International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

A Novel Approach for Recommendation of Cloud Service for Security using Trusted Third Party.

Shital Sumbe[1], Sujata Jadhav[2], Diksha Bejgam[3] ,Shweta Nhavkar[4] ,M.V.Pawar[5]

[1]Department of Computer Engineering, JSPM's JSCOE, Pune, Maharashtra, India,
[2]Department of Computer Engineering, JSPM's JSCOE, Pune, Maharashtra, India,
[3]Department of Computer Engineering, JSPM's JSCOE, Pune, Maharashtra, India,
[4]Department of Computer Engineering, JSPM's JSCOE, Pune, Maharashtra, India,
[5]Department of Computer Engineering, JSPM's JSCOE, Pune, Maharashtra, India,

---

Abstract - *In present IT industry hype, cloud computing(CC) is the highly growing phenomenon. Cloud computing is now become an essential part of today's competitive market. It leverages low cost investment opportunity for the new business enterprise as well as business avenues for cloud service providers(CSP). In the market As the number of the new cloud customer increases, users require a secure, reliable and trustable cloud service provider from the market to store confidential data. As there is more availability of cloud service provider in the market and the Techniques adopted by these are varying in nature. It is very challenging to measure and analyze the security techniques adopted by them. Therefore to choose right cloud service provider so that the data would be securely hosted into the cloud is also challenging part. These security issues are leads to vulnerabilities. Here in our work, we are introducing a trustworthy model to overcome above challenges. Trusted third party application called as Auditor, which is application in between the client and cloud service providers that test different types of attacks like Denial of Service, Brute Force and different security measures such as data integrity, file upload and download time, digital signature on available cloud service provider. The results will be generated by auditor based on cloud service provider's performance against these attacks and based on that we can recommend secure, reliable and trustworthy cloud service provider to the customer.*

***Key Words*: Cloud Security, Cloud Computing, Cloud Service Provider, Cloud Service Customer, Trusted Third Party.**

1. INTRODUCTION

Cloud computing is now become an essential part of today's competitive market. Many organization makes use of cloud services. There are different cloud service provider available in market. Techniques adopted by these cloud service provider are varying in nature. It is challenging to analyze and measure these security metrics. Low cost and convenience of cloud computing services have changed our daily lives. But the security issues are still associated with cloud computing. With the benefits of cloud computing also come new challenges and complexities such as reliability, security etc. that must be properly addressed. These security issues are leads to vulnerabilities. Hackers apply various techniques to gain unauthorized access to clouds interrupt services on clouds in order to achieve specific goal. Security of a cloud service provider should cover many aspects like authentication, authorization data integrity etc. These are the basic security goals and become essential while moving towards the cloud. There are different cloud service provider available in market. Some offer good computing power, some are superior in offering seamless and unlimited storage, and some are excellent in security management while some offer the lowest cost. Therefore a tool that analyse and evaluates these security metrics with respect to cloud services before selection of cloud service provider is the necessary in the cloud environment. So, here we are focusing on developing an application that focuses on security measures like brute force attack, Dos attack, data integrity, reliability, authentication. There is an auditor in between cloud service provider and cloud customer. Auditor test the cloud service provider against the above security measures and generate the result. These results are nothing but the logs of each available CSP according to its performance against the attacks like brute force attack, dos attack, data integrity, test file upload, test file download, digital signature algorithm. By considering these log files the ranking is given to the cloud service provider according to its overall performance. Cloud service provider which gives best result against the security issues is suggested to the customer who want to buy CSP.

1.2 CLOUD SERVICE MODELS

Cloud computing is classified based on the services offered. According to the different types of services offered, cloud computing consist of three layers those are explain below.

Infrastructure as a Service (*IaaS*): is the lowest layer that provides basic infrastructure service. Infrastructure as a Service *(IaaS)* typically uses virtualization technology. It refers to the sharing of hardware resources for executing services, by using virtualization technology. With IaaS approach, multiple users use available resources. The resources can easily be scaled up depending on the demand of user. These resources are typically charged on a pay-per-use basis.

