ISSN:0975-9646

Novel Method for Trusted Third Party Security Services for Cloud

Kalyani Madurwar , Prof. Ismail

Department Of Computer Engineering ACEM Pune,
University of Pune, India

***Abstract*—Cloud Computing is a new generation of utility computing and highly growing phenomenon in the present IT industry hype. It leverages low cost investment opportunity for the new business entrepreneur as well as business avenues for cloud service providers. As the number of the new Cloud Service Customer increases, users require a secure, reliable and trustworthy Cloud Service Provider from the market to store confidential data.**

There are number of service providers are available in the market it is a challenge to choose correct service provider so that the data would be securely hosted into the cloud. Here in our work, we are introducing a trustworthy solution to overcome above challenges.

An idea of trusted third party application called as Auditor, which is additional application in between the customer that is client and cloud service providers which is nothing but servers.

Using different attacks e.g. DoS, Brute Force, DSA etc. The auditor will choose the correct and appropriate cloud service providers depending on the security. For monitoring and troubleshooting purpose the logs would be captured to make the solution finer.

***Keywords*—Cloud Security, Cloud Computing, Cloud Service provider, trusted third party, cloud security.**

I. Introduction

Cloud computing [1-4] promises to provide high performance, flexible and yet low cost on demand computing services with the benefits of speed, ease of deployment, scalability and service oriented architecture. It offers a pay-for-use model, for many businesses, especially for startups, small and medium-sized companies, it is extremely attractive; it offers a readily available and scalable computing environment without substantial capital investment and hardware administrative and maintaining cost.

It is a general perception that cloud computing is reminiscent of the application service provider (ASP) and its associated technologies. In practice, cloud computing platform, such as those offered by Amazon Web Services, AT&T’s Synaptic Hosting, and the IBM/Google cloud initiative, works quite differently than the typical ASPs. It provides and supports little more than a collection of physical servers and offers another level of virtualization by providing the users with virtual machines to install and run their own software, instead of owning, maintaining and running the software themselves. With the advance in virtualization technologies, resource availability is typically very elastic and responsive (deploying more physical servers and providing more VMs automatically when needed), with virtually unlimited amount of computing power and storage capacity readily available on demand. With the benefits of cloud computing also come new challenges and complexities such as reliability, security etc. that must be properly addressed. Indeed, not all service providers are created equal, some are superior in computing power, some are good at offering seamless and unlimited storage, and some excel in security management while some offer the lowest cost.

In such a setting, decisions have to be made somewhere as to which applications or fragments of applications from the users are to be executed on which service providers. It is also important to realize that there are different types of users with different types of applications with different set of requirements. Some applications require substantial computing and storage power while others have compelling need for maximum confidentiality. From the users’ perspective, their goal is to run their applications seamlessly and meet their performance, security and cost target. Therefore, matching and determining the best cloud computing service for a specific application is important and often determines the success of the underlying business of the service consumers.

Due to the massive diversity in the available Cloud services, from the customer’s point of view, it has become challenging to select whose services they should use and what is the base of their choice. Presently, there is a lack of frameworks that can permit customers to evaluate Cloud offerings and rank them based on their ability to meet the user’s Quality of Service (QoS) and security requirements. In this work, a secure Cloud service provider ranking system and a mechanism that measure the secured Cloud services are proposed which can make a major impact and will craft a healthy competition among Cloud providers to satisfy their Service Level Agreement (SLA) and improve their QoS and trustworthiness [6]. Hence, we feel strong requirement of a ranking system by which a new cloud customer can identify his/her needs and take the calculated risk of business data before handover to some unknown cloud service provider in cyber space. Our objective is to run the cloud service provider and the new cloud customer and maintain the smooth trust and provide them a tool that can verify and ranked the Cloud service provider. With these ranked results new cloud customers justifies the business needs in terms of security and reliability which cloud service provider is the best option. This ranked system which provided by the trusted third party, will provide more confidence and validity among the cloud market.

New cloud customers can independently make decisions without any cloud broker which is a significant feature of this model. Moreover, making this TPA model more synchronized and robustly in worldwide a TPA monitoring system is proposed that provide higher confidence and wider acceptability of ranking system homogeneously and impartially worldwide. We advocate these proposed tools and model have a viable business needs and the proposed TPA monitoring model is a feasible business solutions model for cloud computing community.

This paper highlights CSP security aspects and how to ensure of these in cloud user's perspective. We propose a conceptual security vulnerability measuring automated model for ranked the cloud provider authenticity and reliability such as issuing certificates which help the new cloud customer to evaluate the best CSP in the market. The conceptual model contains a monitoring of TPA to protect cloud users rights and cloud provider's security. The regions are divided and employed federated monitoring approach globally. Federated TPA monitoring assures the same service and more interoperable among TPA worldwide.

