IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 12, December 2019

Intrusion Detection and Fail Safe Mechanism to Optimise Performance of Cloud

ER. Sagar Qayoom[1], ER. Gurjeet Kaur[2]

M.Tech., in CSE, SRI SAI College of Engineering & Technology,

IKG Punjab Technical University, Jalandhar, Punjab[1]

Assistant Professor, Department of Computer Science Engineering,

SRI SAI College of Engineering and Technology, Badhani Pathankot, Punjab[2]

Abstract: Cloud computing and resource provisioning is solution to different problems presented through starvation and shortage of resources. To this end, Intrusion detection plays a critical role by providing resources to clients as per requirements of clients. This paper presents study of techniques of Intrusion detection and suggests future enhancements as well. Intrusion detection categories including network, storage, data, desktop and server are discussed in detail with results and further improvement to minimize energy consumption is suggested. Optimization in Intrusion detection is achieved considering load balancing degree. Service in terms of storage is frequent since client storage requirements are in demand due to least cost. In addition, platform related requirements are also satisfied frequently. In case of failure of resources VM migration procedures are in place. This paper also put light on issues of VM migration to optimize migration time.

Parameters Considered: Migration time, degree of load balancing, cost, energy consumed

Techniques: Data, Storage, Server, network and desktop Intrusion detection, Pre-Copy, Post Copy and Hybrid approach under LIVE VM migration

Keywords: Intrusion detection, Migration, Migration time, Cost, degree of load balancing

I. INTRODUCTION

Energy consumption and load balancing is state of the art problem that requires attention of researchers. (Choudhary et al. 2016)To resolve problems corresponding to energy and load balancing, researchers try to optimize Intrusion detection. Process of Intrusion detection is given through figure 1. The Intrusion detection process includes multiple entities including client, service provider, datacenters, brokers, VM selection policies and finally fails safe procedures. Clients provides cloudlets to executed by virtual machines, datacenters are actually physical machines providing resources to the clients a datacenters possessing multiple resources are partitioned into distinct virtual machines. Clients get access to virtual machines. (Shakkeera and Tamils Elvan 2016)Load balancing degree is observed by broker in VM selection mechanism. User requires paying for the service it gets from cloud service provider. Both service providers and clients are bounded by service level agreement.

SLA cannot be violated but no hard and fast rules or punishment is defined in case service provider violets this SLA. To attract mass community towards cloud services, this aspect has to be improved. Never the less, researchers are focusing on increasing mass communities towards cloud services by increasing reliability and optimizing services through fault tolerance strategies. Backup plan in place is critical as VM provides services to client. Loss of service and data is not affordable in this competitive era. This paper focuses on multiple aspects and organization of this paper is listed as under

Section 1 gives introduction about general entities involved within cloud , section 2 present analysis of data, server, desktop and storage Intrusion detection , section 3 gives analysis of fail-safe mechanisms , section 4 presents problems and future enhancements that could be incorporated to improve performance, section 5 presents conclusion and future scope.

