International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com
ISSN No: 2456 - 6470 | Volume - 2 | Issue – 6 | Sep – Oct 2018

Cloud Intrusion and Autonomic Management in Autonomic Cloud Computing

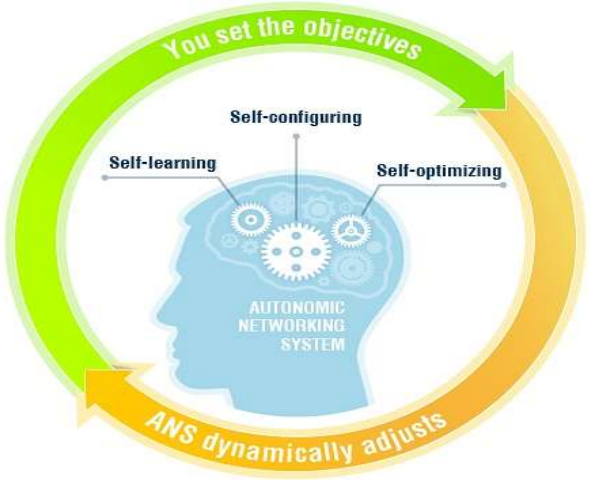
Bilal Hussain CH
Research Scholar, Department of Computer Science and Engineering,
University of Engineering & Technology, Lahore, Pakistan

ABSTRACT
Autonomic cloud emerge as a result of emerging four properties of autonomic computing in cloud that are self-healing, self-monitoring, self-repairing and self-optimization.

We have defined a methodology to improve the security in cloud computing and also defined a methodology that can ensure the autonomic management in autonomic cloud computing. We have selected 1 of the 7 properties of the autonomic cloud computing that is autonomic management. Our main focus is on the security enhancement and avoidance of cloud intrusion in autonomic cloud computing.

Keyword: *Autonomic cloud computing, cloud intrusion, autonomic management.*

I. INTRODUCTION
Autonomic computing refers to the term in which the system would be able to self-monitor, self -repair, and self-optimize itself. Autonomic cloud computing are the systems that have the ability to adapt themselves to the changes in their working environment and thus maintaining the service level agreement (SLA).



Autonomic cloud computing has the basic four properties self-healing, self-optimization, self-repairing and self-monitoring.

There are about 6 basic fields in the autonomic cloud computing that are:-
- Application scheduler
- Energy efficient scheduler
- Security and attack detection
- Dynamic resource provisioning
- Cloud workflow
- Autonomic management

Out of all these fields we have selected autonomic management for our research paper.

Our proposed methodology is that we have redefined the structure in the cloud computing. We are introducing a layer in the structure of cloud computing. This layer or portion will have some necessary and vital importance. The layer introduced by us has the library that has the routines of the various viruses, Trojans, worms and other hacking and intrusion tools.

Our methodology has three basic phases;-

Detection phase:-

In this phase the layer or the portion will detect that the incoming request that is requested by the user is either a virus, a worm, a hacking technique or a legitimate request.

If the request if legitimate the system will allow the request and pass it to the next level. And if the request is not legitimate the request will be discarded. The routine of the incoming request is checked with the routines saved in the library of the layer or the

portion. This way it is checked that the request is legitimate or not.

Prioritization phase:-
In this phase the request that is considered not legitimate and is considered a threat will be prioritize from the number 1 to 10.

The number is assigned by the severity of the attack. The greater the effect of the attack the higher the number it will get. A back end algorithm will be written that will check the severity of the attack on the cloud system.

It will senses the points where the attack is placed and after that a number is assigned to the attack and prioritizes it.

Implementation phase:-
In this phase the implementation to reduce and nullify the attack is done.

In this phase first the experts are informed by the nature of the attack. After that our algorithm comes in to the action. Various activities are done according to the nature and the severity of the attack that we will explain latter. Besides all this work the proceedings will be saved for the future use. And can be used as an evidence against the intruder or attacker.

CLOUD COMPUTING ARCHITECTURE:-
The major providers of the cloud are providing their resources i.e. software as a service, infrastructure as a service and platform as a service to the customers and consumers over the internet. The major providers include Amazon, Google, yahoo, Microsoft.

The services provided by the cloud are mainly platform as a service software as a service and a infrastructure as a service.

The three main services are discussed below:-
Software as a service:-
In this type of service the cloud provides the users ability to use the software that basically owned by the cloud. There are many instances of the software and the end users and consumers uses the instance of the software.

