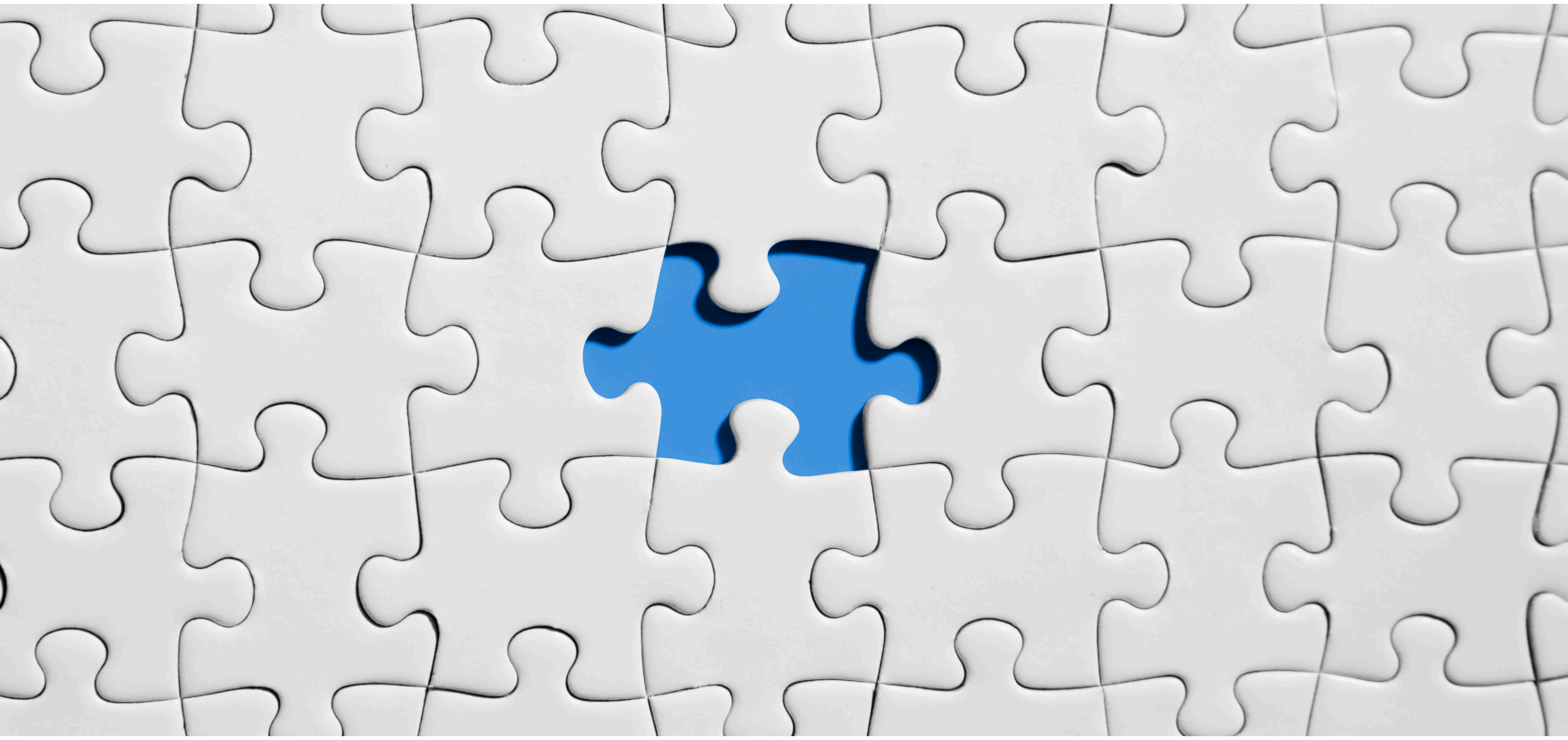
DELL Technologies

SECUREMLM – PRIVACY-AWARE MACHINE LEARNING MODEL



Dr. Shikha Pandey

Advisor, Customer/Technical Training

Dell Technologies

Shikha.Pandey2@emc.com

DELL Technologies Proven Professional

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

Table of Contents

Disclaimer: The views, processes or methodologies published in this article are those of the author. They do not necessarily reflect Dell Technologies' views, processes or methodologies.

Abstract

Machine learning (ML) has been increasingly applied in enterprises to build better and more intelligent products and business strategies. Likely there is no industry ML has not been a part of and its adoption is increasing. With the impact of ongoing digital transformation, cloud computing is utilizing ML concepts not for a radical but for a progressive change. In numerous regards, the transformative union of ML and cloud is poised to accelerate change and be a source of innovation.

