International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 22 (2017) pp. 12189-12196

A Framework for Multipurpose Cloud Based Data Centre Network Security

Mr. RakeshNag Dasari
Research Scholar, Department of Computer Science & Engineering,
Koneru Lakshmaiah Education Foundation University, Green Fields, Vaddeswaram,
Guntur, Andhra Pradesh, India.
Orcid Id: 0000-0001-6504-650X

Dr. Y. Prasanth
Professor, Department of Computer Science & Engineering,
Koneru Lakshmaiah Education Foundation University, Green Fields, Vaddeswaram,
Guntur, Andhra Pradesh, India.

Dr. O. NagaRaju
Head & Asst. Professor, Department of Computer Science & Engineering,
Sri Kasu Brahmananda Reddy Govt. Degree College, Macherla,
Andhra Pradesh, India.
Orcid Id: 0000-0002-4906-529X

Abstract:

In the recent history of computing, the cloud computing is the biggest milestone achieved the researchers and industry. The advancements gained by the paradigm shift with cloud computing made significant enhancements in research, education and consumer application. These applications were hosted in the traditional data centre on the providers' premises and often failed to provide the desired performance on demand. Henceforth, motivated by the performance, cost benefits and consumer demand, the applications were migrated to the cloud based data centres. While migration of the applications to the cloud based data centres, the service providers faced challenges like supervision, control of the data generated by the application and majorly the security. Cloud service providers provide the security of the data. Nevertheless, the security of the application during network transmission is still the challenge faced by the industry. Various research attempts were made to recover the drawbacks. Nonetheless the application providers rejected these attempts at some point of time due to the privacy demand. Hence, most of the application providers demand to have a scope to deploy their own network security mechanisms. However, the recent research enhancements failed to provide any generic framework, which is generic and can accommodate any third party security protocols on demand. Thus, this research introduces a novel generic framework with the capability to accommodate any consumer demanded network security protocols with a suitable monitoring. The work is tested on various workloads such as Two weeks of HTTP logs from Internet Access provider ClarkNet, A day of HTTP logs from the EPA WWW server and A 7 hour trace of Google cluster workload. The results demonstrate a significant low fault monitoring over any data centre.

Keywords: Customizable Security Integration, Hosts metric, Clusters metric, Applications metric, Management Information metric, migration domain security violation alert.

INTRODUCTION

Any cloud based data centre is an architecture that supports hosting of various services and makes the services available to the consumers over the Internet. A cloud based data centre can be of various natures and can be classified based on the services provided. A cloud based data centre will be pronounced as IaaS or PaaS or SaaS, if the data centre provides infrastructure or application hosting platform or only software respectively [1]. Another direction to classify for these cloud data centres based on the visibility of the architecture as public or private. The most popular cloud based data centres are classified as a hybrid due to the dual visibility nature of the architecture.

Also, the data plays yet another major role in defining the data centre nature as in use data or archived data or transmitting data.

Nevertheless, the cloud based data centres are generally a combination of four components as storage, compute, memory and network. In the early days of the computing, the data centre networks are simulated and visualized based on the regular components of the network mechanism. In the recent advancements of the research and with the introduction of the

NSX for VMWare can provide software defined network visualization.

Also, the visualization of the interconnecting components in the cloud based data centre is possible now using Google's B4 network. The demonstration by S. Jain et al. [2] on the software defined wide area network research justifies the workability of the B4. The B4 is popular due to its incorporation of open flow based software defined network. The notable works by J.D. Liu et al. [3] on data centre connectivity and B. H. Yan et al. [4] on data driven connectivity makes the claim of SDN strong.

Hence, with the vision of the flexibility and scope provided by the network visualization capabilities, this work proposes the novel framework for multipurpose cloud based data centre network security.

The rest of the work is framed as in order to justify the research, the challenges of cloud based network security challenges are defined in Section – II, In the Section – III research outcomes from the recent research attempts are formulated to understand the progress and benchmarks expected, in the Section – IV the novel framework is proposed, in the Section – V obtained results are been analysed and in the Section – VI this work presents the conclusion of this research.

CLOUD BASED DATA CENTRE NETWORK SECURITY CHALLENGES

The enhancements in cloud based network virtualization due to the software driven network model exposes the unattended versions of the data centre network security challenges. The challenges are to be well understood before addressing the solutions by the security protocol designers [5].

A. Blurred Boundaries of the Network for Separation

The numbers of users are increasing rapidly as consumers of the data centre services and due the topological differences in the network, the fixed boundaries of the network regions are blurred. Most of the consumers will generate their data from a different source system, business process the data using another system and finally will storage the processed data in a different host system. Thus applying a boundary oriented security policy will create a serious overlapping and confusion during the transactions.

