International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 7 4547 - 4550

Security Certification As a Service Over Cloud

Kalyani Rammohan Madurwar
Student of Master of Computer Engineering
Alard college of Engineering and Management
Savitribai Phule Pune University,
Pune, India
kalyanimadurwar@gmail.com

Prof.Sonali Patil
Professor, Department of Computer Engineering,
Alard Collage of Engineering and Management,
Savitribai Phule Pune University,
Pune, India
Sonalin69@gmail.com

***Abstract*:-** Now a day's Cloud computing is the best solution for IT industry as the infrastructure and application services offerings are enabled on subscription basis. Because of this most of the enterprise level companies like Amazon, IBM, Google, and Microsoft are providing useful offering to their customers as Cloud services. There are multiple criteria on the basis of which the customers may decide the appropriate cloud service provider as there are many cloud service providers are there in the IT medium, Customers don't have any framework on which they can trust, so the idea of designing a framework which can unable trust between end customer and cloud service provider along with raking them according to different attacks like DDoS, brute force, file integrity etc., the framework or solution will be known as Third Party Auditor (TPA).

Keywords:-*Cloud Security, Cloud Computing, Cloud Service provider, third party Auditor.*

*****

I. INTRODUCTION

The biggest Mythology in information technology is the existence of 'cloud'. Actually, there are many clouds available in the market, development and maintenance of each is done by own provider, Provider establishes the different parameters and definitions for its cloud offerings.

With such a promise of something that is unobtainable separations of clouds to choose from and the low fence to entry enterprises may consider try them all, placing different workloads with different cloud service providers. The strategy creates more problems than it solves for which enterprises that go on this route. Manage multiple environments, consoles, vendors and with different pricing schemes, parameters of performance and SLA (Service Level Agreements) increase the huge burden to enterprise level IT. A main drawback while working with multiple vendors it limits the freely performing critical 'inter cloud' functions, example backup and recovery. Multivendor environments may be exposing the company at heavy risk if go ahead without applying security profiles [4].

If the offering of cloud service providers have different characteristic. So this is difficult to choose just one which covers all the required applications and workloads that the customer wants to place in the cloud [1]. The aim is to find the provider which has cloud portfolio is as varied and flexible as the workloads possibly handle now and in to the future. Which cloud service provider's services to be used? Is the big question in front of the customers because huge numbers of cloud service providers (CSP) are available in the market, so this is big challenge for the consumer? There are very less frameworks available in the market which can help us to evaluate and rank the offerings based on its ability to overcome the users (QOS) quality of service and also the security requirements, the idea of providing such an application is born here so in this work a ranking system with high security which can measures the secured cloud services are proposed, so that the service level agreement (SLA) and QOS and trustworthiness can be satisfy among cloud providers [7], Hence we have started implementation of ranking system by which the consumer can identify the risk of business data before hosting it to unknown cloud service provider in market. So the objective of this paper is to maintain smooth trust between customer and cloud service providers and provide an application that can run different test on the CSPs like brute force, file integrity and DDoS etc... And rank them so that the customer can identify the best CSP in the markets in terms of reliability and security, the rank system can be known as TPA (Third Party Auditor).

There would not necessity of any broker, the customer can make decision independently, this is the one of the best feature and advantage of the model, making this TPA model robust more security attacks are applying on the CSP so that customer can get best in the market. Logs are stored for the troubleshooting if required.

This paper highlights CSP security aspects and how to ensure of these in cloud at user's point of view. We propose a concept full security vulnerability measuring automated model for rank the CSP authenticity and reliability such as issuing security certificates which help the new cloud customer to evaluate the best Cloud service Providers in the market. The conceptual model contains a monitoring of TPA to protect cloud users rights and cloud provider's security.

The Paper is divided in below sections: Section 2 discusses existing system, Section 3 introduces the proposed model with block diagram, and explains different attacks and ranking system, Section 4 describes the Experimental Setup and section 5 explains the Result and in section 6 the model is concluded with Conclusion.

