Journal of Engineering and Applied Sciences 12 (Special Issue 2): 6223-6226, 2017
ISSN: 1816-949X

Security Aware Vulnerability Avoidance in Cloud Computing using Nature Inspired Approach

[1]Sachin Gupta, [2]Sanjay Singla and [3]S.N. Panda
[1]Department of Computer Science, I.K. Gujral Punjab Technical University, Jalandhar, Punjab, India
[2]Department of CSE, IET, Bhaddal, Punjab, India
[3]Chitkara University, Punjab, India

Abstract: Cloud computing is emerging as one of the high performance and integrity aware area in the distributed and grid based computing environment. Enormous computing and technology based services are delivered and disseminated throughout the globe using cloud implementations because of increasing usage of technology products. As these products and devices are quite costly to purchase, cloud computing gives the option to hire the computing infrastructure with per usage base. As cloud computing is escalating by number of services, there are lots of issues regarding vulnerability and integrity in the data centers from where these cloud services are disseminated. This research manuscript presents and implements a unique and effectual approach for security of data centers using dynamic approach for encryption during communication and accessing the cloud services. The results in the projected novel approach are effective in terms of cost, complexity and overall performance. The projected novel approach is using nature inspired approach river formation dynamics for the enhancement of results and performance.

Key words: Cloud computing, cloud of things, nature inspired approach, network security, river formation dynamics

INTRODUCTION

Security and vulnerability (Popovic and Hocenski, 2010) analysis are the key features which are frequently addressed in the assorted algorithms by number of scientists and academicians. Numbers of algorithms are devised so far for the identification and avoidance of security issues. These are the algorithms and approaches which works on the security aspects of cloud infrastructure.

In cloud computing (Buyya, 2009), there are multiple scenarios and points where security vulnerability can be identified. These cloud delivery methods can be Infrastructure as a Service (IaaS) (Bhardwaj *et al*., 2010), Platform as a Service (PaaS), Software as a Service (SaaS) (Bassiliades *et al*., 2017), Testing as a Service (TaaS) (Rajput and Gupta, 2014) or any other. All these cloud delivery points can be susceptible to the assaults from different sources and cracking modes.

Security vulnerability aspects in cloud: There are number of attacks and taxonomy of assaults which can be initiated in a network based environment. Any of the following vulnerability and assault attempt can be there in cloud computing environment:

- Sybil attack (Margolin and Levine, 2008)
- Identity threat (Kandias *et al*., 2012)
- Wormhole attack
- Distributed Denial of Service (DDoS) attack
- Jamming assault
- Traffic overloading

Any lots of other assaults: All of these attacks are very precarious to cloud based delivery point for the cloud service provider as well as cloud end user. In this research, a unique and effectual approach for run time cryptography during communication is devised and implemented for the higher degree of security and integrity against such attacks.

MATERIALS AND METHODS

Problem formulation and proposed work: So many algorithms, protocols and methodologies are in

Corresponding Author: Sachin Gupta, Department of Computer Science, I.K. Gujral Punjab Technical University, Jalandhar, Punjab, India

development, still there is a scope of developing new and higher security algorithms which can enforce greater security. In this manuscript, the approach adopted is the dynamic encryption during communication of cloud user, cloud broker and cloud service provider and there are multiple layers in which the communication can be authenticated.

The traditional approaches for security and integrity include ant colony optimization, genetic algorithm, honeybee algorithm, neural networks and similar which are quite conventional and there is need to evolve and integrate a new approach for the greater optimization.

The proposed algorithmic approach in this manuscript is adopting river formation dynamics for higher degree of security and integrity with the layer based refinement of the results. In each layer and phase of river formation dynamics the path of secured cloud based transmission is decided and further global results are evaluated. The proposed work is taking the following layers to evaluate the appropriate path. Evaluation of the vulnerability and sniffing in the existing scenario. Deep learning and analytics on the checkpoints of cloud channels so that, the secured and global optimal path towards secured environment can be devised. The sediments processing the river formation dynamics is keeping track of sniffing points which can be addressed and exploited. By this evaluation, a higher degree of security enabled system is presented as a path of security for integrity and privacy based applications.