B. Static Topological crisis

The data centre networks are virtualized and the physical devices are replicated by the logical device end points. The logical devices are configurable with on demand capabilities for virtualization and the device policies are also to be updated dynamically. However, the policies are configured based on the static topologies, which cannot be supported by the cloud based ever-changing network virtualization [6] [7] [8] [9] [10].

C. Continuous Changing Network Security Requirements

In the space of cloud based data centre networks, the consumers will be accessing various services from the same data centre. The consumers accessing heterogeneous services will be under heterogeneous rules for security. Hence, the challenge is to accommodate various security protocols on a single device for various consumers.

D. VM Migration causing the Security Domain Violation

The data centres are known for the virtual machine migrations due to the load balancing factors. During the migration process, it is most likely possible that one virtual machine migrates to another security policy domain from a different domain. The deployed security policies are tending to fail in this situation. Hence deploying the security for virtual machines is again critical.

OUTCOMES FROM THE PARALLEL RESEARCHES

The outcomes from recent researches have demonstrated a significant growth for Software Defined Network security. For the monitoring of the network data flow, the works by S. Shin at al. [11] on FRESCO, L7 filter project [12] and V. Sekar [13] on cSamp demonstrated remarkable outcomes. The software defined network security is highly appreciated by the researchers and developers due to its nature of incorporating security services on demand. The researches on OpenFlow provided the convenience of managing, monitoring and integration of complex network security in any application architectures.

Yet another direction of the recent improvement is the SLICK framework. T. Benson et al. [14] have proposed the SLICK framework for separation of controller and middle wares from the communication interfaces.

The research issues identified by other group of researchers have demonstrated that, the middle ware boxes must be incorporated in network security design and major part of the processing are to be delegated to middle ware boxes for increasing the throughputs. The research attempts by Z. A. Qazi et al. [15] resulting into SIMPLE framework, K. Wang et al. [16] resulting into LiveSec framework and nonetheless, X. Wang et al. [16] resulting into LiveCloud demonstrated the same conclusions.

Thus, to identify the current demand of the cloud based network security is to allow the customers and service providers the scope of deployment of on demand security protocols. Hence, in the next section of this work

demonstrates a framework for inclusion of customizable and multipurpose network security for cloud based data centres.

PROPOSED FRAMEWORK

The demand for higher availability and less manageability for the data centres are motivating the migration of the traditional data centres towards the cloud based data centres. A data centres is primarily the collection of core components for computing like physical servers, storage devices with replication control, networking interface hardware like cables, routers and switches, power management systems and finally the cooling devices. The impact of small performance degradation may lead to higher business loss in the case of data centres as the data centres are majorly used for business and commercial application hosting.

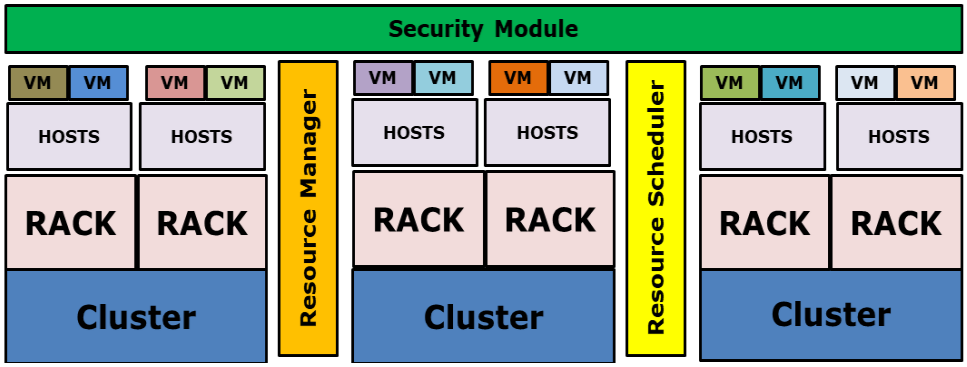

Figure 1: Framework for Multipurpose Cloud Based Data Centre Network Security

The components of the data centre are been discussed here for further analysis:

A. *Cluster*

The clusters are the generic components of the architecture hosting the physical grouping of the racks including power managements and resource management.

B. *Rack*

The racks are similar set grouping of the components for the physical computing devices such as storage, compute, network and memory.

C. *Host*

Each and every host in the setup is a physical system and this proposed framework manages the servers individually and provides the monitoring.

D. *VM*

Nonetheless, the virtual machines in the proposed architecture are the logical separation of the physical infrastructure. Each virtual machine will be connected to the resource monitoring system for detailed report of the security.

