ISSN:0975-9646

Assay of Data Security in Cloud Computing

Navan Preet Singh[1,] Bhavkaran Singh Walia[2]

[1]*Department of Computer Science,*
Guru Tegh Bahadur Institute of Technology – Guru Gobind Singh Indraprastha University, India
[2]*Department of Computer Science,*
Guru Tegh Bahadur Institute of Technology – Guru Gobind Singh Indraprastha University, India)

Abstract: Cloud computing is an internet based model that enables an easy to use, on demand services and access to shared resources. It is a computational technology that fulfills a user's requirements of physical and virtual resources. It is a paradigm where jobs are assigned to a composition of connections, softwares and services. Since cloud computing shares distributed resources via the network in an open environment, it has its own associated risks and threats that compromises integrity and encompasses theft, data leakage and insecure platform.

In this paper, we researched a few of the popular cloud services providers in terms of security threats they faced in the past. We have also mentioned a few solutions that may help in improving the security of data in the cloud and increase trust between the customers and the cloud service providers.

Keywords: Cloud computing, privacy, risks, security, QoS(quality of service).

1. INTRODUCTION

The architecture involves various cloud constituents interacting with each other over a loose connection such as a messaging queue [2][10]. The components involved are infrastructure services, platform services and application services. Security and privacy issues are massive obstacles for large scale adoption of cloud computing. The use of virtualization techniques leaves the system vulnerable to new threats, (which previously were not considered applicable). It is possible that applications hosted in the cloud can process sensitive data and such data can be stored within a cloud storage warehouse which might leave it vulnerable to security threats. The disputes in this area are devising secure and trustable systems from different perspectives: legal, social, and technical.

Types of Cloud Services

Service Provider Type	Examples
IaaS	Amazon EC2, Amazon S3[1]
PaaS	Microsoft Azure Services, Google App Engine
SaaS	Salesforce, Abiquo

SaaS [12][13] represents the largest cloud market. It uses the internet to deliver apps which are managed by a third-party vendor and the interface is accessed on the client's side. Most of the applications used can be directly run from an internet browser and not downloads or installations are required though some may require little plug-ins. PaaS is used for applications and development concomitantly providing cloud components to software. With PaaS[14], the users gain a framework that they can develop or customize apps or even build upon it themselves. With this technology, cloud service providers can manage operating systems, servers, virtualization, networking, storage and the PaaS software itself. In IaaS, users can purchase services based on consumption analogous to utility bills, instead of spending capital on hardware outright. The users manage data, applications, operating systems etc, while the service providers handle servers, storage, virtualization etc.

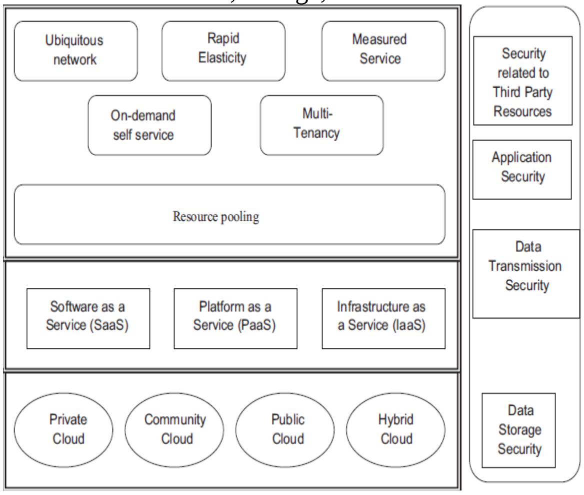

Fig.1 Architecture of a cloud computing environment

2. WHY CLOUD COMPUTING?

2.1 Advantages of cloud computing

One of the major advantages of moving infrastructure and services to the cloud is reduction or removal in the costs that are related to support and maintenance [1]. There is a noticeable improvement in performance since the cloud is a network of powerful computers and not a single computer which results in considerably high processing power. We are freed from maintenance and up gradation, since, the cloud is upgraded and maintained by the service provider. Cloud computing is an eco friendly approach as it allows sharing of resources among users. Hence, it does not require large data centers which need a lot of power. This technology is mobile, because we can access our data anywhere and do not need to carry personal computers. Cloud technology is easily scalable as the user can ask for an increase in resources if the same is required when new functionality or data is added to an application. Also, if requirements are reduced, user can ask for contraction in resources as well. All the data saved in a cloud can be easily and automatically backed up.