RESULTS AND DISCUSSION

For implementation, the prominent cloud computing based library and simulator CloudSim is used which is having all the libraries and base classes for implementation of security at multiple layers. Using cloud analyst and grid sim there is integration of high performance computing in the grid based environment which can impose more security and performance in the higher load to avoid the congestions.

Projected nature inspired approach (river formation dynamics): In this proposed research and implementation, cloudsim is used to call and integrate the cloud components, virtual machines and related objects in the cloud environment. CloudSim provides the library and frame work to with the cloud components. The association of cloud analyst is done to present the data centers and virtual machines with associated factors in the graphical perspectives. The proposed algorithm of river formation dynamics is implemented in this phase of cloud based transmission and communication between the cloudlets and in secured dimensions. The tool R is used to have the deep analytics and statistical measures of the results and security perspectives (Fig. 1-3).

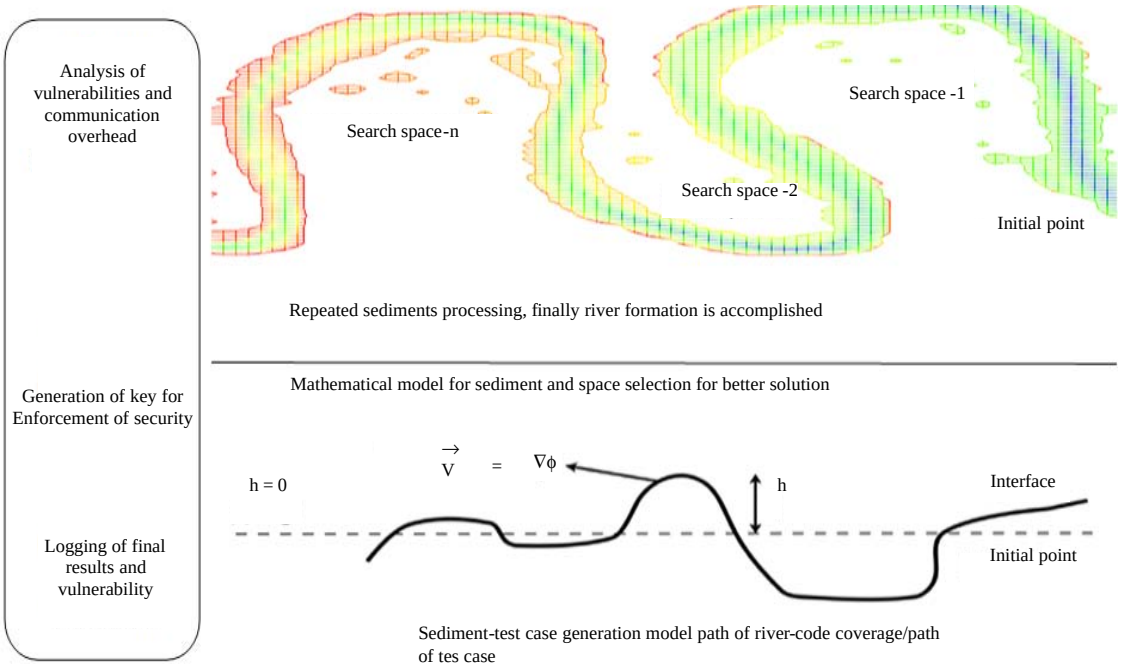


Fig. 1: River formation dynamics in cloud environment

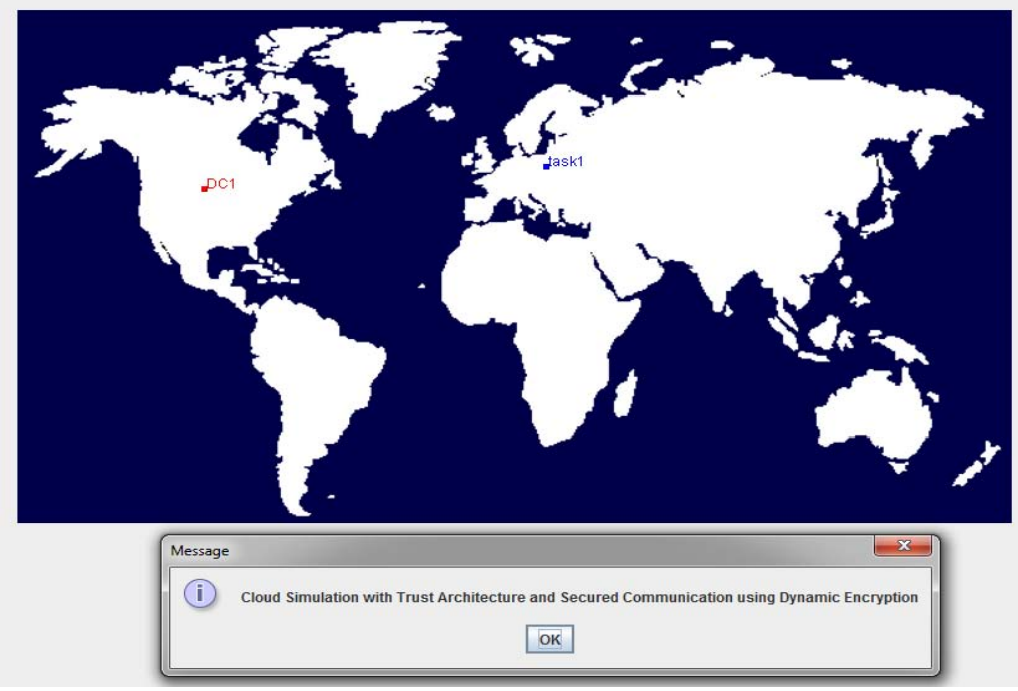
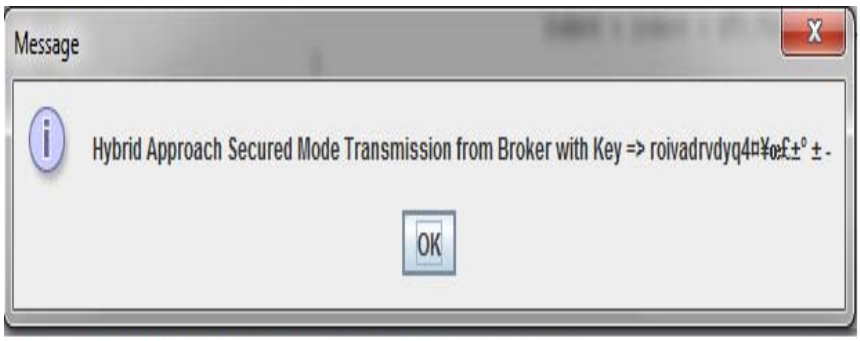


Fig. 2: Initialization of cloud simulator for dynamic security




```
Starting Cloud Simulation with Dynamic and Hybrid Secured Key
---------------------------------------
Initialising...
Trust User Hash Digest(in Hex. format):: 64e5eb5e5d1e597a3e09174964197f94
Hybrid Trust Approach Hash Hex format : aabba6d301b2e834282a38c91ae54d6d8fbdbc71233fa9e87e6fb75608fe9e2b
Hybrid Approach Trust Based Security Key Transmitted =>
roivadrvdyq4¤¥?£±° ?± -
```

Fig. 3: Generation of intermediate key for security aware communication

Tools used for implementation:

- CloudSim
- CloudAnalyst
- GridSim
- Notepad++
- R

It is evident from Fig. 4 and 5 that the complexity and cost in the projected nature inspired approach is very less as compared to the traditional approach. The overall performance of the proposed approach is higher as compared to the traditional approach of ant colony optimization because of the greater security and integrity aware algorithm (Table 1).