DOI 10.17148/IJIREEICE.2019.71206

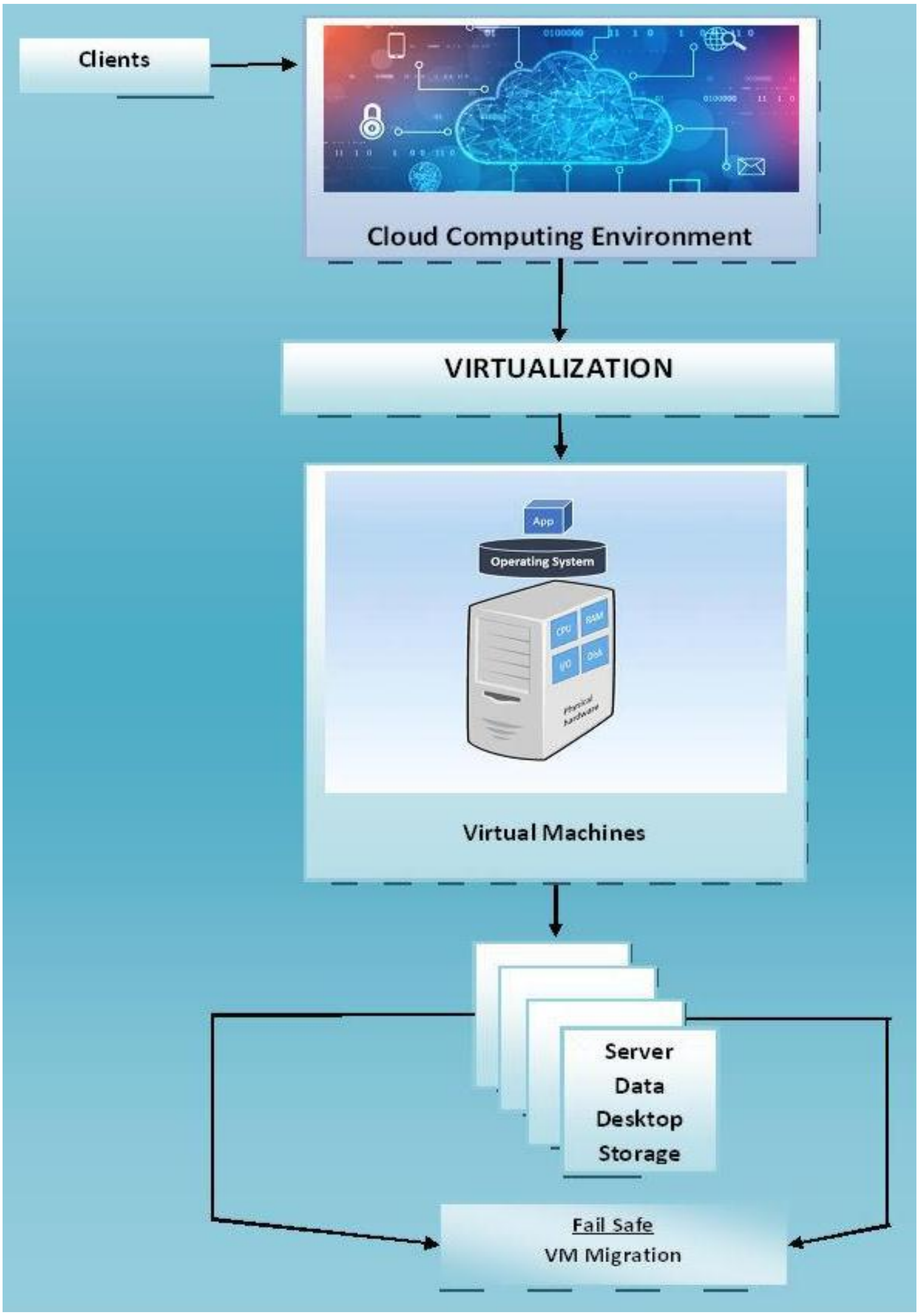

Fig.1: Process of Intrusion detection

DOI 10.17148/IJIREEICE.2019.71206

II. TECHNIQUES OF INTRUSION DETECTION

Research conducted by (Celesti et al. 2011; Liu and Chou 2013; Al-azez et al. 2016; Kurdi et al. 2018) discussed fault tolerance along with energy efficiency in the field of Intrusion detection. Both proactive and reactive fault tolerance strategies are paid stress upon for increasing efficiency of Intrusion detection. Intrusion detection mechanisms are discussed in detail in this section

2.1 Server Intrusion detection

This is resource based partitioning mechanism in which physical server is portioned into small virtual servers. Intrusion detection of this sought is achieved with the help of Intrusion detection software. Virtual servers obtained with the help of Intrusion detection are capable of storing multiple operating systems. It is required to handle multiple requests from clients and hence shadow cores from processor must be portioned. Thus micro portioning of physical server is required in case of server Intrusion detection. Researchers worked upon server Intrusion detection for increasing throughput is listed in table 1.

Table 1: Server Intrusion detection mechanisms

References	Intrusion detection	Description	Future scope
(Kommeri 2012)	Server Intrusion detection	Real time load is applied to test energy efficiency of server. Number of virtualized servers and service play critical role in energy achieving energy efficiency.	Optimization procedure is missing and multi-layer perceptron or genetic algorithm can be accommodated within server Intrusion detection for improvement
(Jin et al. 2016)	Server Intrusion detection	Load based strategy is employed to check energy consumption of server. This paper concludes that load is directly proportional to energy consumed	Fail safe mechanism can also play critical role in case virtual server fail.
(Jin et al. 2012)	Server Intrusion detection	Extensive data collection is done to be employed at server for checking energy consumption. Mathematical formation is done for analysis of server load	Optimization mechanism can be employed and its effect on server load can be monitored in future work
(Padala 2018)	Server Intrusion detection	Resource management is employed to manage the load on each resource to reduce cost and energy consumed.	Cluster of similar resources can be formed for faster searching procedure.