II. EXISTING SYSTEM

A Ranking for cloud component in different designs of Cloud Applications, & proposed of quality and assurance based component ranking system framework for cloud SaaS applications advantages are taking of the past used component can be experience for different components user. Also here other resource provisioning can be used so that the leveraging capacity of local cluster to external resources providers,

because of this the cost will be reduce by using Spot Market. To find the responsibility of Violation as a parameter SLA which can be parameter revenue or profit which is discussed and explained by Alhamad Md. [7] The proposed model by Chan H [8] attributes, an information collection the analytic algorithm and mechanism based on (SVD) Singular Value Decomposition Technique to determine the best service provider for a user application with a specific set of requirements. The model of the SMICloud by Garg S.K.[9] so that users can compare different types of cloud offerings, according to their several dimensions and priorities, and choose overcome to their needs. So the Java based ranking centralized console which can do some calculation and show the cloud services based of all other different applications.

III. PROPOSED SYSTEM

To explain the proposed model we have considered the following scenario. Assume a new cloud customer consider an owner of a company or firm or manager of the company is looking for the cloud facility for their company, the main mandatory and prioritised condition is the data should maintain privacy and security. When Manager looks numbers of CSP in the market? But no particular facility provided to adopt the best and secured cloud service provider for the company. To decide the correct provider the new customer needs trust certificate or security reports of these CSP. That's why the security issues would be the most important and significant for the growth of cloud computing [11, 12]. There are some systems are available for ranking in service provisioning or performance issues but not robust and accurate ranking system for cloud service provider is available..

A. (CSP) Cloud Service Providers

The CSP are the entities who own the big cloud infrastructure and provide cloud services for customers. The implementation and design of cloud service provider infrastructure and price models are we have not consideredin this paper as it is out of the scope of this.

B. Security Metrics (SM)

To know what to measure, how to measure and communicate all those metricises which can help us to improvement of security's efficiency, effectiveness and the business perspective. The generated metricises will provide an initial knowledge to ensure achieve the aimed goals, which will involve over time as per the particular business needs and data security risk aspect.

C. Attack Vectors

Attack vectors are processes used to get into computer systems, usually for evil or penetration purposes. They take advantages of known weak spots to get entry. Mainly, it is nothing but the any methods of attacks can be selected by the hackers to identify weakness or vulnerability on the client side or server end of a network for engineering defects in the system in order to hack or infect system resources.

For security testing purpose the brute force, file integrity, DDos, file upload and download attacks are used.

In fact, by considering several security issues [13-16] we have found obvious to need some sort of proactive monitoring, assurance and trust which would be between Cloud Service providers and third party Auditor. So, Third Party Auditor and ensuring security features gets together and provides valid trust among the cloud community as a whole.

D. Assumptions

In this proposed model, several assumptions are considered as follows:

- TPA must maintain the trust and reliability between Customer and CSP, just like credit Rating company
- TPA should have all required resources to provide for executing and processing their work.
- TPA must maintain and regulated by strict transparent policies, laws, and regulations.
- Both TPA and Cloud Service Provider mutually agree before performing the software penetration test.
- Considered as CSP provide SaaS of its own.
- For ranking results TPA is responsible for collection of non-measurable metrics from trusted source and processes this information
- A Customer looks for security and certificate of trust should pay as fees to the third party to see and use the Results and access their services

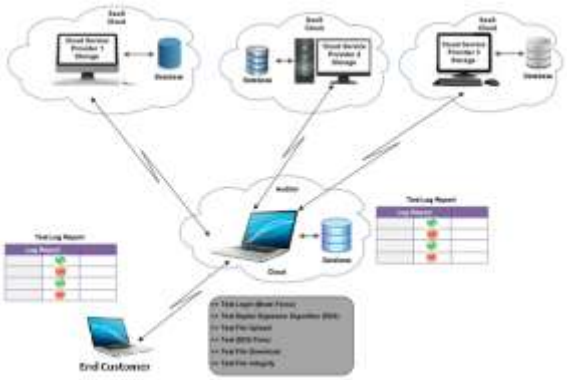


Figure 1Proposed Model to select Cloud Service Provider

Considering several security issues [13-16] we need some sort of monitoring, assurance and trust which not only come from the Cloud Service provider but also from a TPA. So, TPA and security ensuring features together provide trust among the cloud community as a whole. Fig 1 shows the proposed model of Cloud Service Provider ranking system.