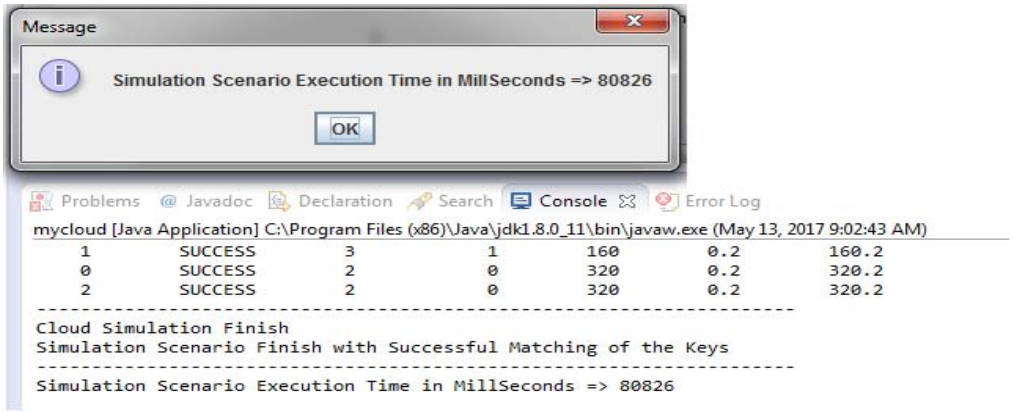


Fig. 4: Fetching the results from cloud simulation on implementation

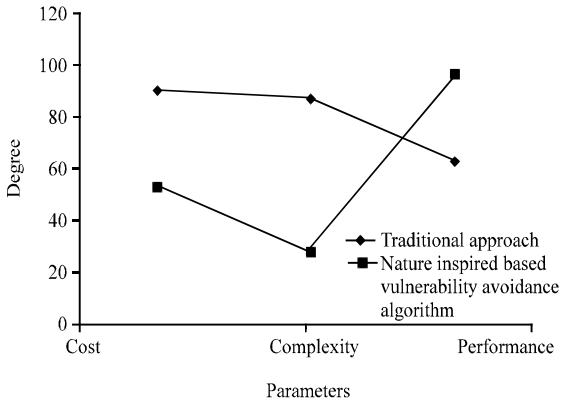


Fig. 5: Generation of intermediate key for security aware communication

Table 1: Comparative evaluation of results on multiple parameters

Parameter/Algorithms	Cost	Complexity	Performance
Traditional approach (ant based optimization)	90	87	64
Nature inspired based vulnerability avoidance algorithm	53	28	96

CONCLUSION

The projected nature inspired approach is river formation dynamics which is used for integration of higher degree of security. River formation dynamics is the process by which the rivers are formed from frequent flowing water from a particular region. Same approach is imitated in the security and overall scheduling of cloud environment. The proposed results are effectual on multiple parameters which can be further improved using assorted soft computing techniques. In soft computing and elaborated nature inspired approaches, there can be the integration of river formation dynamics, bee optimization, lion algorithm, elephant approach, fermentation based algorithms and many others. These approaches are effectual in providing the global optimization.

REFERENCES

Bassiliades, N., M. Symeonidis, G. Meditskos, E. Kontopoulos and P. Gouvas *et al*., 2017. A semantic recommendation algorithm for the paasport platform-as-a-service market place. Expert Syst. Appl., 67: 203-227.

Bhardwaj, S., L. Jain and S. Jain, 2010. Cloud computing: A study of Infrastructure As A Service (IAAS). Int. J. Eng. Inform. Technol., 2: 60-63.

Buyya, R., 2009. Market-oriented cloud computing: Vision, hype and reality of delivering computing as the 5th utility. Proceedings of the 9th IEEE/ACM International Conference on Cluster Computing and the Grid CCGRID 2009, May 18-21, 2009, IEEE, Shanghai, China, ISBN:978-1-4244-3935-5, pp: 5-13.

Kandias, M., N. Virvilis and D. Gritzalis, 2012. The insider threat in cloud computing. Proceedings of the 6th International Workshop on Critical Information Infrastructure Security, September 8-9, 2011, Switzerland, pp: 99-103.

Margolin, N. and B. Levine, 2008. Quantifying resistance to the sybil attack. Financial Cryptography Data Secur., 1: 1-15.

Popovic, K. and Z. Hocenski, 2010. Cloud computing security issues and challenges. Proceedings of the 33rd IEEE International Conference on MIPRO, May 24-28, 2010, IEEE, Opatija, Croatia, ISBN:978-1-4244-7763-0, pp: 344-349.

Rajput, A. and A. Gupta, 2014. A study of testing issues and difficulties in cloud based application and current practices. Intl. J. Technol. Eng. Sci., 2: 2562-2568.