2.2 Data Intrusion detection

Data Intrusion detection is mechanism that allows client to use and manipulates data without going in-depth into technical details to access data. This means abstraction ensuring hiding complexity is ensured through this mechanism. Data Intrusion detection mechanisms are discussed in table 2.

Table 2: data Intrusion detection mechanisms

Reference	Intrusion detection	Description	Future Scope
(Xu et al. 2017)	Data Intrusion detection	Encryption mechanism is employed on data stored within cloud datacenter	Data Intrusion detection is employed but redundancy in key encryption is not considered
(Liu and Chou 2013)	Data Intrusion detection	This mechanism ensures that availability of virtual machine cannot hamper performance of cloud	Data Intrusion detection can be accommodated with bit level DE duplication to ensure better performance
(Al-azez et al. 2016)	Data Intrusion detection	IoT related framework for optical access network to conserve energy of sensors	Distributed energy efficient protocol can be employed to conserve energy further
(L. Silva, J. Alonso 2009)	Data Intrusion detection	Software rejuvenation is achieved with the help of data Intrusion detection	Cost constructive model can be used along with software rejuvenation to achieve accuracy in effort estimation

2.3 Desktop Intrusion detection

This mechanism allows the application from one PC to be executed on multiple distributed machines. This increases overall throughput of the system being used. Terminal network protocol is commonly used for this purpose. In addition user can access the application from remote machine to be used as if sitting in front of that system and using that application. Table 3 gives mechanisms along with future enhancements to those mechanisms.

Table 3: Desktop Intrusion detection mechanisms

Reference	Intrusion detection	Description	Future scope
(Das 2013)	Desktop Intrusion detection	Energy is conserved by the use of terminal network. Resources are used but files are not copied on client machine	Energy conservation mechanism including distributed energy
(Vashishtha et al. 2014)	Desktop Intrusion detection	Desktop Intrusion detection for conserving energy and increasing chances of green computing	Green computing without any fail safe mechanism lead to unreliability
(Fahimeh Farahnakian, Adnan Ashraf, Tapio Pahikkala, Pasi Liljeberg, Juha Plosila, Ivan Porres 2015)	Desktop Intrusion detection	Desktop Intrusion detection is achieved using terminal networking along with file transfer Protocol. Energy is conserved and green computing is achieved using optimization genetic algorithm	Convergence is poor but with multi-layer perceptron, better convergence can be achieved
(Xu et al. 2016)	Desktop Intrusion detection	Task scheduling to virtual machines located at different remote computers with least execution time is achieved.	Optimization is missing and execution of this mechanism led to least classification accuracy. Optimization mechanism such as MLP can enhance overall performance of task scheduling

DOI 10.17148/IJIREEICE.2019.71206

2.4 Storage Intrusion detection

This Intrusion detection is used by mass community over network. Cloud service provider share storage and cost is encountered on pay per uses basis. Intrusion detection of storage is achieved by dividing the storage server into set of virtual machines. Intrusion detection reduces cost of the client since storage independently cost more as compared to share resources. Storage Intrusion detection is described in table 4.

Table 4: Storage Intrusion detection mechanisms

Reference	Intrusion detection	Description	Future Scope
(Yang et al. 2017)	Storage Intrusion detection	K storage servers are employed to tackle the demands of clients. Deadlock is avoided in this case	K means Clustering mechanism can be used for better allocation of storage to client
(Zhu and Zhou 2005)	Storage Intrusion detection	Power aware storage Intrusion detection mechanism conserve energy by locating best possible server for clients.	Clustering mechanism can improve execution time required for allocation
(Wang et al. 2009)	Storage Intrusion detection	Security of storage is ensured using this mechanism	DE duplication can be ensured to reduce storage consumption further
(Wang et al. 2017)	Storage Intrusion detection	Storage Intrusion detection of this sort ensure optimal storage utilization and hence cost is reduced	Clustering ensuring reduced cost and execution time

III. VM MIGRATION

This is also critical since fail safe mechanism must be employed to ensure reliability of cloud. Breach in reliability causes mass community to divert from service provider and choose some other service provider. These fail safe mechanism is generally provided with the help of VM migration. VM migration used in different literatures is expressed in table 5.

