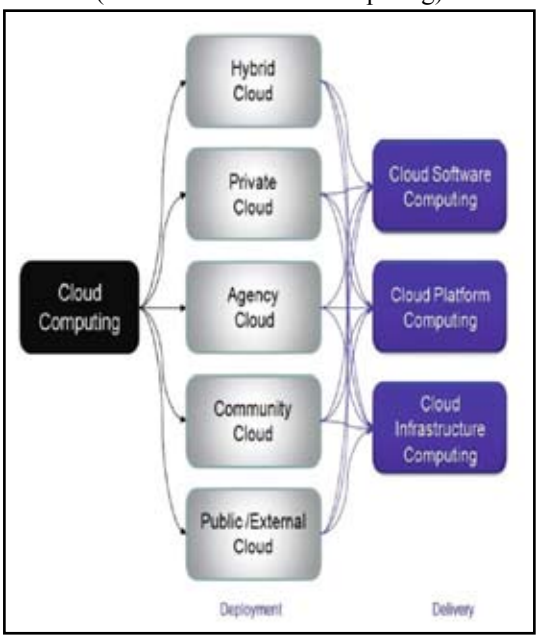


Fig. 1:

The hybrid cloud consists of two or more clouds such as a private cloud joining another vendor's provisioned public cloud. Private cloud is an enterprise-owned cloud exclusively accessed for its operation or activity. It is not shared or co-owned with another enterprise, such as the Microsoft Azure on-premise platform cloud [16]. Fig. 2, shows cloud security relationship framework [12]:



Fig. 2:

Agency cloud is a kind of community cloud exclusively for the military, agency or defense institutions, such as the Defense Information Systems Agency (DISA) cloud [15] and the NBC Federal Computing Cloud [16]. The community cloud is a cloud specifically consumed by a particular set of community, such as financial institutions cloud, health services cloud, etc.

A public or external cloud is a general-purpose cloud computing environment managed by a cloud provider. The cloud provider could be external provider, such as Amazon EC2, Google Apps, Salesforce, Rackspace, etc. that leases third-party cloud resource to the consumer [12].

However the security requirement of different cloud model varies for example security requirement for private clouds are different than public clouds. However private clouds are more secure than public clouds [12]. A cloud security relationship model is a theoretical framework to evaluate cloud deployment and delivery models based on security, cost and capability requirements [12].

III. Security Concerns in Cloud Computing

There are many security issues in cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. The major security issue with cloud computing is that the owner of the data may not have control over the location of the data. The reason behind this is, to take the benefits of using cloud computing, one must also utilize the resource allocation and

scheduling provided by clouds. Therefore, we need to safeguard the data in the midst of untrusted processes [14].
Currently, it would be difficult to provide a complete solution to securing the cloud due to complexity of clouds. Therefore, the best approach to provide security in cloud computing is to make increment enhancements to securing the cloud which finally results in secure clouds.

A. Data Confidentiality
The seller must make sure that customer private information should not be shared with any other operator i.e. it should be secured. As most of the servers are external, the vendor should make sure who is accessing the data and who is maintaining the server thus enabling the seller to protect the customer's personal information [12].

B. Data Location
Currently, clouds are hugely uncontrolled, especially the public ones. ''When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers,''[17]. When it comes to location of the data nothing is transparent even the customer don't know where his own data is located. The seller does not reveal where all the data is stored. The data won't even be in the same country of the customer, it might be located anywhere in the world [18].

C. Regulatory Compliance
Customers are ultimately responsible for the security and integrity of their own data even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are ''signaling that customers can only use them for the most trivial functions,'' [17].

D. Data Segregation
Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. ''Find out what is done to segregate data at rest,'' [17]. The seller must ensure that the encryption schemes were designed and tested by experienced specialists. ''Encryption accidents can make data totally unusable, and even normal encryption can complicate availability,'' [17].

E. Recovery
As I told earlier, the client is not aware of the location of his data but still cloud provider should tell him what would happen to his data in case of disaster. ''Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure,''[17]. Ask your provider if it has ''the ability to do a complete restoration, and how long it will take'' [17].