The main example of the software as a service is salesforce.com

Platform as a service:-
In this type of the service the cloud provides the user's ability to program their own software. The cloud provides the users the software to carry out their instructions and execute them. In this type the consumer can make the program according to the software provided by the cloud.

For example some clouds give the users platform for the development of software only in C# or only in java or only in C or assembly. There are different platforms provided by different cloud companies.

Infrastructure as a service (IaaS):-

Infrastructure as a service provides the user ability to store and compute capabilities over the network. Different type of routers, switches hard drives, servers are pooled together and made available to the users so the users can use them on pay as you go services. This is the most expensive and difficult type of service that is provided to users by the cloud.

Explained view of our methodology:-
As in the introduction we have given you the idea that how our system works. Now we will elaborate the whole idea.

Our defined methodology consists of three phases:-

Detection phase:-

This is the first phase in which the request that is submitted by the user is checked whether the request is authorized and legal or not. For this we have designed a layer which has the routines of the viruses, worms, Trojans and other hacking tools. The routine of the request is checked by the routine saved in the library of the layer. The library of the layer will be enhanced with the more new routines of viruses and worms and Trojans.

In this phase after checking that the request is legal or not some steps are implemented. If the request is legal the system will pass the request and the desired functionality will be performed. And if the request is considered illegal the layer will pass the request to the next phase.

Prioritization phase:-

In this phase the request that is considered as illegal is given the number according to its severity. The severity of the attack is judged by the mechanism that we will define now.

First the intensity of the attack is checked. The system will sense the places where the attacked has affected the cloud. The points where the attacks is placed are counted and the severity of the attack at each point is figured. After this, the attack will be given a number means it is prioritized. The attack will be prioritized with the suitable number for the numbers 1 to 10.

1being the lightest attack and the 10being the most severe attack.

Implementation phase:-

In this phase various steps are performed to nullify and to reduce the effect of the attack.

In this phase the experts are reported about the attack. A report will be generated that will inform the experts about the nature of the attack. After the experts the main algorithms come in to the action.

According to the priority number that is given to the attack various actions are performed.

We will deal three types of cases in this phase.

Case 1:

In this attacks will be placed that have the priority number from 1 to 3. These types to attacks will be considered mild. For such type of attacks the system will automatically heal itself and the ordinary working of the cloud will not be disturbed.

The system will senses the points where the healing is required and the action is done without effecting the normal routine of the system.

Case 2:

In this more severe attacks are placed. The actions performed against this type of actions are more powerful and costly.

The attacks with the severity from range of 4 to 7 are placed. In this case the portion of the cloud on which the attack has taken place will be placed in a black box. The normal execution of the working of the specific portion will be stopped for the specific period of time. The system will try to nullify the attack and to reduce the effect of the attack, until then the normal working of the cloud will be paused and the users wouldn't be able to access the specific portion of the cloud.

Case 3:

In this phase most severe attacks will be placed. The attacks with the severity level of 7 to 10 are grouped together in this phase.

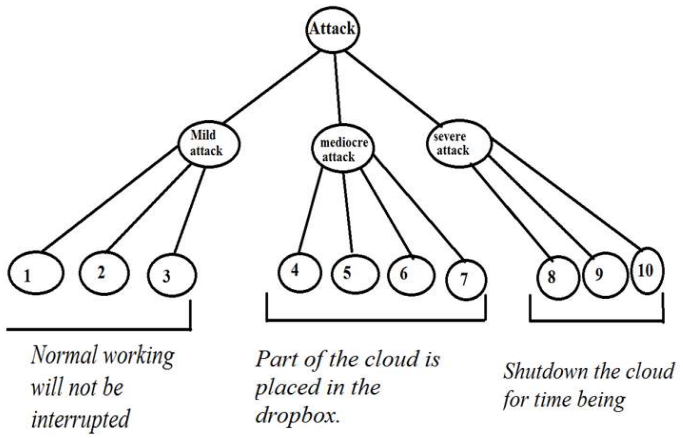
In this case the whole cloud will be forced to stop its normal execution until the attack is nullified.

The user cannot access the cloud during this time. And this is the worst condition for us.

In all three cases first it is decided whether to track the intruder or attacker or not.