E. *Resource Manager*

The resource manager for this framework provides the application management of the deployed applications and application loads.

F. *Resource Scheduler*

The generic resource scheduler is responsible for the load balancing of the deployed applications.

Security Module

The security module is the major component of the framework and allows the customers or the owners of the applications to customize the security protocols. The security module is connected to the overall monitoring of the framework and reports every event in the network as security event.

Henceforth, in the light of the discussed proposed framework, this work elaborates the reliability in the next section.

RESULTS AND DISCUSSIONS

The proposed framework is tested on three various datasets in order to check the reliability of the model. The dataset information is presented here [Table – 1].

TABLE I: DATASET INFORMATION

Name of the Dataset	Duration (Sec)	Interval (sec)	Workload Statistics
ClarkNet-HTTP (Two weeks of HTTP logs from Internet Access provider)	1209400	100	Average: 0.3174230537 • 25%: 0.2076124567 • 50%: 0.3010380623 • 75%: 0.4111880046
EPA-HTTP (A day of HTTP logs from the EPA WWW server)	86200	100	Average: 0.2468806903 • 25%: 0.0669642857 • 50%: 0.1875 • 75%: 0.40625
Google Cluster Data (A 7 hour trace of Google cluster workload Since tasks each have different resource requirements, the workload was calculated by adding the cores required by all the tasks in each time interval, rather than simply the number of tasks, to provide a more accurate trace of the amount of work required.)	22200	300	Average: 0.8344370613 • 25%: 0.811618583 • 50%: 0.8421229708 • 75%: 0.8701741105

The simulation of the analysis is carried on the data centre simulation architecture. The details of the simulation are explained here [Table – 2].

TABLE II: SIMULATION INFORMATION

	Dataset Name		
Parameter Name	**ClarkNet-HTTP**	**EPA-HTTP**	**Google Cluster Data**
Execution time	4.0s	4.0s	1.0s
Simulated time	24.0hrs	24.0hrs	24.0hrs
Metric recording start	0ms	0ms	0ms
Metric recording duration	24.0hrs	24.0hrs	24.0hrs
Application scheduling timed out	0	0	0
Simulation time steps	932	936	325

Henceforth, the framework collects the metric parameters for reliability testing. The metric information is furnished further [Table – 3].

TABLE III: METRIC INFORMATION

Metric Type	Parameter Name	Description
Hosts	• Active Hosts • Data Centre • Power	Information of the Physical Hosts are recorded
Clusters	• Active Racks • Active Hosts Per Rack • Active Clusters • Active Racks Per Cluster • Power	Information of the Clusters are recorded
Applications	• Active VMs • CPU Under provision • SLA • Response Time	Deployed Application statistical information are recorded

	• Throughput	
Management Information	• Messages • Message BW • Migrations	Security information is recorded

*A. **Hosts***

Finally the metric parameters are evaluated on the mentioned datasets.

The parameters for the host metric is been populated [Table – 4]

TABLE IV: HOST METRIC ANALYSIS

Parameter Name	**ClarkNet-HTTP**	**EPA-HTTP**	**Google Cluster Data**
Number of Hosts	20	20	20
Active Hosts			
Max	20	20	20
Mean	10.908	7.825	19.993
Min	0	0	0
CPU util	71.32%	66.10%	76.27%
MEM util	0.09%	0.13%	0.05%
Data Centre			
CPU util	38.90%	25.86%	76.24%
MEM util	0.05%	0.05%	0.05%
Power			
Consumed	55.403kWh	38.833kWh	104.222kWh
Max	3710.415Ws	3503.146Ws	4387.631Ws
mean	2308.466Ws	1618.057Ws	4342.588Ws
Min	1775.205Ws	1068.928Ws	2960.0Ws
Efficiency	69.027cpu/watt	68.508cpu/watt	70.203cpu/watt

*B. **Clusters***

The parameters for the clusters metric is been populated [Table – 5]

TABLE V: CLUSTER METRIC ANALYSIS

Parameter Name	**ClarkNet-HTTP**	**EPA-HTTP**	**Google Cluster Data**
Active Racks			
max	0	0	0
mean	0	0	0
min	9.22E+15	9.22E+15	9.22E+15
Active Hosts Per Rack			
max	0	0	0
mean	0	0	0
min	9.22E+15	9.22E+15	9.22E+15
Active Clusters			
max	0	0	0
mean	0	0	0
min	9.22E+15	9.22E+15	9.22E+15
Active Racks Per Cluster			
max	0	0	0
mean	0	0	0
min	9.22E+15	9.22E+15	9.22E+15