This paper is organized as follows: Section 2 discusses existing system, Section 3 introduces the proposed model with flow charts and block diagram, and explains different attacks and ranking system and finally Section 4 provides the conclusion and section 5 explains the future scope.

II. Existing Systems

A personalized cloud component ranking for different designers of cloud applications, and proposed a QoS driven component ranking framework for cloud applications by taking advantage of the past component usage experiences of different component users. Again several resource provisioning policies can be used to extend the capacity of a local cluster by leveraging external resource providers, as well as reduce the cost by using the Spot Market. Using the indicator as one of the main SLA parameters to determine who is responsible for the violation of the revenue or profit parameters were proposed and explained by M. Alhamad et al. [7]. Proposal of a set of cloud computing specific performance and quality of service (QoS) attributes, an information collection mechanism and the analytic algorithm based on Singular Value Decomposition Technique (SVD) to determine the best service provider for a user application with a specific set of requirements were proposed by H. Chan et al. [8]. The SMICloud model was proposed by S. K. Garg et al. [9] which let users compare different Cloud offerings, according to their priorities and along several dimensions, and select whatever is appropriate to their needs. An analytical Hierarchical Process (AHP) based ranking appliance was proposed which can calculate the Cloud services based on different applications

III. Proposed System

We consider the following scenario for explaining our model. Consider a scenario of a new cloud customer; say a company owner or manager is considering adopting cloud facility for the company. Main priority and mandatory condition is to protect company data security and privacy. The manager can see lots of cloud service provider in the market but not adequate guidelines to adopt the best secured cloud service provider for an organization. New cloud customer needs the security and trust certificate or report of these providers for making a decision to choose the right provider in terms of reliability, security and trustworthiness. So, clearly security issues are the most significant issue which is impeding the growth of cloud computing [10, 11]. However, few ranked systems are available in service provisioning or performance issues but not adequate cloud service provider security ranking system is currently available.

A. *Cloud Service Providers*

The Cloud service providers are the entities who own the cloud infrastructure and provide cloud services for consumers. The design and implementation of cloud provider infrastructure and price models are outside the scope of this paper.

B. *Security Metrics*

To know what to measure, how to measure and communicate those metrics which can help us to improve security's efficiency, effectiveness and standing in the business perspective. The generated metrics will provide an initial baseline to ensure achieving the targeted goals, which will evolve over time according to particular business needs and information security risk aspect..

C. *Attack Vectors*

Attack vectors are normally routes or methods used to get into computer systems, usually for evil purposes. They take advantage of known weak spots to gain entry. Many attack vectors take advantage of the human element in the system, because that's often the weakest link. Mainly, it refers to any methods of attacks chosen by hackers to identify weak points or vulnerability on the client or server end of a network for engineering defects in the user system in order to infect or achieve control over system resources.

In fact, by considering several security issues [12-15] we found obvious to need some sort of monitoring, assurance and trust which not only come from the Cloud Service provider but also from a trusted third party. So, Trusted Third Party and security ensuring features together provide trust among the cloud community as a whole.

D. *Assumptions*

In this conceptual model, several assumptions should be considered as follows:

- Like credit Rating company, TPA must maintain the trust and reliability.
- TPA should have enough resources to provide for processing and executing their own work.
- TPA must be maintained and regulated by strict laws, regulations and transparent policies.
- Both TPA and CSP mutually agree before executing the software penetration test.
- Considered as CSP provide SaaS, PaaS and IaaS of its own.

- TPA is responsible for collecting non measurable metrics from trusted source and processes this information for ranking results.
- A new cloud customer looking for security and trust certificate should pay to the third party to see the ranked Results and use their services

Ranking Algorithm

We provide two algorithms and both are explained here Pseudo code 1 explains the calculating procedure of security metrics S and Pseudo code 2 describes the final calculation of ranking results, R. Figure 2 shows the flow chart of the system

Pseudo code 1: Calculating Security metrics S

```
/* Calculate Security metrics S */
Initially S=0;
/* Negotiate with CSP side from TPA to network and connection setup */
While connection setup =0 do
    connection setup=1;
end;
/* 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 */
While I! = 0 do
    /* Execute the specific software coding to test the strength or defence mechanism of CSP */
    If successful to break the specific security, S=S+1;
    endif ;
end;
/* finally send the Security metrics S to the TPA*/
Send S to TPA
```