1) Ranking Algorithm

We are going to provide two algorithms and both are explained in details here Pseudo code 1 explains the calculating procedure of security metrics SM and Pseudo code 2 describes the final calculation of ranking results, Rn.

Pseudo code 1: Calculating Security metrics SM

```
1 //Calculating Security metrics SM
2 Initially SM=0;
```

 ISSN: 2321-8169
4547 - 4550

3 //Negotiate with Cloud Service Provider side from TPA to network and connection setup
4 While connection setup =0 do
5 connection setup=1;
6 end;
7 //Software scripting try to break the security of CSP side.
Here, I is the several numbers of top threats defined and included in TPA software scripting
8 While I! = 0 do
9 //Execute the specific software coding to test the strength or defence mechanism of CSP
10 If successful to break the specific security, SM=SM+1;
11 endif;
12 end;
13 /* finally send the Security metrics S to the TPA*/
14 Send SM to TPA

Pseudo code 2: Calculating Final Rank Rn

1 //Collect the non-measurable metrics (F) from reliable sources and input by the TPA
2 Get the input F;
3 Get the input Rn //As collected by employing Pseudo code 1 by TPA
4 Final Rank, R=S+F;
5 Published the Rank result, or to the TPA website.

IV. EXPERIMENTAL SETUP

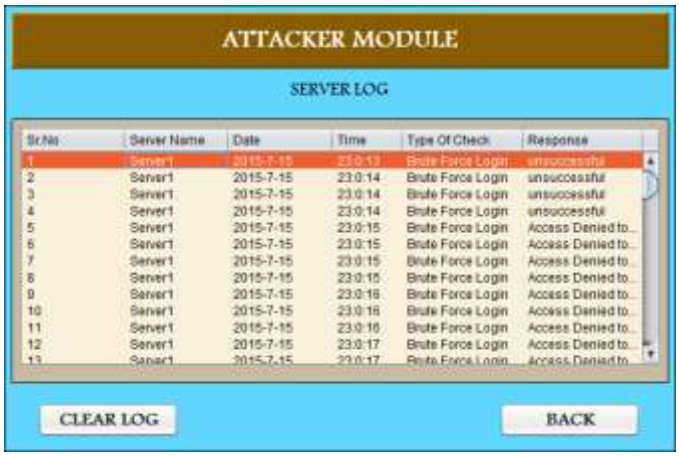
For the implementation of the project the below technical setup is required.

- OS: Microsoft Windows XP Professional SP3/Vista SP1/Windows 7 Professional:
- Processor: 2.6 GHz Intel Pentium IV or equivalent
- Memory: 2 GB
- Disk space: 1 GB of free disk space
- Glassfish web server
- NetBeans
- Java 7
- MySQL

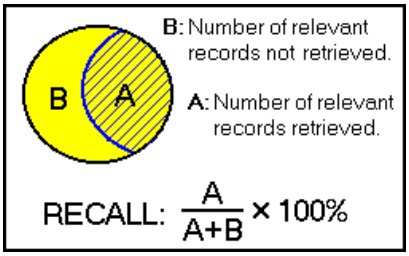
V. RESULTS

The home console of the attacker is look like

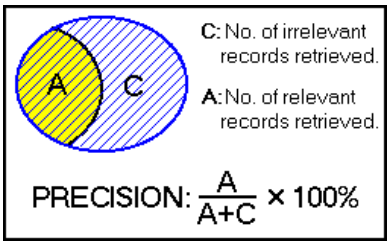
Log will be looking like



RECALL is the ratio of the numbers of relevant record retrieve to the total numbers of relevant record in the database. Expressed as a (%) percentage



PRECISION is the ratio of the numbers of relevant record retrieved to the total numbers of irrelevant and relevant records retrieve. It is expressed as a (%) percentage



So from above data we can calculate the expected result for our model.