This article focuses on the importance of Machine Learning in modern technologies such as multi-cloud. Along with use of Machine Learning in multicloud, we propose a framework known as “SecureMLM”, a novel privacy-aware machine learning model capable of protecting data privacy at time of resource migration.

The proposed model is designed to enhance privacy by partitioning the computation between the client and the cloud. SecureMLM leverages dataflow graph semantics to evaluate and judiciously select a partition point, and then apply homomorphic encryption (HE) encryption algorithm during data migration.

According to best of the knowledge, the SecureMLM-Privacy-aware machine learning model for multicloud is a unique mechanism to ensure privacy to all cloud environments, not only to multicloud environments. The proposed method will not only be designed to ensure end-to-end-security during data migration, but also achieve the goal of fulfilling the vision of any device, any application, and any cloud message that enable the customers to simplify their IT operations, and increase agility, efficiency, and productivity.

Keywords: Machine Learning, Multi-cloud, Load balancing, Security.

Introduction

The rise of Machine Learning techniques is changing the way IT professionals approach data center operations and management. The possibilities are endless from predicting load, to reducing time to deploy, to lowering operational cost. There has been no doubt that Machine Learning is transforming the data center and so the multi-cloud operations and its management.

The amalgamation of Machine learning with multi-cloud will help to build up the predictions and analyze the situations to perform resource provisioning tasks more efficiently.

With the rapid increase of user access, load balancing in data center has become an important factor affecting stability of the cloud clusters. As the demand is increasing, the issue of load fluctuation is greatly affecting the performances. Therefore, load balancing, which aims at alleviating resource migration, is becoming increasingly important in multi-cloud environment.

Also, as Machine Learning becomes more pervasive, privacy concerns become paramount on the adopting technologies. Therefore, the proposed model provides the unique mechanism to ensure privacy in the multi-cloud environment. The use of deep reinforcement learning (DRL) will make our model more intelligent.

SecureMLM leverages dataflow graph semantics to evaluate and judiciously select a partition point, and then apply homomorphic encryption (HE) encryption algorithm during data migration.

Related work and Research perspective

This article analyzes various scheduling methods that reduce energy consumption. The analyzed algorithm reduces energy consumption to some extent, so thee author proposed a" crossbreed algorithm" in order to minimize the energy consumption. Round robin, FCFS and Priority-based scheduling algorithms are the scheduling algorithm which are analyzed. [7]

Pustchi. N et.al have proposed a fine-grained cross-cloud domain trust model with resource sharing capabilities between domains across distinct homogeneous clouds. They have implemented a proof of concept with extending OpenStack identity and federation services to support cross-cloud domain trust where the adopted approach does not introduce any authorization overhead within current models. Also, the entire mechanism depends upon the Mapping rules. [8].

Elkhatib.Y analyzed the need for development of APIs for cross-cloud. According to him, the application deployed in cross-cloud consumes more than one cloud API under a single version of the application[9].

Huioon K. et.al also focus on the need of integrated APIs. They have developed a mechanism to overcome the issue of heterogeneity of the APIs by developing integrated cloud API in order to provide a RESTful access.[10].

Allam Q.et al proposed a resource sharing process between two different tenants (cross-cloud) with cloud resource mediation service, the entire mechanism defined by the activation, delegation, forward revocation, and backward revocation along with their formal verification.[11].

An "orchestration algorithm" to reach migration of a component between different providers in an agnostic way has been determined by Dur´an F. and Pimentel E. The main characteristics of the algorithm is that along with the stateless, it is too not bounded to any service level of any particular provider which overcomes vendor lock-in. To ensure agnosticity the proposed algorithm is built over the concept of trans cloud, i.e. bidimensional cross-cloud.[13].

Pucher A. proposed EXFed, an efficient cross-federation system for IaaS clouds that "migrates" process/application between different clouds. EXFed also provides ahead-of-time certainty about resource availability despite retaining individual clouds' ability to preempt foreign workload after admission[14].The paper determines the extensions to the Federated CloudSim framework that considerably improve simulation and evaluation of cross-cloud. Service-level agreements (SLAs), scheduling and brokering strategies on various levels have been widely used for the purpose of evaluation [15]. A cross-layer scheduling framework is proposed for the purpose of resource allocation. Their approach computes the placement/allocation and routing paths for the new job. The process of routing adopted for determination of routing path is between structured and random topology [16].