Pseudo code 2: Calculating Final Rank R

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

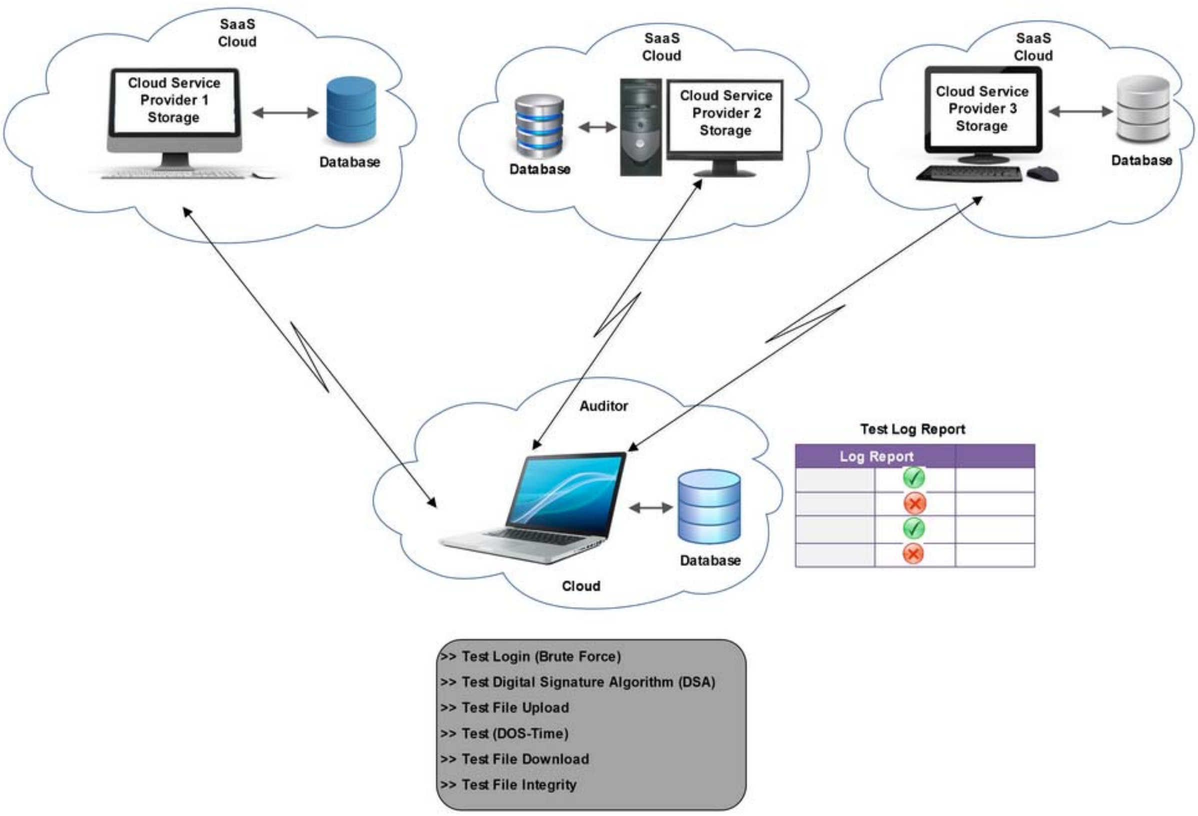

Fig 1 Implementation Model to select Cloud Service Provider

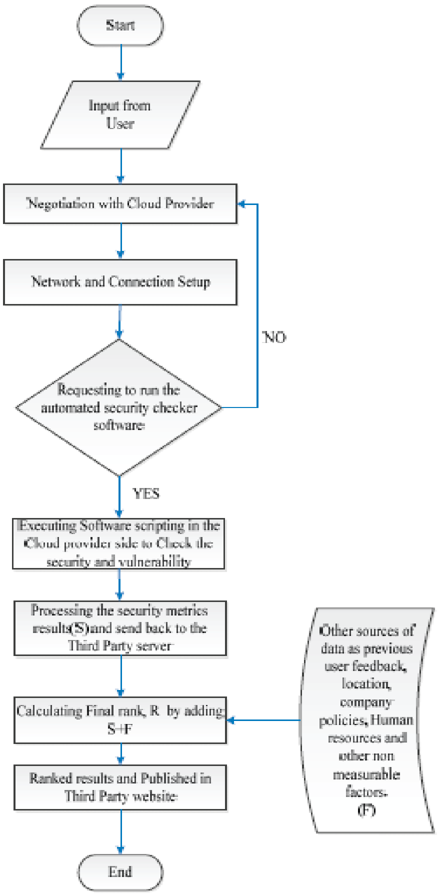
Start
Input from User
Negotiation with Cloud Provider
Network and Connection Setup
Requesting to run the automated security checker software
NO
YES
Executing Software scripting in the Cloud provider side to Check the security and vulnerability
Processing the security metrics results(S)and send back to the Third Party server
Calculating Final rank, R by adding S+F
Ranked results and Published in Third Party website
Other sources of data as previous user feedback, location, company policies, Human resources and other non measurable factors. (F)
End

