Effectual Approach for Cloud Data Center Security using Metaheuristic based Global Optimization

L.A Abdul Rasul A. AL WAILI
University of Wasit / College of Education – Computer Science Department

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 Metaheuristic Approach for the enhancement of results and performance.

Keywords – Cloud Computing, Cloud of Things, Nature Inspired Approach, Network Security, River formation dynamics Metaheuristic Approach

I. FOREWORD AND INTRODUCTION

Security and vulnerability [1] 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 [2], there are multiple scenarios and points where security vulnerability can be identified. These cloud delivery methods can be Infrastructure as a Service (IaaS) [3], Platform as a Service (PaaS) [4], Software as a Service (SaaS) [5], Testing as a Service (TaaS) [6] or any other. All these cloud delivery points can be susceptible to the assaults from different sources and cracking modes.

II. EVALUATION OF SECURITY 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 [7]
- Identity Threat [8]
- 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 work, 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.

III. PROBLEM IDENTIFICATION

So many algorithms, protocols and methodologies are in 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 Metaheuristic Approach for higher degree of security and integrity with the layer based refinement of the results. In each layer and phase of River formation dynamics Metaheuristic Approach, 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

(i) Evaluation of the Vulnerability and Sniffing in the Existing Scenario.

(ii) Deep Learning and Analytics on the Checkpoints of Cloud Channels so that the secured and global optimal path towards secured environment can be devised.

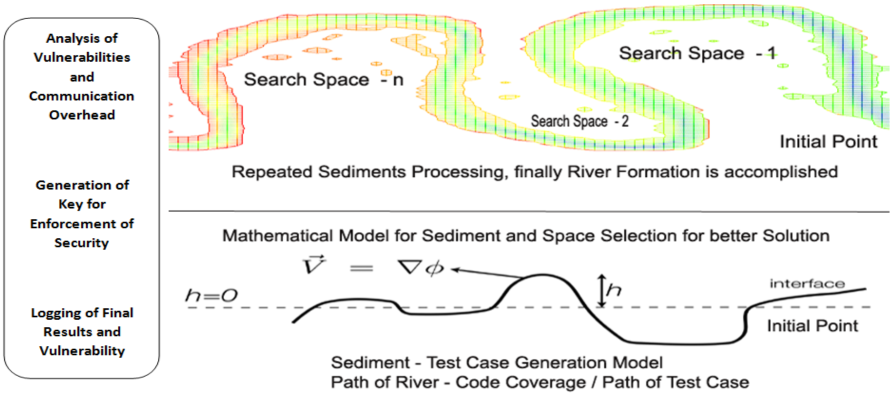
(iii) The sediments processing the River formation dynamics Metaheuristic Approach is keeping track of sniffing points which can be addressed and exploited. By this evaluation, a higher degree of security enabled system is presented as a path of security for integrity and privacy based applications.

IV. IMPLEMENTATION ON CLOUD SIMULATOR AND RESULTS

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 CloudAnalyst and GridSim, 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.

