

Making a Cloud Data Secure and Effective for Better Performance of Services

Sangeet Mishra¹, Asis Kumar Tripathy², Pallavi Joshi³

^{1,2}School of Information Technology and Engineering

³School of Electronics Engineering
VIT UNIVERSITY

*Corresponding author, e-mail: ¹Sangeet.mishra8@gmail.com, ²asistripathy@vit.ac.in,
³pallavi.white@gmail.com

Abstract

Cloud data security is one of the major and crucial concerns in everyday life. Now a days cloud computing is emerging as vast and fastest growing technology depending on the usage. Cloud computing does not allow to keep data at user site and thus a data security is concerned to be a major challenging task regarding data storage. This paper overall describes the monitoring of the cloud data concerning data storage. In this paper we proposed a new methodology that can efficiently managed the security to the data and provide privacy to the consumer using the services of the cloud. Our proposed technique provides data security by using the third party monitoring system which acts as an interface between the cloud consumer and cloud owner. Basically third party monitors the each and every activity of the cloud consumer and based upon his performance he respond to the cloud owner for taking decision. Our proposed concept provides the security from consumer point of view and owner side of view making the flexibility to the cloud infrastructure. Existing works focus mainly on security from owner side of view that not well fitted into the lifecycle of data security.

Keywords: cloud computing; monitoring; privacy; cloud consumer; cloud owner; cloud infrastructure

Copyright © 2016 Institute of Advanced Engineering and Science. All rights reserved.

1. Introduction

Cloud computing is the latest and fastest emerging technology. The usage of this technology mainly depends upon the activities performed by the cloud consumer. Basically we followed the PaaS (Platform as a service) model, so we can monitor overall performance of cloud activities. As there are more advantages of cloud computing [1] but in spite of that the main challenge faced by the cloud computing is lack of information security, as Figure 1. Private cloud is not better in comparison to the public cloud. In Private cloud the consumer and data owner are identical, so they have full control over the physical resources and also they can install monitoring agents inside physical machine to collect complete necessary information. Whereas in public cloud, the consumer is different and owner is different; thus the owner cannot do anything in consumer virtual machine. The existing [2] system does not completely fit into the life cycle of data security. However the contribution of the existing system does not solve consumer's problem. Now we introduce the successive step concerning the field of monitoring, henceforth called MPCA (Monitoring performance of cloud activities). Cloud computing involves sharing of computing resources [3] instead of using local servers to execute application. Cloud is classified on the basis of their location and their types. Based on the location they are public cloud, private cloud and hybrid cloud. Based on their types they are Infrastructure as a services, Platform as a services and Software as a services. The main advantage of using public cloud is that customer has not the not control authority over the cloud computing infrastructure and thus it can be shared between anyone. Various technologies [4] such as virtualization, utility computing, load balancing makes the cloud computing objective to be achieved successfully. Instead of many advantages of cloud computing there are few serious problem against it such as data integrity, data privacy and data security for using the cloud in vast aspect. Internet is one of the technology consist [5] of group of followed on the concept of cloud computing. In now a days user need licensed software to work. This made a user to be heavily restricted on configuration of software and hardware of system on which this software will be installed. Cloud computing [6] has been evolved for solving all these issue. The main objective of this paper to

provide security to the data stored in cloud database from security threats issue related to cloud. This paper uses an additional monitoring system which acts as an interface between cloud consumer and cloud owner. This new proposed concept has the extra feature to block the consumer account on doing wrong activity.



Figure 1. Issues related to cloud security

This paper [7] overall describes the monitoring of the cloud data concerning data storage. The importance of the paper is to make a secure framework for cloud data security. This new proposed concept has extra feature to block the customer account on doing wrong activity. Basically this module acts as an interface between the owner and consumer. The main objective of this paper to provide security to the data stored in cloud database from security threats issue related to cloud. As in future demands for cloud technology will be increased because of huge spreaded data all around the world. This cannot be assured that this data is definitely secured. So concerning for future reference we proposed the methodology that can be well suited for security of these huge spreaded data. The set of procedures which are discussed in existing concept implies that they are not well suited to the lifecycle of data security. This makes the existing monitoring solution not well suited for cloud infrastructure. Therefore we provide a successive step in this field i.e. data security which provides the platform for the cloud infrastructure to make its services flexibly and efficiently available for the users. The proposed system provides a better and flexible monitoring framework that makes the cloud infrastructure more securable. It provides the monitoring to both i.e. cloud owner and cloud consumer. This provides the cloud consumer a monitoring platform through which he/she can customize the monitoring resources. The proposed system makes the monitoring framework more reliable by allowing third party which overall monitor the activities of cloud owner.