Figure 2 Security Ranking System Overall Flow

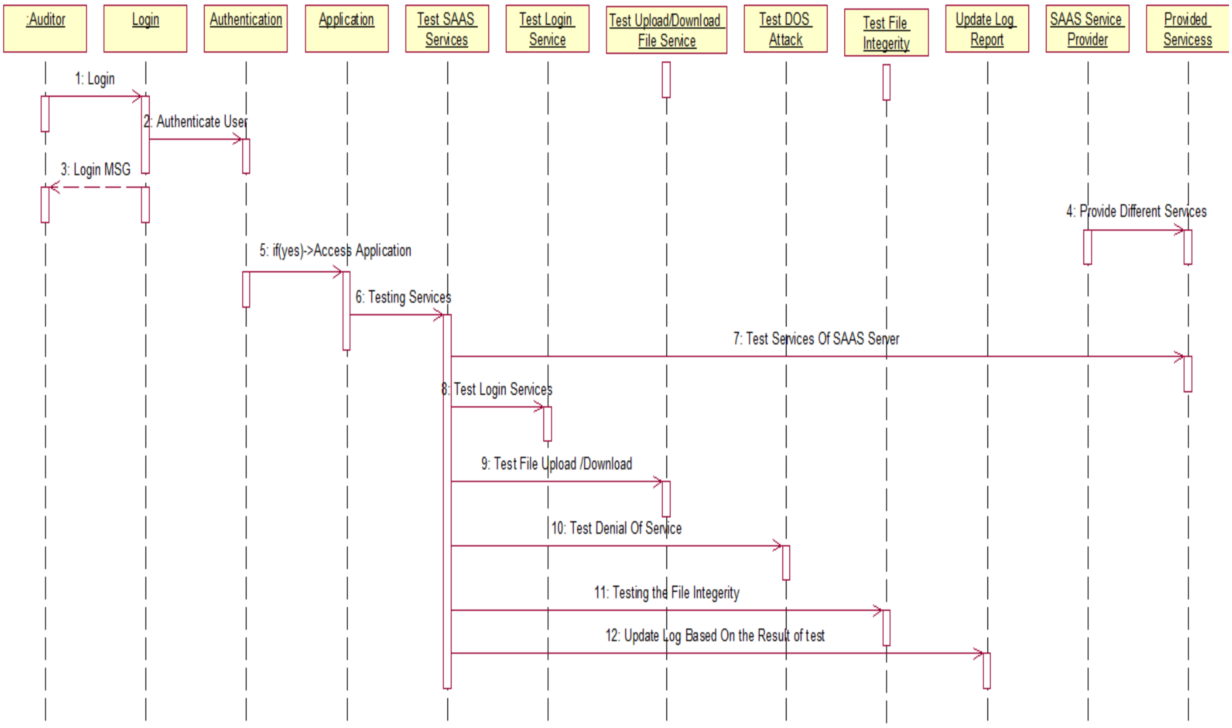
:Auditor
Login
Authentication
Application
Test SAAS Services
Test Login Service
Test Upload/Download File Service
Test DOS Attack
Test File Integerity
Update Log Report
SAAS Service Provider
Provided Servicess
1: Login
2: Authenticate User
3: Login MSG
4: Provide Different Services
5: if(yes)->Access Application
6: Testing Services
7: Test Services Of SAAS Server
8: Test Login Services
9: Test File Upload /Download
10: Test Denial Of Service
11: Testing the File Integerity
12: Update Log Based On the Result of test

Fig 3. Sequence Diagram of Cloud Service Provider Security Checking

IV. ADVANTAGES

In this section, the benefits and advantages of our model are explained.

- Our proposed model provides an easy and convenient way to find a secure CSP by rank system
- The interpretation of ranking system is easy so customer can evaluate the ranked result for TPA website and interpreted themselves
- No need of any brokerage or other help to find desired CSP.
- This rank system conceptually monitored by different layer of supervision and monitoring which ensures the homogeneity of rank system worldwide.
- Unavailability of one TPA will not be a problem since multiple TPAs will work in one region.
- Our proposed model ensures a new customer to adopt best secured cloud from the market.

V. CONCLUSIONS

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.

ACKNOWLEDGMENT

It was very difficult task to finish without help of my guide and College So I am thankful to them and whoever helped me to complete this task.

REFERENCES

[1] [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

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

[3] 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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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