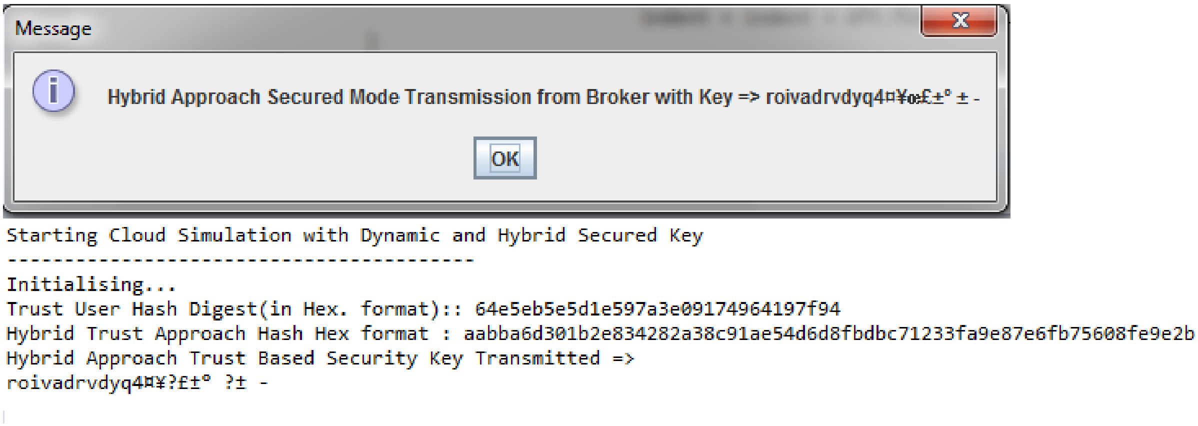
In the proposed work and implementation of Projected Nature Inspired Approach : River formation dynamics Metaheuristic Approach, cloudsim is used to call and integrate the cloud components, virtual machines and related objects in the cloud environment. Cloudsim provides the library and framework to with the cloud components. The association of cloudanalyst is done to present the data centers and virtual machines with associated factors in the graphical perspectives. The proposed algorithm of River formation dynamics Metaheuristic Approach 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.

Figure 1. Integration and Implementation RFDMA Approach in Cloud


Analysis of Vulnerabilities and Communication Overhead
Generation of Key for Enforcement of Security
Logging of Final Results and Vulnerability
Search Space - 1
Search Space - n
Search Space - 2
Initial Point
Repeated Sediments Processing, finally River Formation is accomplished
Mathematical Model for Sediment and Space Selection for better Solution
$\vec{V} = \nabla \phi$
$h=0$
h
interface
Initial Point
Sediment - Test Case Generation Model
Path of River - Code Coverage / Path of Test Case