Table 5: VM migration strategies along with future scope

References	Type	Description	Future scope
(Li 2016)	Live VM migration	Both source and destination machines areactive while migration is executed	Shortest distance mechanism can be incorporated to overcome `extensive energy utilization
(Asif et al. 2015)	Pre, post and hybrid migration	All these mechanism are discussed and pre copy approach is demonstrated to be the best one	Energy consumption while migration is high that can be reduced by the use of Handling distance mechanism
(Katsipoulakis et al.	Adaptive live VM	Source and	Clustering and

DOI 10.17148/IJIREEICE.2019.71206

2013)	migration	destination machines are up while storage and process is migrated	distance based mechanism can substantially reduce migration time
(Sekhar et al. 2013)	Cost efficient live VM migration	During migration cost is preserved and less energy is consumed	By applying redundancy handling mechanism, cost can be further reduced

IV. PROBLEM DEFINITION

During the last few years, there has been a sharp increase in the number of cloud-based computer attacks. This has led many researchers to study this field in great depth in order to develop novel methods that are capable of eliminating this threat from today's computer clouds. It describes various attacks like DDOS and spoofing. The DDOS attack generates a large volume of flow that attacks the victim and victim is unable to defend because the detection of attack is late. Thus this leads to data loss and late packet delivery ratio. In existing technique PMNIDS algorithm is used to detect attack by using Queue based techniques. The TPR is low and FPR is more with this technique which is has to be optimized.

OBJECTIVE OF STUDY

The proposed work deals with the mobility of nodes along with the static nodes to reduce the identity based attacks in the cloud like clouds. The objectives are listed as follows

- ✓ To study the clustering techniques for data mining.
- ✓ To detect normal and abnormal data in intrusion detection systems.
- ✓ To identify the false positive, false negative, and Accuracy generated using hierarchical algorithm;
- ✓ Comparison of the results of Feature detector and hierarchical algorithm.

V. CONCLUSION

Cloud computing is a emerging field of study providing resources with least cost to clients. Clients can access resources on pay per use basis. Effective storage utilization can be achieved by accommodating better space handling procedure like deduplication with DNA encryption to enhance reliability. Cost effective procedure can attract mass community towards services offered by cloud service provider. In case of failure of service, fail safe procedure must be present within the cloud environment. This fail safe mechanism includes live VM migration. Pre and post copy approaches are commonly used fail safe mechanisms. In addition hybrid procedure in place but it is expensive. Pre copy approach can be used if processing requirements are more and post copy if storage requirements are more. Distance handling mechanism can be used in order to ensure faster allocation of virtual machine. Overall optimization, distance handling procedure and fail safe mechanism must be included with Intrusion detection increase reliability and decrease cost associated with resource utilization and increase reliability.

REFERENCES

[1]. Al-azez ZT, Lawey AQ, El-gorashi TEH, Elmirghani JMH (2016) Energy Efficient IoT Intrusion detection Framework with Passive Optical Access Networks. ICTON 1–4

[2]. Asif S, Shah R, Jaikar AH, Noh S (2015) A Performance Analysis of Precopy , Postcopy and Hybrid Live VM Migration Algorithms in Scientific Cloud Computing Environment. IEEE Access 229–236

[3]. Celesti A, Tusa F, Villari M, Puliafito A (2011) An Approach to Enable Cloud Service Providers to Arrange IaaS , PaaS , and SaaS Using External Intrusion detection Infrastructures. doi: 10.1109/SERVICES.2011.92

[4]. Choudhary A, Rana S, Matahai KJ (2016) A Critical Analysis of Energy Efficient Virtual Machine Placement Techniques and its Optimization in a Cloud Computing Environment. Procedia - Procedia Comput Sci 78:132–138 . doi: 10.1016/j.procs.2016.02.022

[5]. Das T (2013) LiteGreen : Saving Energy in Networked Desktops Using Intrusion detection