2. Related Work

Jose M Alcaraz Calero et al [1] have discussed about monitoring architecture and its benefits towards cloud data security. They talk about the challenges faced by cloud computing. These challenges should be addressed seriously in order to provide better monitoring solutions. Firstly they provide successive solution corresponding to monitoring platform i.e. IaaSMon (Infrastructure as a service) but this is not well fitted into the data security life cycle. It provides information of infrastructure to owner but does not involve any consumer related information. So they proposed a new scheme concerning monitoring architecture i.e. MonPaaS. It provides monitoring scheme from both the side i.e. owner side as well as consumer side. Lifei Wei et al [8] have work on making the cloud data stable and flexible for its efficient use. They have considered the security feature along with data storage. They have proposed Sec- Cloud framework based on probabilistic sampling technique as well as designated verifier technique.

Basically they focused on divide the data in sample form which are small in size and then distribute it. Thus it does not create overload on server. By this they preserve data storage, computation. Preeti Sirohi et al [4] focus on the encryption and decryption approach facilitating cloud user with data security assurance. The proposed solution talks only about the security of data not concerning about the authentication scheme that can lead to more level of security. A New model for data security in cloud computing environment using the information stated in the previous section is offered. The proposed system uses a three layer system structure in which these layers are used for ensuring data security. The proposed model ensures that protection of the user confidential information by ensuring faster retrieval of the data using security intelligence and advanced security data protection. Jesus Montesa et al. [9] have discussed about monitoring large scale distributed system. Various studies have been made to analyze and discuss about monitoring of distributed system and specifically of cloud computing. This paper focuses on analysis of monitoring system from the cloud provider point of view but not focuses on the need of cloud consumers. Kun Ma et al [10] have discussed about monitoring platform for the cloud infrastructure. As in today's scenario cloud is becoming the necessary part of the organization, Application being deployed on to the cloud has become a major priority. This paper discussed the overall experience with public cloud and so their proposed work is that they have designed the light weight public cloud framework.

3. Methodology

The below given diagram will explain the overall working of the proposed system. The proposed system includes three modules i.e. cloud owner, cloud consumer and third party. First of all the cloud consumer will register on the application deployed in the cloud, then after registering consumer will login on to the application. After successful login cloud consumer will first sent the request to cloud owner. Then after that cloud owner will check that whether he/she got the request from cloud consumer. If he got the cloud owner will generate one public key and one secret key (private key) for cloud consumer. By using that key consumer will encrypt their data which he wants to be uploaded in cloud database. After this when consumer wants his/her data from the cloud database, the cloud owner will provide the task to cloud consumer. After doing the task, third party which acts as an interface between cloud owner and cloud consumer will match the information filled out by consumer during the task completion. If he got right details then consumer will able to use the services of cloud or else third party will directly inform to the owner that the particular consumer is doing wrong something and simultaneously the cloud owner will generate a warning message to the consumer that you can fill the wrong details only three times after that your account will be disabled. This way our proposed system will provide security (Figure 2).

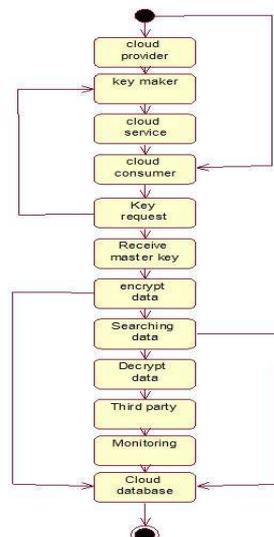


Figure 2. Flow diagram of the system

4. Previous System

They basically focus on the monitoring frame-work which resolves the issues faced by IaaSMon. In the previous system security is not being provided upto the standard being accepted in data security life cycle. In the existing system security is being provided from the owner point of view and consumer point of view. The owner is self-monitoring authority. Only monitoring from authentication point of view has been done in existing system but that is not well enough for security purpose. Existing system is basically based on monitoring agents installed inside the machine to gather information. These facts make the traditional monitoring solutions not fit for cloud infrastructures. So we proposed a successive step i.e. called MPCA (Monitoring performance of cloud activities) which perfectly removes the issues faced by existing system. The drawbacks of previous system are as follows:

- We can't monitoring the cloud storage
- We can't find out the authorization

5. Proposed System

The proposed system provides a better and flexible monitoring framework that makes the cloud infrastructure more securable. It provides the monitoring to both i.e. cloud owner and cloud consumer. This provides the cloud consumer a monitoring platform through which he/she can customize the monitoring resources. The proposed system makes the monitoring framework more reliable by allowing third party which overall monitor the activities of cloud owner. The advantages of proposed scheme are as follows:

- We can monitoring the cloud storage
- Can find out the authorization

Proposed algorithm:

Step 1: Create an VM (virtual machine)

Step 2: Until "done"

- Distribute the files or data's (MPCA)
- Distribute Mon pass to the Nagios(recombination)
- Monitoring the metrics (mutation)
- VM for Tenant Monitoring does not exit
- Wait until Mon ready configuration access

In the proposed framework monitoring feature is much powerful than existing system so that no user even registered also can harm the cloud infrastructure. Here both i.e. cloud provider and third party are keeping eye contact on all the activities done by consumer. In this system we created three warnings for the consumer doing wrong activities. After third warning also, if he is doing wrong activities his account can be blocked or might be deleted from registered user list.

6. System Architecture

The users or nodes involved in our projects are sender, intermediate and receiver, as Figure 3. In order to send file, the sender has to find out the list of nodes which are connected with the sender. From that available list he can choose receiver. Then the sender has to analyze the performance of each and every node which is connected with the sender. The performance analysis list will return the priority based result so that sender can choose the intermediate to send the file. The Intermediate will receive the file from sender then it will analyze the performance so that it can send data to another intermediate or receiver. In the receiver side, the receiver has to select the file path to receive the file from sender or intermediate. Then the receiver can view the file received file.

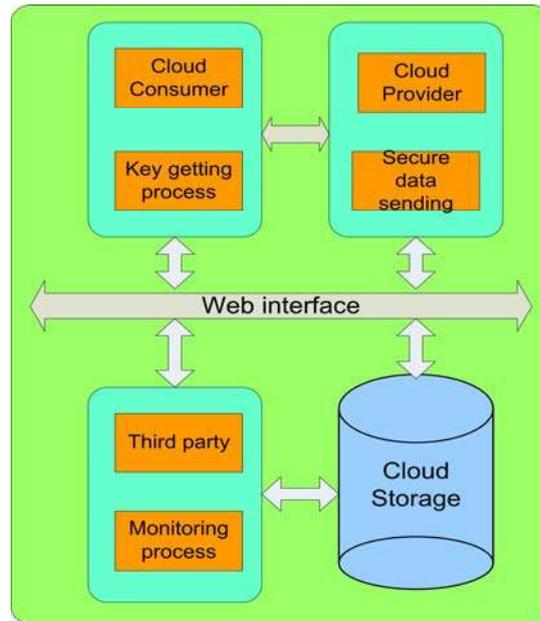


Figure 3. Overall System Architecture

7. Software specification

This is about the software language and the tools used in the development of the project. The platform used here is .NET. The Primary languages are C#, VB, and J#. In this project C# is chosen for implementation. Basically we have worked .NET platform which gives look and feel to the application. .NET has built in components which provide the user to directly use them and build a simple user interface application. We have used ASP.NET with visual c# for front end designing and SQL Server for back end designing. When we developed the web application so one necessary thing we have to kept in our mind while developing i.e. how to store data which are being used by web services in order to operate efficiently.

8. Result and discussion

In previous researches concerning cloud data security there was no provision of making the cloud secure from consumer point of view, it was giving the security only for cloud provider(owner).Also the existing system lacks the alert system(message alert system). But this new system developed in this project has got all the above mentioned features that is now the cloud data is secured both for owner as well as consumer. The Table 1 below shows the comparison for monitoring time for registering the consumer T time interval of 24 seconds for both the existing system and the presently implemented system, Figure 4 refers to this-

Table 1. Comparison between two systems for registering tenants for 24 sec time interval

S No.	No. of tenants	For Existing system	For present system
1	1	20	28
2	2	31	32
3	4	41	38
4	8	80	90

Similarly other figures like Figures 6,7,8 are showing the tenant and Admin time for registrations for different number of tenants and at different intervals and different monitoring times for 25, 26, 27 seconds etc. Basically the results have slight fluctuation between the performances of cloud services for owner as well as customer sites w.r.t time. Ping Time is the amount of time taken for the first request being responded by virtual machine. In Figure 4,

Figure 7 the overall performance of monitoring time is not in linear manner. In Figure 5 the overall performance is being shown in curve form increasing in parallel manner. In Figure 6 the overall performance is being increased in parallel and linear manner.