Software as a Service *(SaaS):* Software as a Service *(SaaS)* is the top most layer which ensures a complete application offered as service on demand. SaaS ensures that complete applications are deployed on the internet and users use them. The payment is made on a pay per-use model. It eliminates the need to install and run the application on the customer's local computer, thus minimizing the customer's burden for software maintenance.

Platform as a Service approach (PaaS): Platform as a Service (*PaaS)* layer is the middle layer, which offers platform oriented services, and providing the environment for hosting user's applications. In the *Platform as a Service approach (PaaS)*, it offers software execution environment. For example, there could be a PaaS application server that enables the developer to deploy web-based applications without buying actual server. Aim of Paas model is to protect data, which is specially important in case of storage as a service. In case of congestion, there is the problem of outage from a cloud environment. Thus the need for security against outage is required to ensure load balanced service. The data needs to be encrypted when store on a platform for security reasons. Cloud computing architectures making use of multiple cryptographic techniques towards providing cryptographic cloud storage have been proposed.

2. CLOUD SECURITY THREATS

Three cloud service models (Software as a service, Platform as a Service and Infrastructure as a Service) provide different types of services to end users nothing but customer also provide information about security issues and risks of cloud computing systems.

First, the hackers use the forceful computing capability provided by clouds by conducting illegal activities. IaaS is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud. It maximizes extensibility for users to customize a "realistic" environment that includes virtual machines running with different operating systems. Hackers could rent the virtual machines, analyze their configurations, find their vulnerabilities, and attack other customers' virtual machines within the same cloud. Infrastructure as a Service also enables hackers to perform attacks, e.g. brute-forcing cracking, that need high computing power. Since Infrastructure as a Service supports multiple virtual machines, it provides an ideal platform for hackers to launch attacks (e.g. distributed denial of service (DDoS) attacks) that require a large number of attacking instances.

Second, an important security risk of cloud models is data loss. In Software as a Service cloud models, companies use applications to process business data and store customers data in the data centers. In Platform as a Service cloud models, developers use data to test software integrity during the system development life cycle (SDLC). In Infrastructure as a Service cloud models, users create new drives on virtual machines and store data on those drives. However, data in all three cloud models can be accessed by unauthorized internal employees, as well as external hackers. The internal employees are able to access data accidently. The external attackers gain access to databases in cloud environments using a range of hacking techniques such as session hijacking and network channel eavesdropping.

Third security threat identified is, Denial of service(DoS) attack is an attempt to interrupt a server or network resource in order to make authorized users unable to access the computer service. They come in different varieties and aim at a variety of services. Generally, they are categorized into three basic types: consumption of scarce, limited, or non-renewable resources, alteration of configuration information, and physical destruction of network components. Among them, flooding is the most common way in which hackers disrupt the authorized user's system with the use of number of forged requests; therefore, the services to authorized users are blocked.

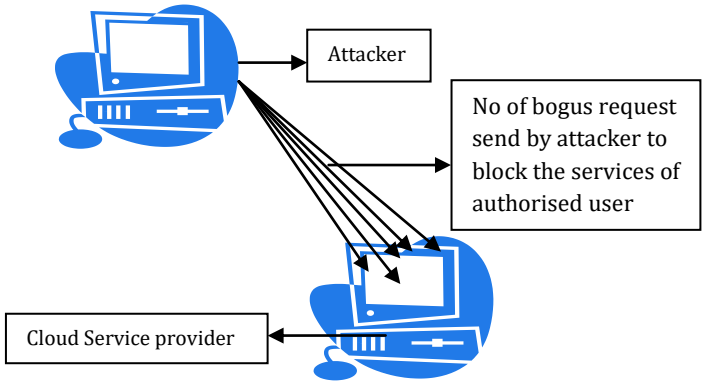


Fig -1: Denial of service attack

service(DoS) is occurred to all requests from authorized users. Moreover, the flood attack could possibly cause indirect DoS to other servers in the same cloud when the servers share the workload of the victim server, which results lack of availability on all of the services. It is necessary to identify the possible cloud threats in order to implement better security mechanisms to protect cloud computing environments.