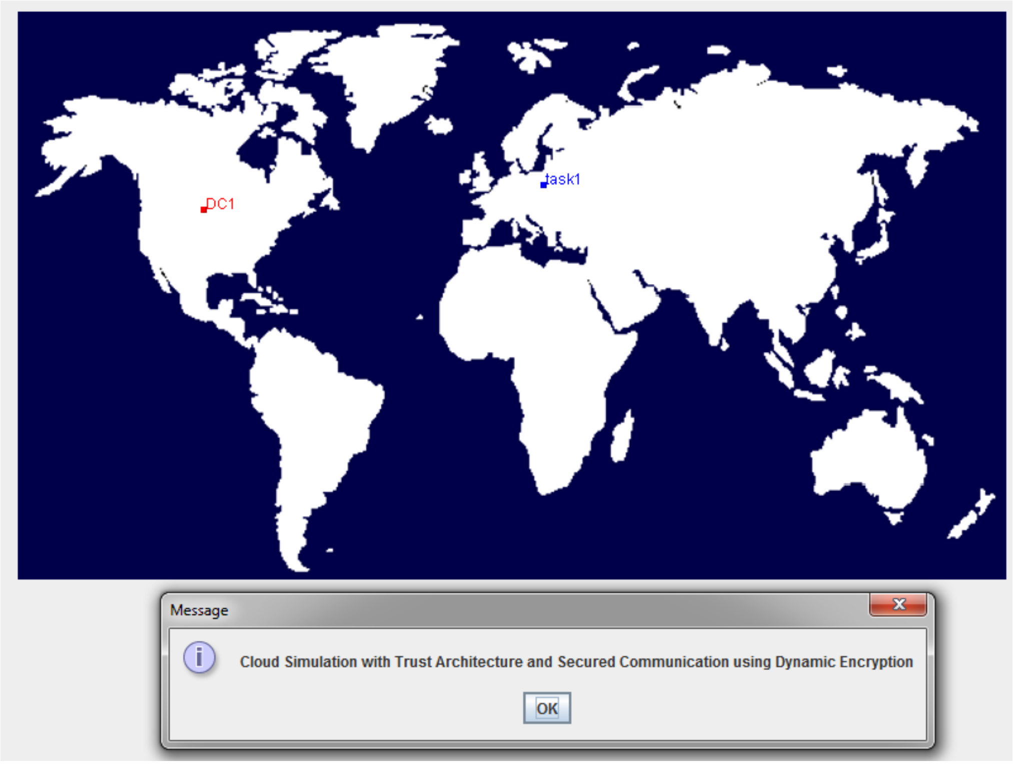
Tools used for Implementation

- Ubuntu Linux
- CloudSim
- CloudAnalyst
- GridSim
- Notepad++
- R
- JCharts
- Advance Java
- Java APIs



Hybrid Approach Secured Mode Transmission from Broker with Key => roivadrvdyq4¤¥œ£±° ± -

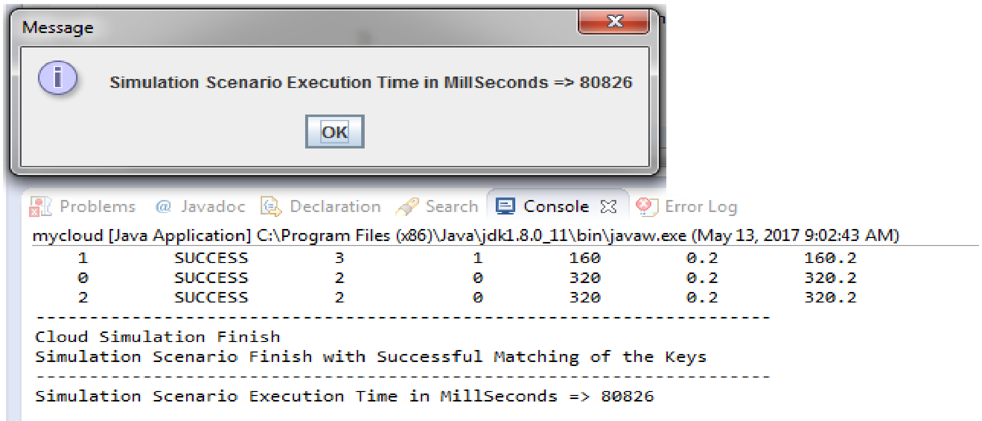
```
Starting Cloud Simulation with Dynamic and Hybrid Secured Key
-----------------------------------------
Initialising...
Trust User Hash Digest(in Hex. format):: 64e5eb5e5d1e597a3e09174964197f94
Hybrid Trust Approach Hash Hex format : aabba6d301b2e834282a38c91ae54d6d8fbdbc71233fa9e87e6fb75608fe9e2b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



Cloud Simulation with Trust Architecture and Secured Communication using Dynamic Encryption

Figure 2. Activation of Cloud Components for further Secured Transmission

Figure 3. Dynamic Generation of Private Secured Keys for Data Transmission in Cloud



Simulation Scenario Execution Time in MillSeconds => 80826