Power			
consumed	0.0kWh	0.0kWh	0.0kWh
max	0.0Ws	0.0Ws	0.0Ws
mean	0.0Ws	0.0Ws	0.0Ws
min	.223372036854776E15Ws	9.223372036854776E15Ws	9.223372036854776E15Ws

C. ***Application***

The parameters for the application metric is been populated [Table – 6]

TABLE VI: APPLICATION METRIC ANALYSIS

Parameter Name	**ClarkNet-HTTP**	**EPA-HTTP**	**Google Cluster Data**
Total Applications	40	40	40
Spawned	0	0	0
Shutdown	0	0	0
Failed placement	0	0	0
average size	100.00%	100.00%	100.00%
Active VMs			
total	160	160	160
max	160	160	160
mean	159.889	159.889	159.889
min	0	0	0
Types			
CPU Under provision			
percentage	3.52%	7.05%	0.00%
SLA Achievement			
>= 99%	11	2	0
>= 95%	27	18	40
>= 90%	35	29	40
< 90%	5	11	0
mean	95.85%	92.91%	97.33%
stdev	4.04%	5.46%	0.22%
Max	100.00%	99.54%	97.92%
95th	99.99%	99.06%	97.92%
75th	99.07%	97.48%	97.27%
50th	97.45%	94.27%	97.22%
25th	93.20%	89.37%	97.22%
min	87.14%	81.47%	97.22%
Aggregate penalty			
total	143360	244800	92279
max	13	15	6
mean	1.659	2.833	1.068
min	0	0	0
Per application penalty			
mean	3584.012	6120.024	2307
stdev	3487.825	4711.877	193.566
max	11100.033	16000.065	2400
95th	10696.535	15590.033	2400
75th	5875.083	9175.058	2400
50th	2200.016	4950.017	2400
25th	800	2175	2355
min	0	400	1800
Response Time			

max	0.806	1.188	0.464
mean	0	0	0
min	0.056	0.047	0.257
Throughput			
max	52.906	40.671	90.486
mean	0	0	0
min	35.223	21.078	80.681

D. Management

The parameters for the management metric is been populated [Table – 7]

TABLE VII: MANAGEMENT METRIC ANALYSIS

Parameter Name	ClarkNet -HTTP	EPA-HTTP	Google Cluster Data
Messages			
HostStatusEvent	3161	2274	5760
Message BW			
HostStatusEvent	0	0	0
Migrations			
ConsolidationPolicy	119	163	0
RelocationPolicy	63	59	0
Intrarack	182	222	0
Intracluster	0	0	
Intercluster	0	0	

Finally, the findings are visualized here for Message events [Fig – 2] and Migration events [Fig – 3].

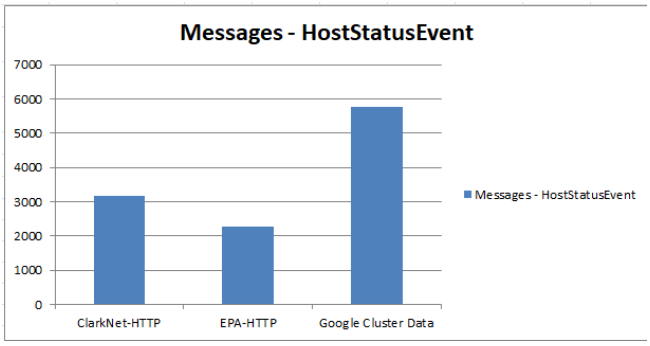

Figure 2: Host Status Notification

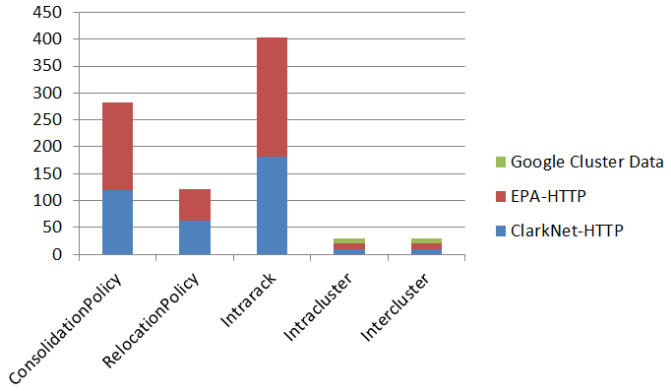

Fig.ure 3: Migration Event Notification Events

Hence it is natural to understand that the framework is able to detect the security warnings related to single host or during the migration for multiple hosts.