F. Investigative Support
Investigating inappropriate or illegal activity may be impossible in cloud computing [17]. ''Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible''[17].

G. Long-Term Viability
The seller of cloud computing would never run away or acquired by large company or never leaves his business. But the client must be ensuring that his data would remain available even after such an event. ''Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application,'' [17].

H. Data Integrity
Data integrity is another security issue in cloud computing. Any one from any location can access the data on the cloud. Cloud does not differentiate between a sensitive data from a common data thus enabling anyone to access those sensitive data. Thus there is a lack of data integrity in cloud computing [18].

I. Data Theft
As the servers for cloud computing are very expensive therefore many cloud computing seller instead of purchasing server lease a service from other service provider because they are cost effective and flexible for operation. The client never knows about these things so there is a high probability that data can be stolen by malicious user from external server.

J. Infected Application
The cloud provider should have the complete access to the server. It is required for monitoring and maintenance and also prevents any malicious user to upload any infected application onto the cloud. The infected application would surely affect the customer.

K. Data Loss
Another serious security issue in cloud computing is data loss. If the vendor closes due to financial or legal problems there will be a loss of data for the customers. The customers won't be able to access those data's because data is no more available for the customer as the vendor shut down [18].

L. Security on Vendor Level
Vendor should make sure that the server is well secured from all the external threats it may come across. A Cloud is good only when there is a good security provided by the vendor to the customers [18].

M. Security on User Level
Even though the vendor has provided a good security layer for the customer, the customer should make sure that because of its own action, there shouldn't be any loss of data or tampering of data for other users who are using the same Cloud [18].

N. Data Security
This risk stems primarily from loss of physical, personnel and logical control of data. Issues include virtualization vulnerabilities [20], SaaS vulnerabilities (e.g. a case in which Google Docs exposed private user files) [21], phishing scams [22] and other potential data breaches. Other data security risks mentioned in [23] include data leakage and interception, economic and distributed denial of service and loss of encryption keys. Unique risks also arise due to the multi-tenancy and resource-sharing models as pointed out in [19, 22, 24-26].

O. Third Party Control

This is probably the prime cause of concern in the cloud. With the growing value of corporate information, third party access can lead to a potential loss of intellectual property and trade secrets. There is also the issue of a malicious insider who abuses access rights to tenant information. The fear of corporate espionage and data warfare also stems from third party control. Provider compliance with regulations such as those on auditing also raise questions on how that can be effected on site in a globally distributed multi tenant environment [27, 19].

P. Privacy and Legal Issues

Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Pearson summarized the main privacy issues of cloud computing [28]. Users are made to give away their personal information without knowing where it is stored or what future purpose it might serve. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks [19].

IV. Conclusion

Cloud computing is one of the emerging field in IT industry. There is no doubt on the services and benefits provided by cloud computing. But still there are many security issues associated with it that are still unresolved. Lot of work is required in the fields of securing cloud computing. Both the seller and the customer should make sure that the cloud is safe from all the external threats thus there will be a mutual understanding between the customer and the seller when it comes to the security on cloud.

References

[1] Katarina Stanoevska-Slabeva, Thomas Wozniak,"Grid and cloud computing, Springer Cloud Basics – An Introduction to Cloud Computing".

[2] Gartner (2008),"Gartner Says Contrasting Views on Cloud Computing Are Creating Confusion", Gartner press release, 29 September 2008. [Online] Available: http://www.gartner.com/it/page.jsp?id=766215.

[3] Gens F (2008),"Defining Cloud Services and Cloud Computing", IDC exchange, 23 September 2008. [Online] Available: http://www.blogs.idc.com/ie/?p=190.

[4] Fellows W (2008),"Partly Cloudy – Blue-Sky Thinking About Cloud Computing", 451 Position Paper, Executive Overview, The 451 Group. [Online] Available: http://www.451group.com/reports/executive_summar.php?id=619.

[5] Merrill Lynch (2008),"The Cloud Wars: $100+ billion at stake", Merrill Lynch research note, May 2008.