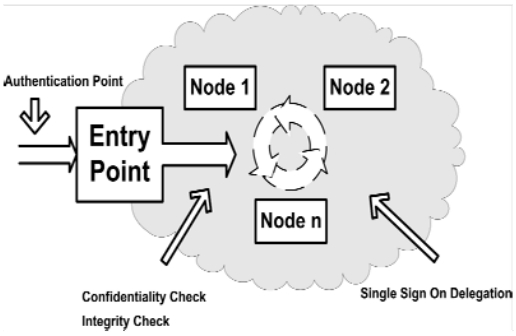

Fig.2 Data security checkpoints

3. Threats And Challenges To Data Safety

3.1 Disadvantages of cloud computing

As the customers are liable for security of data, hence if due to any unavoidable circumstances, if the data is lost then the service provider will not responsible. Therefore, the chances of high jacking are high [6]. There is a possibility of an insider attack by the cloud service provider, as a fraudulent employee may indulge in stealing and phishing data. In cloud computing the user has negligible control over services. There is a chance that the user and the service provider are from different countries and hence disputes may arise in implementation of jurisdiction. There would be Issues in portability from one service provider to another as they have different architectures. QoS (quality of service) is an unattended array as of now. Since the focus of the cloud service provider is of cost effectiveness and not of QoS.

3.2 Survey on security issues faced by different cloud service providers

There have been a number of threats that cloud services providers have faced over the years. The Amazon EC2 [18], which provides IaaS type services suffered data loss in April 2011 where small amounts of data were lost for some users due to a human error. It also suffered from an attack in 2009 in which "numerous Amazon systems were hijacked to run Zeus Botnet nodes". The report doesn't mention what the Botnet nodes did but it did result in Amazon shutting down the compromised EC2 nodes, which were detected by a security firm named Prevx. [3]

In the case of Microsoft, on February 29 2012, a service outage had affected its Azure cloud service. This problem was caused by a Leap year bug that was triggered when at midnight on Feb. 28, a HTTPS certificate expired. If these certificates don't get renewed on time, then the entire system collapses. The electronic control hadn't taken into account the extra day in a leap year after every four years. The error was a simple human error which could have been easily avoided. [19]

In 2007, a phishing attack on Salesforce.com, compromised the company's credentials and valuable data. The attacker was then able to contact its customers and started phishing attacks on them. These attacks are not easy to detect because it is not immediately evident. Generally, consumers and financial institutions fall prey to these attacks. Institutes like Bank of America, SunTrust and Automatic Data Processing fell prey to this phishing attack. The attackers used malicious software which stole data by asking the unaware user to click on a link. Unfortunately, such attacks are just the beginning of a long series of attacks and were of serious ramifications. In July 2012, Salesforce.com was once again facing issues. This time, the attack focused on the email service which caused a considerable decline in its performance for about 7 hours. [4]

4. Tradeoff Between Cost And Security

One of the potential enterprise security benefits for cloud is that it can enable affordable business continuity plans. Therefore there is a huge potential for cost savings The need to disparate between Information Risk Management versus Enterprise Risk Management (business impact) [7] when examining the security impacts of Cloud, and the need to trade off between cost savings resulting from use of cloud and the need to invest in cloud security When a user registers for a cloud computing service, strict verification check should be done about the user's information. The user and the Cloud Service Provider must enter into a Service Level Agreement (SLA), clearly specifying the responsibilities and roles of both the signatories and the terms and conditions of the contract. Responsibility in case of loss of data [8][15] because of the cloud service provider need to be clearly stated and means of data backup should be available and implemented. The Cloud Service Provider should enforce stringent authentication and validation policies for employees. There should be an auditing procedure for the cloud service. Intelligent data for enterprises to enhance control to data in the cloud, we propose moving from securing the data from the inside rather than the outside. We call this approach of data and information protecting itself data centric. This self securing technique requires intelligence be put in the data itself. Data needs to be self protecting and describing, irrespective of its environment. Data needs to be bundled and encrypted with a security policy. When accessed, data should consult its own security policy and strive to recreate a secure environment using virtualization and decrypt itself only if the environment is found to be reliable. Data centric security is a plausible extension of the trend towards reliable and more employable data protection.

5. Possible Solutions

5.1 Fog computing as a security solution

Fog computing [5][9], also known as fogging is a technique in which data storage, application services and computing are concentrated in devices at the edge of the network rather than existing entirely in the cloud. This concentration at the edge means that data will be stored locally rather than being sent on to the cloud for computing and processing. Since the data is processed and stored locally it would never be sent to the servers and hence it provides greater security than the cloud. Even if the cloud servers are hacked or compromised the data is still safe as most of the data exists locally. Not only is this a great security solution but it would save a great deal in bandwidth. For example: a jet engine at an average produces 10 TB data of its condition and performance in half hour. Broadcasting this data over to the cloud and transmitting the response back puts a great deal of stress on the bandwidth, needs a substantial amount of time and can lead to latency. While in a fog computing environment, most of the processing would take place in a router, rather than being transmitted. Hence fog computing can address services and applications that do no fit the paradigm of the cloud and also provides added features of security.