[6]. Fahimeh Farahnakian, Adnan Ashraf, Tapio Pahikkala, Pasi Liljeberg, Juha Plosila, Ivan Porres and HT (2015) Using Ant Colony System to Consolidate VMs for Green Cloud Computing. IEEE Trans Serv Comput 184–198

[7]. Jin Y, Wen Y, Chen Q (2016) An Empirical Investigation of the Impact of Server Intrusion detection on Energy Efficiency for Green Data. IEEE Access

[8]. Jin Y, Wen Y, Chen Q (2012) Energy Efficiency and Server Intrusion detection in Data Centers : An Empirical Investigation. IEEE Access

[9]. Katsipoulakis NR, Tsakalozos K, Delis A (2013) Adaptive Live VM Migration in Share-Nothing IaaS-Clouds with LiveFS. In: 2013 IEEE 5th International Conference.

[10]. Kommeri J (2012) Energy Efficiency of Server Intrusion detection. IEEE Access 90–95
[11]. Kurdi HA, Alismail SM, Hassan MM (2018) LACE: A Locust-Inspired Scheduling Algorithm to Reduce Energy Consumption in Cloud Datacenters. IEEE Access 6:35435–35448 . doi: 10.1109/ACCESS.2018.2839028
[12]. L. Silva, J. Alonso and JT (2009) Using Intrusion detection to Improve Software Rejuvenation. IEEE Trans Comput 58:1525–1538
[13]. Li Z (2016) Optimizing VM Live Migration Strategy Based On Migration Time Cost Modeling. IEEE ACCESS 99–109
[14]. Liu CYJ, Chou CHW (2013) On improvement of cloud virtual machine availability with Intrusion detection fault tolerance mechanism. IEEE Access. doi: 10.1007/s11227-013-1045-1

[15]. Padala PR (2018) Intrusion detection of Data Centers study on Server Energy Consumption Performance. IEEE Access
[16]. Sekhar J, Jeba G, Nadu T (2013) Energy Efficient VM Live Migration in Cloud Data Centers. IEEE Access 2:71–75
[17]. Shakkeera L, Tamilselvan L (2016) Energy-Aware Application Scheduling and Consolidation in Mobile Cloud Computing with Load Balancing. IEEE Access. doi: 10.1007/978-981-10-0287-8
[18]. Vashishtha V, Gupta A, Sarwar PS (2014) Green Computing : An Approach Of Saving Energy By Computer Intrusion detection . 3:103–106
[19]. Wang C, Wang Q, Ren K, Lou WJ (2009) Ensuring Data Storage Security in Cloud Computing. Iwqos 2009 Ieee 17th Int Work Qual Serv 37–45\n302 . doi:10.1109/IWQoS.2009.5201385
[20]. Wang J, Luo W, Liang W, Liu X, Dong X (2017) Locally Minimum Storage Regenerating Codes in Distributed Cloud Storage Systems. IEEE ACCESS 82–91
[21]. Xu D, Fu CAI, Li G, Zou D (2017) Intrusion detection of the Encryption Card for Trust Access in Cloud Computing. IEEE Access 5:
[22]. Xu X, Cao L, Wang X(2016) Resource pre-allocation algorithms for low-energy task scheduling of cloud computing. IEEE Access 27:457–469
[23]. Yang T, Pen H, Li W, Yuan D, Zomaya AY (2017) An energy-efficient storage strategy for cloud datacenters based on variable k-coverage of a hypergraph. IEEE Trans Parallel Distrib Syst 28:3344–3355 . doi: 10.1109/TPDS.2017.2723004
[24]. Zhu Q, Zhou Y (2005) Power - Aware Storage Cache Management. IEEE Trans Comput 54:587–602

BIOGRAPHIES

Sagar Qayoom received his B.E in CSE from SSM College of Engineering and Technology, University Of Kashmir in 2016 and pursuing M.Tech from SRI SAI College of Engineering and Technology, IKG Punjab Technical University, Jalandhar Punjab.

Gurjeet Kaur received her B.Tech degree from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib Punjab in 2011 and received M.Tech from Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India. At present working as Assistant Professor, Department of Computer Science Engineering, SRI SAI College of Engineering and Technology, Badhani Pathankot, Punjab.

.

DOI 10.17148/IJIREEICE.2019.71206