Brute force attacks work by calculating every possible combination that could make up a password and testing it to see if it is the correct password. As the password's length increases, the amount of time, on average, to find the correct password increases exponentially. That is short passwords can usually be discovered quite quickly, but longer passwords may take decades.

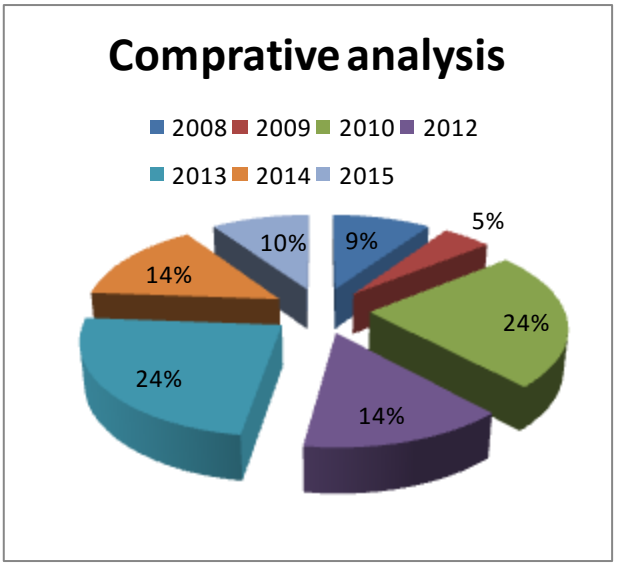


Chart -1: Year wise comparative analysis.

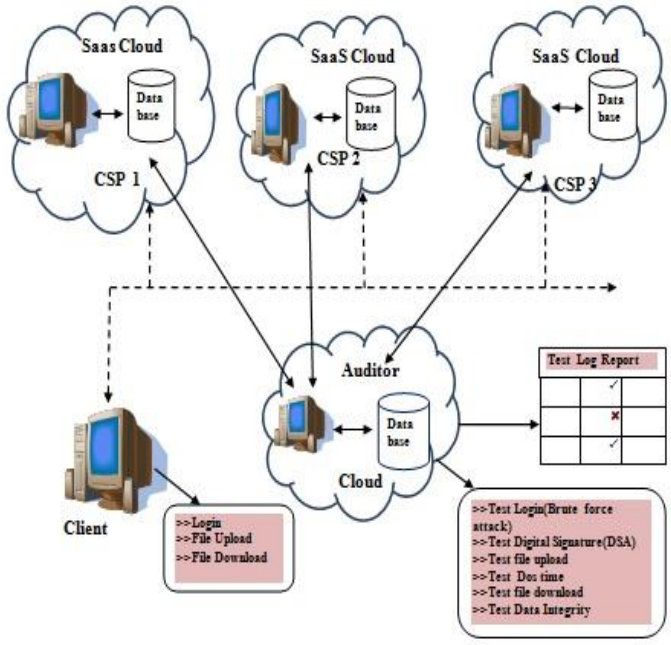
3. COMPARATIVE STUDY

Citation	Paper Name	Security issues covered	Year
Rizwana Shaikha, Dr. M. Sasikumar.	Trust Model for Measuring Security Strength of Cloud Computing Service.	1.Authentiction 2.Data Confidentiality	2015
Poonam Yadav, and Sujata.	Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA.	1.DDOS	2013
Dhaval Patel, M.B.Chaudhari.	Data security in cloud computing using digital signature.	1.Data integrity 2.Authentication 3.Confidentiality	2014
Dr.V.Venkatesa Kumar, M.Nithya.	Improving security issues and security attacks in cloud computing.	1.DOS 2. Data integrity 3.Data loss	2014
Smita Parte, Noumita Dehariya.	Cloud Computing: Issues Regarding Security, Applications and Mobile Cloud Computing.	1.Dos	2015
T. Sivasakthi and Dr. N Prabakaran.	Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing.	Digital signature Algorithm (SHA)	2014

4. EXISTING SYSTEM

In existing work, Cloud Service Provider side security issues and tolerance of security strength is identified by applying and introducing 'Trusted third party(TTP)' which provide us CSP ranking system. Using different types of attack vectors to protect and ensure customer interest and confidence by providing security ranking systems to select secure CSP is the first time in Mobile cloud computing(MCC). First, TTP uses automated software scripting to check security and vulnerabilities in CSP side by running software scripting to break the security strength of the CSP. Thus, considering several non-measurable metrics such as customer satisfaction, previous down time, location etc. factors, TTP announce a secured CSP ranked system in their website.