The work of Theng D., and Hande P. deals VM images scheduling in a cross-cloud computing environment. An efficient approach for VM management is proposed and implemented to overcome the issue of cross cloud scheduling. Factorizing self-scheduling (FSS) and heterogeneous factorizing scheduling (HFSS) are two scheduling proposed [17]. An approach based on self-organizing a multi-agent system to achieve cross-cloud services management, including service provision at the tenant-end and services aggregation at the cloud-end, clouds services are managed by a series of agents capable of autonomously accessing managed services. The paper details the architecture, mechanisms, and algorithms to implement aggregation and provision of services in cross-clouds. The author also develop a relevant cross-cloud services management platform – CloudMan – upon which several experiments based on the public data sets have been conducted. Experimental results show the efficiency and usability of our proposed approach [18].

Goonasekera N et.al. proposed an open source Python library – CloudBridge – that provides a simple, uniform, and extensible API for multiple clouds.

As the cloud is extensively used for deploying applications, it is important to seamlessly utilize resources and services from multiple providers. Proprietary vendor APIs make this challenging and lead to conditional code being written to accommodate various API differences, requiring application authors to deal with these complexities and test their applications against each supported cloud.

Challenges

Resource allocation is an important and challenging issue due to:

- **Variability:** Variability of data center network induces unpredictable application performance concerns at the time of resource allocation at the dispersed nodes.
- **Flexibility and Portability**: Use of proprietary vendor APIs and vendor lock-ins has not only led to limited flexibility and portability but because of it, resource sharing and utilization in aggregated cloud platforms has become difficult. It also provides limited flexibility for tenants to manage their communication.
- **Security:** Data center networks do not restrict the communication pattern and bandwidth use of each application, making the network vulnerable to attacks.
- **Governance, Risk, and Compliance**: Since the cloud environment involves communication between different cloud platforms, it must abide to the changes in the communication behavior,

semantics, charging models, and SLA terms. The communication becomes important during acquisition of load information.

- **Heterogeneous nature:** The heterogeneous nature of the cloud environment make allocation and selection decision troublesome.[6][7]
- Lack of complete control of underlying hardware resources to their user.

Proposed Work

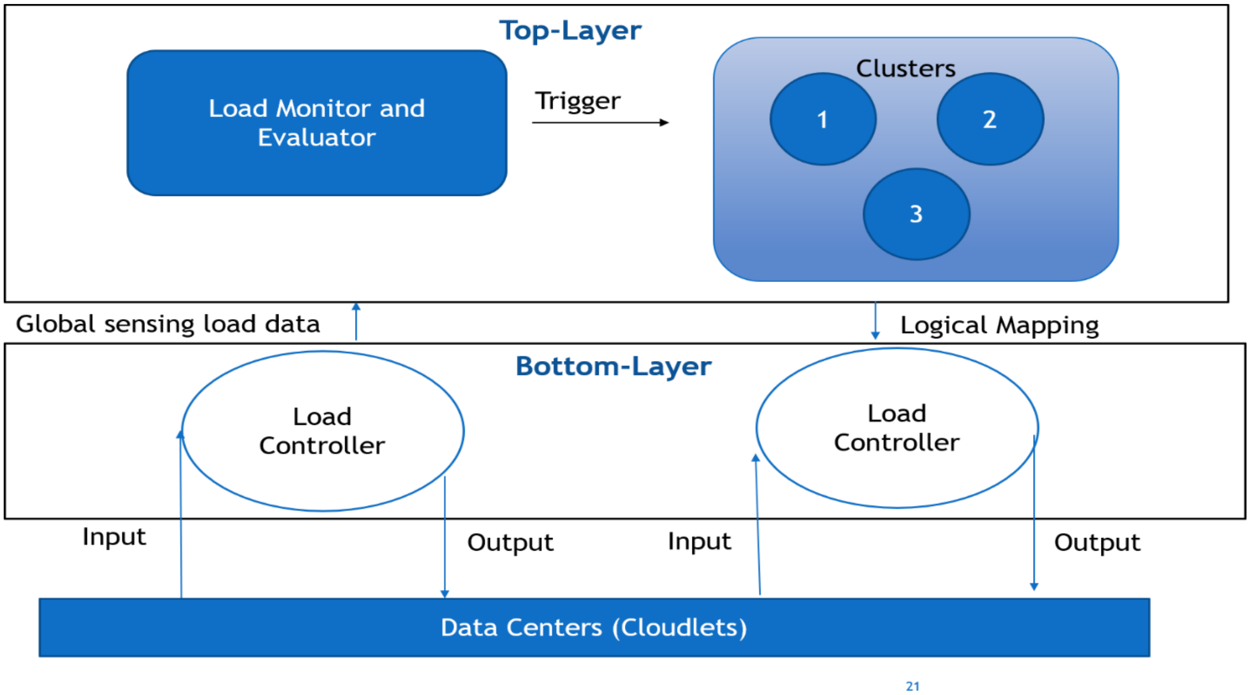
In our proposed work, we present a Secure Machine Learning Model ("SecureMLM") which develops an end-to-end security solution during data migration in multi-cloud environments by using the concept of Multi-level security. The presented model is designed to enhance privacy by partitioning computation between the client and the cloud.

