**Old Dominion University**

**School of Cybersecurity**

**Machine Learning in Cloud Computing Security**

**Research/Term Paper**

**Alexander Bonhomme - 01214110**

**Applied Machine Learning in Cybersecurity – CYSE 420/520**

**Professor Kami Islam**

**12/5/2021**

**ABSTRACT**

Cloud security, or cloud computing security, is a set of policies, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure. Machine Learning is the development and use of computer systems that can learn and adapt by inference. This inference implements algorithms and statistical models to analyze patterns in given (or not given) data. This whole process is the process of automatic analysis model construction. Being able to move computing into the “Cloud” makes computer processing so much easier. While it is more convenient to operate, cloud computing may present new safety hazards/problems that may affect the integration of Machine Learning into the cloud.

**INTRODUCTION**

Recent advances in Machine Learning (ML) have enabled the use of technology in a broad range of applications, significantly outperforming previous state-of-the-art methods in various fields, including image classification, face recognition, and object detection. As a result, each of these ML techniques, particularly deep learning (DL)–based techniques, requires a large amount of training data to achieve various specific tasks with a high level of performance. Refer to the figure below for tasks that may be accomplished using Machine Learning in the Cloud.



Figure 1: ML tasks that may be outsourced

Training Deep Learning models on large datasets is typically done using a high-performance graphics processing unit (GPU) and a tensor processing unit. Given the cost of GPU and tensor processing units and the fact that small businesses and individuals cannot buy such computing resources, deep model training is typically outsourced to the cloud. Operating systems such as Tensorflow in Google Colab is what helps to offset those costs as Machine learning in cloud computing continues to grow.

**PROBLEM**

The main challenge with these methods is to get an unbiased and distortion-free dataset in real time. Many datasets are internal and may not be shared for data protection reasons or it may even lack certain statistical characteristics. For this reason, researchers prefer to generate datasets for training and testing purposes in simulations or in closed experimental settings that may lack integrity. Machine learning models trained on a single dataset usually create a semantic gap between the results and their application. There is a lack of research demonstrating the effectiveness of these models across various datasets that may be captured in different environments. The robustness of machine learning models needs to be tested, especially under a variety of operational conditions that are prevalent in cloud scenarios.

**SOLUTIONS**

Whether you are attempting to utilize Machine Learning in Cloud Computing as an organization or individually, there are certain things you should know. As valuable as machine learning is, this value cannot be recognized when ML is applied to a system that doesn’t benefit from making predictions based on patterns of data. Business intelligence can be come smarter as machine learning continues to develop in the cloud. With ML, AI can use cloud data, which may help enterprises gain insight regarding real-time situations. Therefore, by integrating machine learning into enterprises’ cloud infrastructure, it may be easier to predict future outcomes and use transfer learning.

****

Figure 2: Ways to integrate ML into CC services for Businesses

Regarding the specific algorithms used, there are many that can be applied to cloud computing specifically. Although, in a nutshell, no one algorithm works for every problem, they all have their strengths and weaknesses for supervised and unsupervised learning. The main ones that can be used toward cloud computing includes Linear regression and Classification. Linear regression, one of the most commonly understood algorithms, uses predictive modeling to cultivate accurate predictions. Classification is also a predictive modeling problem where a class label is predicted for a given example of input data. Classification can work in cloud computing in how the clouds themselves are parsed into public, private, and hybrid clouds. One can also determine the type of data being used in those clouds using classification machine learning models as well. This can help to reduce the amount of memory and RAM used.

**CONCLUSION**

Cloud security, or cloud computing security, is a set of policies, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure. Machine learning is the development and use of computer systems that can be learned and adapted through reasoning. This conclusion is implemented using algorithms and statistical models to analyze patterns of specified (or unspecified) data. This entire process is the process of building an automated analysis model. The ability to move computing to the "cloud" makes computing much easier. Although more convenient to use, cloud computing can introduce new security risks / issues that can affect the integration of machine learning into the cloud. There are certain tasks and ML algorithms that can combat these issues, but it is up to the user to determine what algorithms to use to find solutions to each problem.

**REFERENCES**

Butt, Umer Ahmed, et al. “A Review of Machine Learning Algorithms for Cloud Computing Security.” *MDPI*, Multidisciplinary Digital Publishing Institute, 26 Aug. 2020, https://www.mdpi.com/2079-9292/9/9/1379/htm.

“Feasibility of Supervised Machine Learning for Cloud Security.” *IEEE Xplore*, https://ieeexplore.ieee.org/abstract/document/7885853?casa\_token=CZmUj6Ha7rUAAAAA%3ADpwHY\_vQMlweGuzm1c3zGqyxfP6ieaPDvYb1C3TiRXI6YhoOBocpBZd4AcO-hDgjNqnhtt9O19Q.

Gumaste, Pavan. “Impact of Machine Learning on Cloud Computing.” *Whizlabs Blog*, 28 Jan. 2021, https://www.whizlabs.com/blog/machine-learning-and-cloud-computing/.

Label Your Data. “What Is Mlaas – Machine Learning as a Service.” *High Quality Data Annotation for Machine Learning*, Label Your Data, 21 Apr. 2021, https://labelyourdata.com/articles/machine-learning-as-a-service-mlaas.

Le, James. “The Top 10 Machine Learning Algorithms Every Beginner Should Know.” *Built In Beta*, https://builtin.com/data-science/tour-top-10-algorithms-machine-learning-newbies.

Linthicum, David. “Machine Learning in the Cloud: How It Can Help You Right Now.” *TechBeacon*, TechBeacon, 22 Jan. 2019, https://techbeacon.com/enterprise-it/machine-learning-cloud-how-it-can-help-you-right-now.

Qayyum, Adnan, et al. “Securing Machine Learning in the Cloud: A Systematic Review of Cloud Machine Learning Security.” *Frontiers*, Frontiers, 1 Jan. 1AD, https://www.frontiersin.org/articles/10.3389/fdata.2020.587139/full.