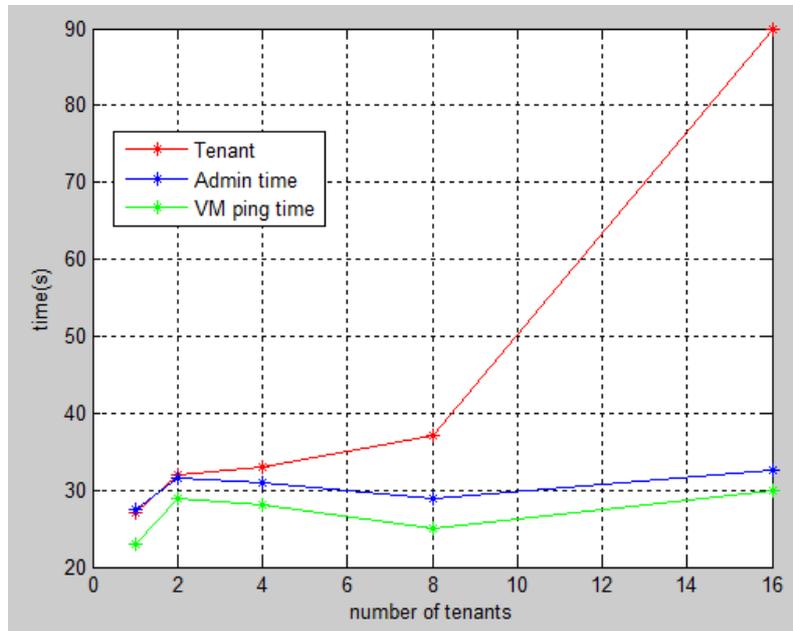


Figure 4. Monitoring time for 24 seconds of time interval

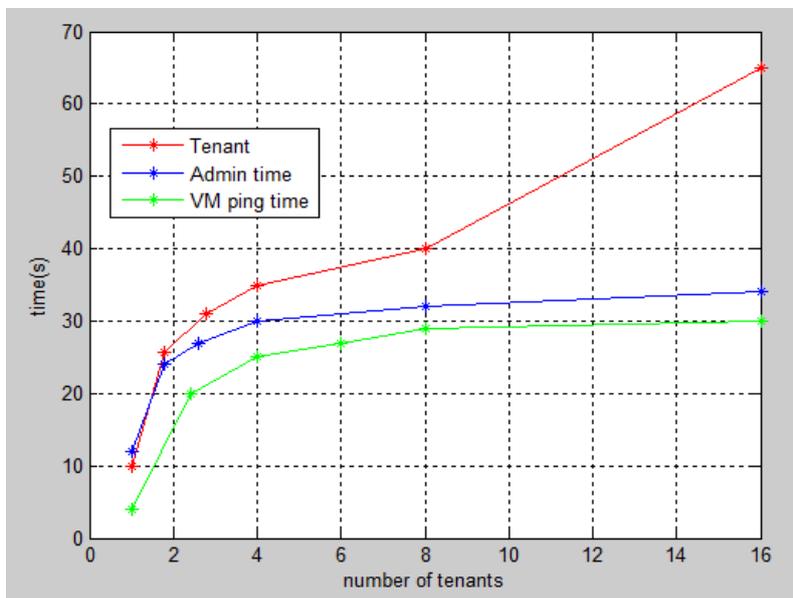


Figure 5. Monitoring time for 25 seconds of time interval

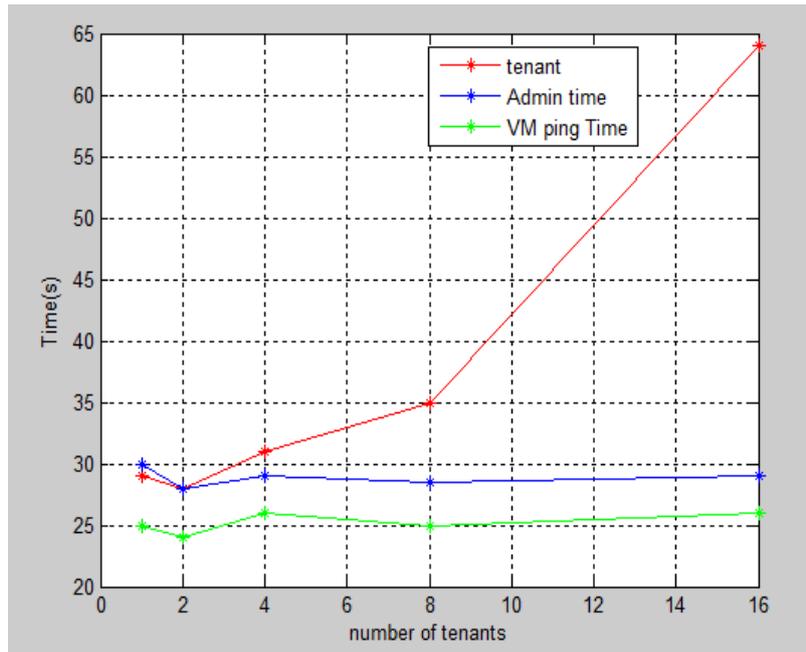


Figure 6. Monitoring time for 26 seconds of time

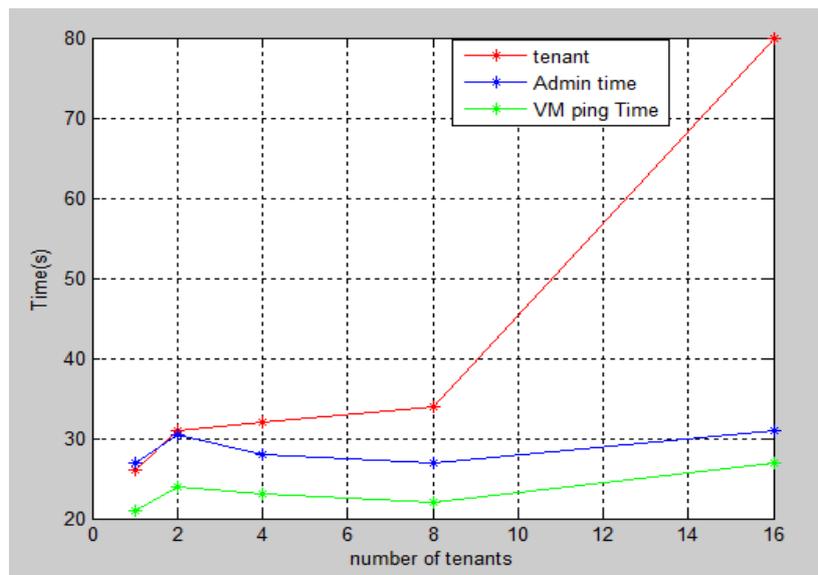


Figure 7. Monitoring time for 27 seconds of time interval

9. Conclusion

A distributed and flexible monitoring framework has been provided to the cloud community. Under the different stressing workload condition this monitoring architecture performs really well. In this paper we also introduce the concept of third party monitoring system who overall monitor the entire cloud activities done by user especially cloud consumer. The proposed framework gives the adaptability to the cloud administrations and cloud assets offered to the client. Our future work will focus on the model and methodology that will work much well even in workload condition. We might want to augment the observing engineering utilizing workload adjusting capacities for the checking administrations of the cloud shopper too. In future

we will utilize load adjusting strategy to maintain a strategic distance from the heap on server for assigning assets.

References

- [1] Jose M Alcaraz Calero, et al. "MonPaaS: An Adaptive Monitoring Platform as a Service for Cloud Computing Infrastructures and Services". *IEEE Transaction on service computing*. 2015; 8(1).