CONCLUSION

The data centre networks cannot be statically analysed for the security protocols. Demand from the consumers and application owners make it always critical to configure and always demands for on demand customization. Hence the need for a novel framework with customizable security capabilities cannot be denied and addressed in this work. Further it is the responsibility of the framework provider to accommodate security alert messaging feature in the framework. This work generates the event driven messaging alert system for the host systems and during the migration where maximum of the security domain violation is possible. With the use of this framework, the application owners and consumers can deploy their own security protocols and effectively monitor the events.

REFERENCES

[1] NIST definition of cloud computing, http://csrc.nist.gov/publications/PubsNISTIRs.html, 2007.

[2] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, J. Zolla, U. Hozle, S. Stuart, and A. Vahdat, B4: Experience with a globally-deployed software defined WAN, in Proc. ACM SIGCOMM 2013 Conference on SIGCOMM, Hong Kong, China, 2013, pp. 3-14.

[3] J.D. Liu, A. Panda, A. Singla, B. Godfrey, M. Schapira, and S. Shenker, Ensuring connectivity via data plane mechanisms, presented at 10th USENIX Symposium on Networked Systems Design and Implementation, Lombard, IL, USA, 2013.

[4] J. D. Liu, B. H. Yan, S. Shenker, and M. Schapira, Datadriven network connectivity, in Proc.10th ACM Workshop on Hot Topics in Networks, New York, USA, 2011, p. 8.

[5] Qihoo 360 Internet Security Center, Development trend of enterprise security in the internet ages, http://www.gartner.com/technology/mediaproducts/pdfindex.jsp?g=Qihoo issue1, 2013.

[6] X. M. Chen, B. P. Mu, and C. Zhen, NetSecu: A collaborative network security platform for in-network security, in Proc. 3rd International Conference on Communications and Mobile Computing, Qingdao, China, 2011, pp. 59-64.

[7] D. H. Ruan, C. Lin, Z. Chen, and J. Ni, Handling high speed traffic measurement using network processors, presented at International Conference on Communication Technology, Guilin, China, 2006.

[8] J. Ni, C. Lin, and Z. Chen, A fast multi-pattern matching algorithm for deep packet inspection on a network processor, presented at the IEEE International Conference on Parallel Processing, Xi'an, China, 2007.

[9] Z. Chen, C. Lin, J. Ni, D.H. Ruan, B. Zheng, Y. X. Jiang,X. H. Peng, Y. Wang, A. A. Luo, B. Zhu, Y. Yue, and F. Y. Ren, AntiWorm NPU-based parallel bloom filters for TCP/IP content processing in giga-Ethernet LAN, in Proc. the IEEE International Conference on Communications, 2006, pp. 2118-2123.

[10] Z. Chen, C. Lin, J. Ni, D. H. Ruan, B. Zheng, Y. X. Jiang, and F. Y. Ren, AntiWorm NPU-based parallel bloom filters for TCP/IP content processing in Giga-Ethernet LAN, in Proc. the IEEE International Conference on Local Computer Networks, Sydney, Australia, 2005, pp. 748- 755.

[11] S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. F. Gu, and M. Tyson, FRESCO: Modular composable security services for software-defined networks, presented at Network and Distributed Security Symposium, 2013.

[12] L7 filter project, http://l7-filter.sourceforge.net/Pattern-HOWTO, 2008.

[13] V. Sekar, M. K. Reiter, W. Willinger, H. Zhang, R. R. Kompella, and D. G. Andersen, cSamp: A system for network-wide flow monitoring, in Proc. 5th USENIX Symposium on Networked Systems Design and Implementation, San Francisco, USA, 2008, pp. 233-246.

[14] B. Anwer, T. Benson, N. Feamster, D. Levin, and J. Rexford, A slick control plane for network middleboxes, in Proc. Association for Computing Machinery, Hong Kong, China, 2013, pp. 147-148.

[15] Z. A. Qazi, C. C. Tu, L. Chiang, R. Miao, V. Sekar, and M. Yu, SIMPLE-fying middlebox policy enforcement using SDN, in Proc. Association for Computing Machinery, Hong Kong, China, 2013, pp. 27-38.

[16] K. Wang, Y. Qi, B. Yang, Y. Xue, and J. Li, LiveSec: Towards effective security management in large-scale production networks, in Proc. IEEE 32nd International Conference on Distributed Computing SystemsWorkshops, Macau, China, 2012, pp. 451-460.

[17] X. Wang, Z. Liu, Y. Qi, and J. Li, LiveCloud: A lucid orchestrator for cloud datacenters, in Proc. IEEE 4th International Conference on Cloud Computing Technology and Science, Taipei, China, 2012, pp. 341-348.

[18] VMWare Network security, http://www.vmware.com/products/nsx/resources.html, 2013.