[6] Katarina Stanoevska-Slabeva, Thomas Wozniak,"Grid and cloud computing", Springer Grid Basics.

[7] A K Chakravarti,"Cloud computing – challenges and opportunities".

[8] Dimitris N. Chorafas,"Cloud computing strategies", CRC press.

[9] O'Rielly, T. Mather, S. Kumarasuwamy, S. Latif,"Cloud Security and Privacy", 2009.

[10] A.S, A.K, M.B.,"An insight to security issues and solutions in cloud computing".

[11] J. W. Rittinghouse,J. F. Ransome,"Cloud Computing: Implementation, Management and Security", CRC Press, 2009.

[12] Cyril Onwubiko,"Cloud computing, principles, systems and application", Security Issues to Cloud Computing.

[13] Kaufman LM (2009 July/August) Data security in the world of cloud computing. IEEE Sec Priv 7(4), pp. 61–64.

[14] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham,"Security Issues for Cloud Computing".

[15] Greenfield T (2009),"Cloud computing in a military context – Beyond the Hype, Defense Information Systems Agency (DISA)", DISA Office of the CTO. [Online] Available: http://www.govinfosecurity.com/regulations.php?reg_id = 1432.

[16] NBC Federal Cloud Playbook (2009),"National business center, Department of the Interior", Washington DC. [Online] Available: http://www.cloud.nbc.gov/PDF/NBC%20Cloud%20White%20Paper%20Final%20(Web%20Res).pdf.

[17] Gartner,"Seven Cloud-Computing Security Rrisks".

[18] Lord Crusader,"Problems Faced by Cloud Computing".

[19] Aderemi A. Atayero, Oluwaseyi Feyisetan,"Security Issues in Cloud Computing", The Potentials of Homomorphic Encryption.

[20] "VMware Shared Folder Bug Lets Local Users on the Guest OS Gain Elevated Privileges on the Host OS", (2008), [Online] Available: http://www.securitytracker.com/alerts/2008/Feb/1019493.html.

[21] "Google Docs Glitch Exposes Private Files", (2011): [Online] Available: http://www.pcworld.com/article/160927/google_docs_glitch _exposes_private_files.html.

[22] Salesforce.com(2011),"Warns Customers of Phishing Scam", Retrieved April 9, 2011 from [Online] AVailable: http://www.pcworld.com/businesscenter/article/139353/salesforcecom_warns_customers_of_phishing_scam.html.

[23] Catteddu, D., Hogben, G.,"Cloud Computing: benefits, risks and recommendations for information security", Technical Report. European Network and Information Security Agency, 2009.

[24] J. Brodkin, (2008),"Gartner: Seven cloud-computing security risks, [Online] Available: http://www.infoworld.com/d/security-central/gartnerseven-cloud-computing-security-risks-853

[25] Brunette, G., Mogull, R.,"Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.Technical Report", Cloud Security Alliance, 2009.

[26] Maggi, F., Zanero, S.,"Rethinking security in a cloudy world. Technical report", Dipartimento di Elettronicae Informazione, Politecnico di Milano, 2010.

[27] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, J. Molina,"Controlling data in the cloud: Outsourcing computation without outsourcing control", In ACM Workshop on Cloud Computing Security, 2009.

[28] Pearson, S.,"Taking account of privacy when designing cloud computing services", In ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada, 2009.

[29] "Expert Reference Series of White Papers global knowledge", 10 Security Concerns for Cloud Computing.



Satinder Singh received his master degree in Computer Science, M.Tech degree in Information Technology from Guru Nanak Dev University, Amritsar. He is presently working as Assistant Professor in the Department of Computer Science & I.T at Lyallpur Khalsa College, Jalandhar (Punjab) India. He has more than 6 years of teaching experience of post graduate classes. He has guided number of major and minor projects of graduate and post graduate classes. He has also supervised thesis of M.Tech students. His research interests include theory of automata, cloud computing, software engineering. He has to his credit more than 14 research papers in National and International conferences and 6 textbooks in Computer subjects.