- [2] Louai A Maghrabi. "The Threats of Data Security over the Cloud as Perceived by Experts and University Students". 978-1-4799-2806-4/14/\$31.00 ©2014 IEEE.
- [3] Mr Krunal Patel, et al. "Data Security and Privacy using Data Partition and Centric key management in Cloud". *ICICES2014 publication journal*, ISBN No. 978-1-4799-3834-6/14.
- [4] Lifei We, et al. "*Sec Cloud: Bridging Secure Storage and Computation in Cloud*". IEEE 30th International Conference on Distributed Computing Systems Workshops. 2010.
- [5] Cong Wang, et al. "*Towards Secure and Effective Utilization over Encrypted Cloud Data*". 31st International Conference on Distributed Computing Systems Workshops. 2011.
- [6] Louai A Maghrabi. "The Threats of Data Security over the Cloud as Perceived by Experts and University Students". 978-1-4799-2806-4/14/\$31.00 ©2014 IEEE.
- [7] Gaurav Garkoti, et al. "Detection of Insider Attacks in Cloud based e-Healthcare Environment". 2014 *International Conference on Information Technology*. 978-1-4799-8084-0/14 \$31.00 © 2014 IEEE DOI 10.1109/ICIT.2014.43.
- [8] Afzaal Ahmad, et al. "Ensuring Data Security and Privacy in Cloud Computing through Transparency as Service Model". 2014 *IJ-CLOSER*. 2014; 3(5): 253-259.
- [9] Mr Krunal Patel, et al. "Data Security and Privacy using Data Partition and Centric key management in Cloud". *ICICES 2014 publication journal*, ISBN No. 978-1-4799-3834-6/14.
- [10] Devki Gaurav Pal. "A Novel Open Security Framework for Cloud Computing". *IJ-CLOSER*. 2012; 1(2): 45-52.