SecureMLM leverages dataflow graph semantics to evaluate and judiciously select a partition point, and then apply homomorphic encryption (HE) algorithm during data migration. The partition point is selected with consideration of not only ensuring privacy but also enhancing overall performance compared to traditional resource migration techniques by adopting reinforcement learning (RL) method which analyze and predicts the processing load of a data center based on the environmental condition of the data center and the VMs processing time.

Architecture

The proposed model is divided into two layers; a centralized load-driven clustering controller at the top layer and several self-automated load balancing controllers at the bottom layer. The use of the hierarchical structure helps decouple non-critical nodes with the critical nodes and control and large-scale load balancing for multi-cloud environment in an automated manner.

As shown in figure below:



The top layer aims to segregate the critical nodes and non-critical nodes into a bunch of separate clusters according to their historical load levels. This dynamic grouping of critical and non-critical nodes is performed periodically and upon the global load variations in the data centers.

The clustering at this level depends upon the load-based initialization, which is either based on the detection of load hotspots (highly overloaded, loaded) or on position of virtual machines, which aims to group the load hotspot with their nearby hotspot based on the cluster distance.

We also propose to choose the top N load hotspots as the initial partition point in order to efficiently offload the load and achieve load balancing. The selection of this initial cluster partition point can largely influence the clustering result. Given the list of partition points from the initialization phase, we can easily group the nodes for subsequent balancing.

The bottom layer aims to balance the load within each cluster by implementing the Q-learning algorithm which helps find the optimal action-selection policy using a Q function.

Procedure

As seen in the image, load information from different data centers or cloudlets is provided as input to the bottom layer where the controller forwards the information to top layer of the architecture. The top layer clusters the information and provides the information back to the lower layer which applies the Q-learning algorithm to balance and further process the load.

In this way, the top layer adapts to the dynamic global traffic fluctuations from a macroscopic view, while the bottom layer tunes the intra-cluster load distribution at a finer level.

The hierarchal architecture provides a better opportunity to apply multiple independent levels of security. Each security level is classified into categories of Sensitive and General and is associated with access rules and permissions. Our model classifies the critical nodes as Sensitive and non-critical nodes as General to further ease our process and also maintain the privacy.

To enhance the privacy and security of the proposed model we embedded the features of privacy homomorphism known as CDAP (Concealed Data Aggregation and Protection) at time of migration from bottom layer to top layer. Being an encryption transformation mechanism, direct calculation on cipher text is possible with symmetric or asymmetric encryption. Either technique can be applied to obtain cipher texts. In our work, we have used privacy homomorphism based on symmetric keys because of induced vulnerabilities and disadvantage of asymmetric key in distributed and virtualized environment.

Conclusion and Future work

With enormous changes happening in the development of both machine learning and cloud, the future seems increasingly tied together. In future, there will come a time where no cloud will exist without machine learning. Also, since the Cloud environment depends upon the large number of customized and interconnected nodes with the supporting feature of scalability and on demand request processing, there is a need for a proper resource allocation mechanism. The proposed mechanism not only efficiently handles the load balancing process but also helps build a framework for embedding security during the process of load balancing. How the process impacts other sets of evaluation values (fitness) can be carried out in future.

Bibliography

1.Bhujbal A. et.al, “Load Balancing Model in Cloud Computing”, International Journal of Emerging Engineering Research and Technology, Volume 3, Issue 2, PP 1-6, ISSN 2349-4395 ,2015.

2.Patel D. et.al, “Efficient Throttled Load Balancing Algorithm in Cloud Environment”, International Journal of Modern Trends in Engineering and Research, p-ISSN: 2393-8161, pp 463-480,2015.