5.2 *Auditing by the data owner*

There has been a lack of transparency which is deterring businesses from moving their data to the cloud. Data owners want to audit the way their data is being managed at the cloud, and make sure that their data is not being leaked or misused, or at least leave an audit [17] trail when it happens. the database servers must show a retractable evidence that it is rightly storing all the user's data.

5.3 *Security enhanced business intelligence*

Another approach of keeping control of data is to do the encryption of all cloud data. The issue with encryption is that it limits data usage. Especially the searching and indexing of data is problematic. With orthodox, randomized encryption techniques, it is impossible to search for documents using a keyword. While it can be easily done if data is saved in clear-text. State of the art cryptography offers new methods to solve these issues. Recently, cryptographers have invented adaptable encryption techniques that would allow computations and operations on the encrypted text. For e.g. Searchable encryption allows user to determine a capability from a clandestine key. A capability ciphers a search query, and the cloud uses this capability to determine which documents match the query, without knowing of any additional information. Other primitive cryptographic techniques like Private Information Retrieval [11] and homomorphic encryption [24] execute computations on cryptic data without decrypting. When these methods mature, they may open a new array of possibilities for cloud computing security. Whereas in a lot of cases, extensive research is required to make these cryptographic algorithms practical for the cloud, they present the optimal solution for a clear distinction for cloud computing, since these algorithms would enable users to benefit from each others' data in a controlled environment. Even cryptic data can be used++ to detect irregularities that might be valuable from a business intelligence point of view. Further now, if the service provider is empowered with some ability to search the cryptic data, the acceleration of cloud data can enable better insider threat detection.

6. Conclusion

Most of the fears of cloud computing come from the perception of loss of control of delicate data [16]. The prevailing control techniques do not sufficiently address cloud computing's third party information storage and processing needs. We believe that the extension of control techniques from the business into the cloud through the application of secure computing and cryptographic algorithms. These techniques should mitigate most of today's apprehensions of cloud computing and have the capability to give supportable business intelligence benefits to cloud participation. Analyzed the trusted computing in the cloud computing environment and the function of trusted computing platform in cloud computing. The future vision relates to issues and abuses arising from a higher dependence on cloud computing, and how to preserve security in case of such attacks. Specifically, new threats require new structures to improve and preserve security. Among these are tools to understand and control privacy leaks, performing verification, and guaranteeing availability in case of cloud DoS(denial of service) attacks.

We presented possible intelligent security solutions that not only would enhance the robustness of the cloud services but also increase trust between the customer and the service provider which is an important factor prevalent in the customers mindset, highly influencing his future business decisions.

References

1. Amazon elastic compute cloud (2008), http://aws.amazon.com/ec2/
2. Twenty Experts Define Cloud Computing (2008), http://cloudcomputing.syscon.com/read/612375_p.htm
3. John, H.: Security Guidance for Critical Areas of Focus in Cloud Computing (2009), http://www.cloudsecurityalliance.org/guidance/ (Accessed 2 July 2009)
4. Salesforce.com Warns Customers of Phishing Scam. http://www.pcworld.com/businesscenter/article/139353/salesforcecom_warns_customers_of_phishing_scam.html
5. Fog computing applications, http://www.cisco.com/web/solutions/trends/tech-radar/fog-computing.html
6. Lithuania Weathers Cyber Attack, Braces for Round 2. http://blog.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html.
7. Don't cloud your vision. http://www.ft.com/cms/s/0/303680a6-bf51-11dd-ae63- 0000779fd18c.html?nclick_check=1.
8. FTC questions cloud-computing security. http://news.cnet.com/8301-13578_3-10198577- 38.html?part=rss&subj=news&tag=2547-1_3-0-20
9. Fog Computing, Ecosystem, Architecture and Applications, http://www.cisco.com/web/about/ac50/ac207/crc_new/university/RFP/rfp13078.html
10. Twenty Experts Define Cloud Computing (2008), http://cloudcomputing.syscon.com/read/612375_p.htm
11. David S. Linthicum, Cloud Computing and SOA Convergence in your Enterprise, Pearson, 2010.
12. Mehrdad Mahdavi Boroujerdi, Soheil Nazem, Cloud Computing: Changing Cogitation about Computing, World Academy of Science, Engineering and Technology 58 2009.
13. 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.
14. IaaS, SaaS, PaaS, http://apprenda.com/library/paas/iaas-paas-saas-explained-compared/
15. Top Threats to Cloud Computing V1.0, Cloud Security Alliance, March 2010.
16. 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
17. 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.
18. Amazon web service, [Online]. Available: http://aws.amazon.com/
19. Microsoft's Azure Fails Over Unrenewed Security Certificate http://www.forbes.com/sites/timworstall/2013/02/23/ridiculous-microsofts-azure-fails-over-unrenewed-security-certificate/