Assume:

- We are trying to upload 20 files
- The 18 files uploaded out of 20
- But only 17 files are relevant

Below is the method to calculate precision and recall
A: Total number of relevant files uploaded.
B: Total number of relevant files not uploaded
C: Number of irrelevant files

So here,
A = 18, B= (20-17) 3, C= (20-18) 2
RECALL = (17/ (17+3)) = 0.85
PRECISION= (17/ (17+1)) = 0.94
Accuracy percentage (%) = (Total Files Uploaded) / (Correct Retrieved Object) = (20/17)*100% = 85%

VI. CONCLUSION

In this paper, we identify and highlight the CSP side security issues and tolerance of security strength by employing and introducing TPA which provide us CSP ranking system. To the best of our knowledge, using attack vectors to protect and ensure customer interest and confidence by issuing security ranking systems to select secure CSP is the first time in Cloud Computing. First, TPA uses automated software scripting to check security vulnerabilities in CSP side by running software scripting to break the security strength of the CSP. Therefore, considering several non-measurable metrics such as customer satisfaction, Security, availability etc. factors, TPA announce a secured CSP ranked system in their website. We compare this TPA Cloud provider ranking system like as a credit rating agency.

For troubleshooting and detailed information the logs would be captured for every event with the help of which we will compare the Good Cloud Service Provider.

.

VII. ACKNOWLEDGMENT

It is with the greatest pleasure and pride that I present this paper. At this moment, I cannot neglect all those who helped me in the successful completion of this paper. I am verythankful to my respected project guide. Associate Professor, for his ideas and help proved to be valuable and Helpful during the creation of this paper and guide me in the right path. I would also like to thank all the faculties who have cleared all the major concepts that were involved in the understanding of techniques behind this paper. Lastly, I am thankful to my friends who shared their knowledge in thisfield with me.

REFERENCES

[1] Md Whaiduzzaman, Abdullah Gani, “Measuring security for cloud service provider : A Third party approach” 2013 International Conference on Electrical Information and Communication Technology (EICT) 978-1-4799-2299-4/13

[2] Z. Sanaei, S. Abolfazli, A. Gani, and M. Shiraz, "SAMI: Servicebased arbitrated multi-tier infrastructure for Cloud Computing," in Communications in China Workshops (ICCC),2012 1st IEEE International Conference on, 2012, pp. 14-19

[3] M. Shiraz, M. Whaiduzzaman, and A. Gani, "A Study on Anatomy of Smartphone," Computer Communication & Collaboration, vol. 1, 2013

[4] M K Nasir and M. Whaiduzzaman, "Use of Cell Phone Density for Intelligent Transportation Systems(ITS) in in Bangladesh," Journal Of Information Technology, Jahangirnagar University, vol. 1, 2012

[5] Md Whaiduzzaman, M.Sookahak, A.Gani and R.Buyya, “A survey on vehicular c;oud computing” , Journal of network and computer application.

[6] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," Future Generation Computer Systems, vol. 29, pp. 1012-1023, 6// 2013.

[7] Z. Zibin, Z. Yilei, and M. R. Lyu, "CloudRank: A QoS-DrivenComponent Ranking Framework for Cloud Computing," in Reliable Distributed Systems, 2010 29th IEEE Symposium on, 2010, pp. 184-193.

[8] M. Alhamad, T. Dillon, and E. Chang, "SLA-Based Trust Model for Cloud Computing," in Network-Based Information Systems (NBiS), 2010 13th International Conference on, 2010, pp. 321-324.

[9] C. Hoi and C. Trieu, "Ranking and mapping of applications to cloud computing services by SVD," in Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP, 2010, pp. 362-369.

[10] S. K. Garg, S. Versteeg, and R. Buyya, "SMICloud: A Framework for Comparing and Ranking Cloud Services," in Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on, 2011, pp. 210-218.

[11] M. T. Khorshed, A. B. M. S. Ali, and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Future Generation Computer Systems, vol. 28, pp. 833-851, 6// 2012.

[12] R. Buyya, Y. Chee Shin, and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities," in High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on, 2008, pp. 5-13.

[13] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, pp. 599-616, 6// 2009.

[14] A. T. Monfared and M. G. Jaatun, "Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments," in Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on, 2011, pp. 772-777.

[15] J. L. Garcia, R. Langenberg, and N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," presented at the Proceedings of the 2012 ACM Workshop on Cloud computing security workshop, Raleigh, North Carolina, USA, 2012.

[16] S. M. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on, 2011, pp. 933-939