An algorithm is also written for this step. If the user is in the cloud and your authorized user and is trying to access other user account or trying to damage the cloud the user will be tracked and the services will be revoked from the user and will be charged with the guilty.

And if the attacker or intruder is not your user, for the time being we will not track him/her because it would be the costly procedure. And besides all these functionalities all the proceedings will be saved for the future use and the routine of last placed attack will be placed in the library of the layer so that the this type of attack will never happen again.

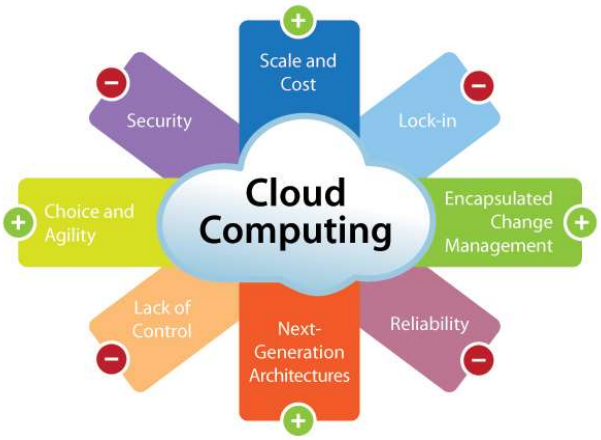


Benefits of our methodology:-

There are several characteristics of a cloud. Some of them are given below:

- **Scalability and elasticity:-**
  Our methodology will enhance more scalability and elasticity in the structure of the cloud.
- **Invulnerability :-**
  Our proposed system will make the autonomic cloud system immune of most of the attacks Thus becoming the cloud invulnerable of virus, worms and hacking.
- **Manageability and interoperability:-**
  As our methodology is self automated the experts don't have to do the most of the work as it is done by the system itself.

  It increases the manageability of the cloud; the cloud would be manageable easily. The experts also don't have to give the instructions every time when the system is attacked. Thus increases its interoperability.
- **Performance and optimization:-**
  Our methodology will increases the performance of the cloud both directly and in directly. As the system is less vulnerable to attack the efficiency and the performance of the cloud will automatically increases. The structure of the cloud will be more optimized this way.



- **Paragon for other techniques:-**
  Our methodology will be used as a paragon for the others models to enhance the security in the autonomic cloud. We have used workflow efficient algorithms which can be used in other schemes to enhancing the security.

Conclusion:-

We have defined a methodology for the autonomous cloud computing which has the three basic steps. In first step we are detecting that either the incoming request is a virus or some hacking tools trying to harm or hack the cloud.

In the second phase we are prioritizing the attack from the number 1 to 10. 1being the mildest attack and 10being the most severe attack. In the last step we are applying our designed algorithms to enhance the security in the autonomous cloud computing.

Future work:-

In the future more layers can be introduced in our methodology to enhance the security. We have defined our implementation in one layer and that layer does all the work. In the future more layers can be defined and each will do its separate work. Introducing more layers means introducing more security in the cloud.

Besides that DaaS can be implemented in the autonomous cloud computing which stands for defense as a service. As we know we have IaaS, PaaS, SaaS. Besides three basic services DaaS can also be implemented which only accounts for ensuring the security in the cloud.

AI can also be introduced in the autonomous computing

REFERENCES

1. Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." *Future Generation computer systems* 28.3 (2012): 583-592.
2. Pearson, Siani, and Azzedine Benameur. "Privacy, security and trust issues arising from cloud computing." *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*. IEEE, 2010.

3. Krutz, Ronald L., and Russell Dean Vines. *Cloud security: A comprehensive guide to secure cloud computing*. John Wiley & Sons, 2010.
4. Buyya, Rajkumar, Chee Shin Yeo, and Srikumar Venugopal. "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities." *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on*. Ieee, 2008.
5. Mell, Peter, and Tim Grance. "Effectively and securely using the cloud computing paradigm." *NIST, Information Technology Laboratory* (2009): 304-311.
6. Buyya, Rajkumar, Rodrigo N. Calheiros, and Xiaorong Li. "Autonomic cloud computing: Open challenges and architectural elements." *Emerging Applications of Information Technology (EAIT), 2012 Third International Conference on*. IEEE, 2012.
7. Lombardi, Flavio, and Roberto Di Pietro. "Secure virtualization for cloud computing." *Journal of Network and Computer Applications* 34.4 (2011): 1113-1122.