5. PROPOSED SYSTEM ARCHITECTURE



In existing system ranking of the Cloud Service Provider(CSP) based on few security measures so here we are introducing a system that can rank the cloud service provider based security issues like brute force attack, denial of service attack, data integrity, file upload and download time.

The architecture of system consist of three Cloud Service Provider(CSP), client , auditor.

Client: At client side, User does login by using username and password. Then User perform test file upload and test file download activities.Here first user does login at client side. After login user check the server performance against dos attack, brute force attack, file integrity, how much time is required for test file upload and download activities.

Auditor: Auditor is Trusted Third Party(TTP) that resides in between client and CSP. Auditor is work as a tester that test the cloud service provider by performing different types of attack on CSP's. Auditor will measure the performance of all three cloud service provider against brute force attack, denial of service attack file integrity, file upload/download. Then at auditor side the log file is generated that is nothing but the results of performance of all cloud service provider. This log file is useful to decide which Cloud Service Provider is secure, reliable and trustworthy.

5.1 ALGORITHMS USED

5.1.1 Digital Signature Algorithm:

Digital signature are used for authentication purpose. Digital signatures are used when user does login into the system and try to upload file to the CSP, at this time digital signature is attach with that file. If any unauthorized user want to download that file the digital signature algorithm first check the digital signature previously attach with the file and the digital signature while downloading the file. if it is not match it will not give permission to download the file. Digital signature is used for data integrity purpose. For digital signature hashing algorithm that is SHA-1 is used.

5.1.1 Secure Hash Algorithm:

The SHA1 encryption algorithm specifies a Secure Hash Algorithm (SHA1), which is used to generate a representation of a message called a message digest. The SHA1 is required to use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required. SHA1 is used for computing representation of a message or a data file. When a message of any length <

2^64 bits is input, the SHA1 produces a 160-bit output called a message digest. The message digest can then be input to the Digital Signature Algorithm (DSA), which generates or verifies the signature for the message. Signing the message digest rather than the message improves the efficiency of the process because the message digest is usually much smaller in size than the message. In proposed system SHA 1 is also used for data integrity purpose.

6. RESULTS

There are three cloud service provider. These cloud service provider are tested based on security measures such as:
1.Test login(Brute force attack)
2. Test digital signature
3. Test file upload
4.Test file download
5. Test dos time.
6.Test file integrity
all these tests are perform by auditor(TTP).
The results of all these test are shown in below table.

Security parameters	CSP 1	CSP 2	CSP 3
Test login(Brute force attack)	Access denied. when more than three times user enter the wrong password	Access denied when more than ten times user enter the wrong password	It will give access to the attacker if he enter wrong password more than twenty times.
Security	Secure	Less secure than CSP1	Not secure any more

Table-1: Test login(Brute force attack).

Parameters	File Size	Time
File upload/download	6 KB	1sec
File upload/download	11 KB	2-3sec
File upload/download	120 KB	15 sec
File upload/download	3 MB	9 min

Table-2: Test file upload/Download

Parameter	CSP 1	CSP 2	CSP 3
File integrity	upload in auditor data table(file intact)	Save File in partitions in auditor partition table.(file intact)	Save File in partitions in auditor partition table.(will show damage to file since SHA does not match)
Result	Secure	less secure than CSP 1	not secure

Table-3: Test File Integrity

Parameter	CSP 1	CSP 2	CSP 3
Dos time detection	1.After 20 requests robot detection.	1.After 40 requests robot detection.	1.Request accepted
Result	Secure	Less secure than CSP1	Not Secure

Table-3: Test Dos time

On the basis of these results cloud service provider1 is the most secure, reliable and trustworthy cloud service provider among all CSP's. So based on these results we can recommend best CSP to the customer who want to buy cloud service.