3.Saba N. and Song A. et.al, “Grammatical Evolution Enhancing Simulated Annealing for the Load Balancing Problem in Cloud Computing”, Proceedings of the Genetic and Evolutionary Computation Conference 2016, pp.997-1003, ISBN: 978-1-4503-4206-3, ACM,2016.

4. Gangwar I.et.al ,”Juxtaposition of Load Balancing Algorithms in Cloud Computing using Cloud Analyst Simulator”, International Journal of Computer Applications (0975 – 8887) Volume 97– No.2, pp 21-26, 2014

5. Paya A. and Marinescu A., “Energy-aware Load Balancing and Application Scaling for the Cloud Ecosystem”, IEEE TRANSACTIONS ON CLOUD COMPUTING, Issue: 99, ISSN: 2168-7161,2015.

6. Upadhyay A.et.al, “The-impact-of-network-parameters-in-cloud-environment-A-detailed-analysis”, International Journal of Scientific & Engineering Research, Volume 7, Issue 9, ISSN 2229-5518, pp 613-618 ,2016

7. Upadhyay A.et.al, “Suboptimal mechanism for load balancing in cloud environment”, 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 2017 Chennai

7.A cross cloud scheduling algorithm at SaaS level on Rack Space, Go Daddy and Azure platforms

2016 International Conference on Computing, Communication and Automation (ICCCA)

8.Multi Cloud IaaS with Domain Trust in OpenStack

Navid Pustchi ,Farhan Patwa ,Ravi Sandhu, CODASPY’16 March 09-11, 2016, New Orleans, ACM ISBN 978-1-4503-3935-3/16/03. DOI: http://dx.doi.org/10.1145/2857705.2857745,pp 121-123

9. Elkhatib Y, Mapping Cross-Cloud Systems: Challenges and Opportunities, https://www.usenix.org/node/196337

10 Kim H. et.al, Experience in Practical Implementation of Abstraction Interface for Integrated Cloud Resource Management on Multi-Clouds, KSII Transactions on Internet & Information Systems. Jan2017, Vol. 11 Issue 1, p18-38. 21.

11. Alam Q et.al, A Cross Tenant Access Control (CTAC) Model for Cloud Computing: Formal Specification and Verification IEEE Transactions on Information Forensics and Security ,Volume: 12, Issue: 6, 2017.

12.www. Vm ware blog com. https://www.vmware.com/radius/cross-cloud-introduction

13. Dur´an F. and Pimentel E., Component-wise Application Migration in Bidimensional Cross-Cloud Environments.

14. A Pucher, EXFed: Efficient Cross-Federation with Availability SLAs on Preemptible IaaS Instances, IEEE International Conference on Cloud Engineering (IC2E), IEEE,2017.

15. Andreas Kohne et.al, Financial Evaluation of SLA-based VM Scheduling Strategies for Cloud Federations**.** Crosscloud'17 Proceedings of the 4th Workshop on Cross Cloud Infrastructures & Platforms Article No. 1 ISBN: 978-1-4503-4934-5,2017

16. Alkaff H et.al, Cross-Layer Scheduling in Cloud Systems Cloud Engineering (IC2E), 2015 IEEE International Conference on

17. Theng D et.al, VM Management for Cross-Cloud Computing Environment, pp 731-735.IEEE ,2012 International Conference on Communication Systems and Network Technologies,2012.

18. Goonasekera N , Cloud Bridge: A Simple Cross-Cloud Python Library (ACM),2015XSEDE16 Proceedings of the XSEDE16 Conference on Diversity, Big Data, and Science at Scale.

19.http://www.dummies.com/programming/cloud-computing/hybrid-cloud/types-of-workloads-in-a-hybrid-cloud-environment/

20. Wei Yi et.al, “Cost-optimal service selection approach for collaborative workflow execution in clouds”, IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD),IEEE , ISBN: 978-1-5090-1915-1 ,2016.

21. Kanit et.al. Visualizing Dataflow Graphs of Deep Learning Models in TensorFlow

IEEE Transactions on Visualization and Computer Graphics (Volume: 24 , Issue: 1 , Jan. 2018

23**.** Mingwei et.al. “Distributed machine learning load balancing strategy in cloud computing services”

https://link.springer.com/article/10.1007/s11276-019-02042-2

22. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security-enhanced_linux/mls

23.http://www.semdesigns.com/Products/DMS/FlowAnalysis.html

Dell Technologies believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL TECHNOLOGIES MAKES NO RESPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying and distribution of any Dell Technologies software described in this publication requires an applicable software license.