```
mycloud [Java Application] C:\Program Files (x86)\Java\jdk1.8.0_11\bin\javaw.exe (May 13, 2017 9:02:43 AM)
    1         SUCCESS         3          1         160        0.2        160.2
    0         SUCCESS         2          0         320        0.2        320.2
    2         SUCCESS         2          0         320        0.2        320.2
---------------------------------------------------------------------
Cloud Simulation Finish
Simulation Scenario Finish with Successful Matching of the Keys
---------------------------------------------------------------------
Simulation Scenario Execution Time in MillSeconds => 80826
```

Figure 4: Real Time Analytics of Results from Cloud Data Centers

Table 1: Effectual Comparative Analysis of Traditional and Projected Approach

Parameter / Algorithm	**Cost**	**Complexity**	**Performance**
Traditional Approach (Ant Based Optimization)	89	85	64
Nature Inspired Based Vulnerability Avoidance Algorithm	52	27	94

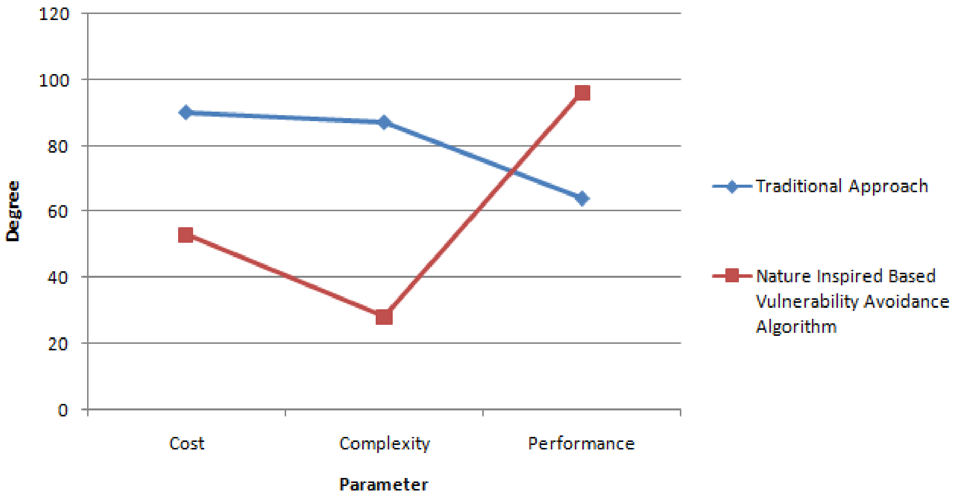


Figure 5. Generation of Intermediate Key for Security Aware Communication

It is evident from the figure 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.

V. CONCLUSION

The projected nature inspired approach is River formation dynamics Metaheuristic Approach which is used for integration of higher degree of security. River formation dynamics Metaheuristic Approach (RFDMA) 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 Metaheuristic Approach, bee optimization, lion algorithm, elephant approach, fermentation based algorithms and many others. These approaches are effectual in providing the global optimization.

REFERENCES

[1] K. Popovic and Z. Hocenski, “Cloud computing security issues and challenges,” MIPRO, 2010 Proc. 33rd, no. January 2016, pp. 344–349, 2010.

[2] R. Buyya, “Market-oriented cloud computing: Vision, hype, and reality of delivering computing as the 5th utility,” 2009 9th IEEE/ACM Int. Symp. Clust. Comput. Grid, CCGRID 2009, no. June 2009, p. 1, 2009.

[3] S. Bhardwaj, L. Jain, and S. Jain, “Cloud Computing : a Study of Infrastructure As a Service (Iaas),” Int. J. Eng., vol. 2, no. 1, pp. 60–63, 2010.

[4] P. Westner and S. Hermann, “VR | ServE : A Software Toolset for Service Engineering using Virtual Reality,” Icserv 2015, 2015.

[5] N. Bassiliades, M. Symeonidis, G. Meditskos, E. Kontopoulos, P. Gouvas, and I. Vlahavas, “A semantic recommendation algorithm for the PaaSport platform-as-a-service marketplace,” Expert Syst. Appl., vol. 67, no. September, pp. 203–227, 2017.

[6] A. Rajput and A. Gupta, “A Study of Testing Issues and Difficulties in Cloud Based Application and Current Practices,” Ijtes.Com, vol. 2, no. November, pp. 2562–2568, 2014.

[7] N. B. Margolin and B. N. Levine, “Quantifying resistance to the sybil attack,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5143 LNCS, pp. 1–15, 2008.

[8] M. Kandias, N. Virvilis, and D. Gritzalis, “The Insider Threat in Cloud Computing,” Crit. Inf. Infrastruct. Secur. 6th Int. Work. CRITIS 2011, vol. 6983, no. c, pp. 93–103, 2013.