6.1 GRAPHICAL ANALYSIS OF RESULT

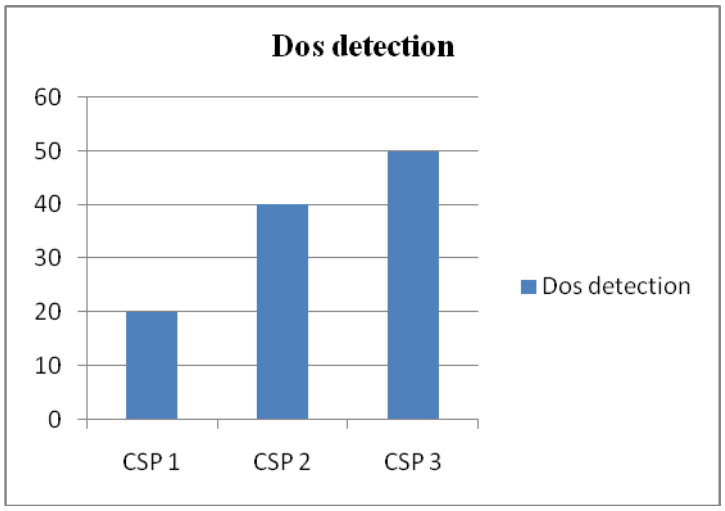


Chart-2: Dos attack detection by CSP's

CSP 1 gives better performance against denial of service attack. It recognize that user is sending forged request to fill up the server and after 20 request it will denied that user's access to the CSP1.CSP 2 will give less better performance than CSP 1 because it recognizes the dos attack after 40 forged request. After that it will denied user access to the CSP 2.CSP 3 is not secure any more because after 50 request it will give access to the user to access services of CSP 3.

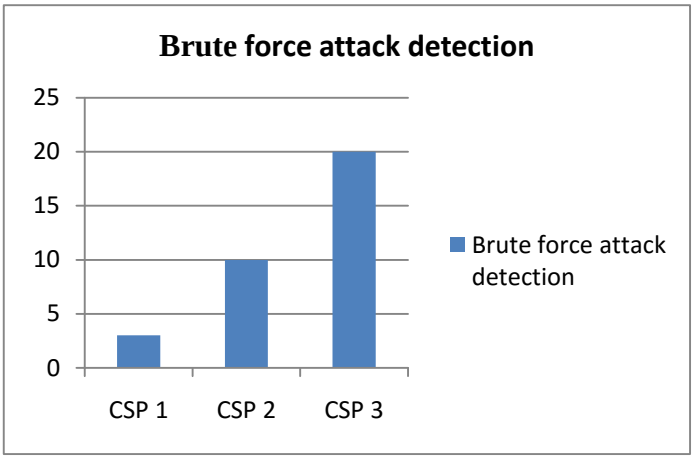


Chart-3: Brute force attack detection by CSP's

In brute force attack detection CSP1 Will give 3 chances to the user to try password and after that it will denied access.CSP 2 will give 10 chances to the user to try the password and after that access is denied.CSP 3 will give access to the unauthorized user if he tries password more than 20 times.

7. CONCLUSION

In this paper we are measuring the security of cloud service provider and Cloud service recommendation model offers significant performance gain for increasing response time and because of this cost is also reduced under dynamic workload. Performance of system is reliable, scalable. Identification of CSP side security issues and tolerance of security strength is done, that provide CSP ranking system. Using different types of 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. Therefore, considering several non-measurable metrics such as customer satisfaction, Security, availability factors, CSP ranking will be done.There are multiple cloud service provider available. But when people want to buy cloud service provider they are confused. Because there is no ranking system available that can rank the CSP according to performance, security reliability , data integrity. So we are introducing the system that rank the cloud service provider based on major security issues like dos time, brute force attack, file upload, file download, digital signature, Data integrity. According to these security measures our application gives ranking to the CSP and recommend the best CSP to the customer.

Acknowledgement

This work is supported by JSPM‟s Jayawantrao Sawant College of Engineering, Pune Maharashtra. First and foremost, we would like to thank our guide Prof. M.V. Pawar. Providing us with their invaluable support, motivation, suggestion and guidance throughout the course of the paper. We would like to express our gratitude towards Prof. A. S. Devare whose support and consideration has been a valuable asset during course of this paper. We convey our gratitude to our respected head of department, Prof. H. A. Hingoliwala for his motivations and guidance throughout the work. And, last but not least we would like to thank Principal Dr. M. G. Jadhav for directly and indirectly help us for this work.

REFERENCES

[1] Shital Sumbe, Sujata Jadhav, M.V.Pawar," A Survey of Modern Approach for Cloud Service Recommendation based on Security.", International Journal of Computer Applications (0975 – 8887) Volume 129 – No.6, November 2015.

[2] Md Whaiduzzaman, Abdullah Gani “Measuring Security for Cloud Service Provider: A Third Party Approach.” International Conference on Electrical Information and Communication technology(EICT),2013.

[3] Rizwana Shaikh, Dr. M. Sasikumar,"Trust Model for Measuring Security Strength of Cloud Computing Service", International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

[4] Poonam Yadav, and Sujata," Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA",International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.3, June 2013.

[5] Dhaval Patel,M.B.Chaudhari.," Data security in cloud computing using digital signature ", International

Journal For Technological Research In Engineering Volume 1, Issue 10, June-2014.

[6] Dr.V.Venkatesa Kumar, M.Nithya, "Improving security issues and security attacks in cloud computing.", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 10, October 2014.

[7] T. Sivasakthi1,Dr. N Prabakaran, "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing",International Journal of Innovative Research in Computer and Communication Engineering *(An ISO 3297: 2007 Certified Organization)*Vol. 2, Issue 2, February 2014.

[8] S. Venugopal, X. Chu, and R. Buyya, "A Negotiation Mechanism for Advance Resource Reservation using the Alternate Offers Protocol", Proceedings of the 16th International Workshop on Quality of Service, IWQoS‟08 .

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

[10] M. Alhamand, T. Dillon and E. Chang." SLA- Based Trust Model for cloud computing," in Network-Based information Systems (NBiS), 2010 13th International conferences on 2010, pp. 321-324.

[11] IEEE Computer Society, Enschede, Netherlands, 2008, pp. 40–49.Zibinzheng, Yeleizhang and Michael R.lyu, "Cloud Rank: A QoS driven component framework ranking for cloud computing", 2010 29th IEEE International Symposium on Reliable Distributed System.

[12] Geoff Skinner , Rukshan Athauda " A Holistic Review on Trust and Reputation Management System fir Digital Environments" in International journal of computer and information Techology (2277- 0764),september2012.

[13] M. Whaiduzzaman M. Sookhak, A. Gani, and Buyya "A survey on vehicular cloud computing." Journal of Network and Computer Applications August 2013.

[14] 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.

[15] Abolfazli S, Sanaei Z, Ahmed E, Gani A, Buyya R "Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges. In: IEEE Communication Surveys and Tutorials," June 2013.

[16] 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 System, vol. 28, pp. 833-851, 6// 2012.

[17] R. Buyya, C.S. Yeo, S. Venugopal, "Market-oriented cloud computing: vision, hype, and reality for delivering it services as computing utilities," 2008.

[18] R. Buyya, R. Ranjan and R. N. Calheiros, "Inter Cloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services", in : Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing, ICA3PP‟10, Springer, Busan, South Korea, 2010, pp. 13–31.

[19] Rodrigo N. Calheiros, Adel Nadjaran Toosi, Christian Vecchiola and Rajkumar Buyya, "A coordinator for scaling elastic applications across multiple clouds", Future Generation Computer Systems, Volume 28, No. 8,Pages: 1350-1362, ISSN: 0167-739X, Elsevier Science, Amsterdam, The Netherlands, October 2012.

[20] Rohit Bhadauria, Sugata Sanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques."