UNIVERSITY OF WESTMINSTER

INFORMATICS INSTITUTE OF TECHNOLOGY

University of Westminster

Trends in Computer Science

4COSC008C

Machine Learning

2.d. Overview of Machine Learning. What are the opportunities it brings to developers? What threats does it pose to society?

Name –K.D.A.Perera

UOW Number - W2052093

IIT Number – 20220794

Group Members:

Name	UOW Number	Student ID
Disandu Perera	W2052093	20220794
Yuthmika Gamage	W2053137	20220952
Banusha Kalhara	W2052094	20220801
Tharusha Jayawardena	W2052103	20220910

Table Of Contents

Table of Contents

1. ACKNOWLEDGMENT

I would like to express my sincere gratitude to the University of Westminster and the Informatics Institute of Technology (IIT) for their excellent support and provision of resources, which were essential to the successful completion of this study. We would especially like to thank Dr. M. Chondrogianni for all of her help and advice on this project.

In addition, I would like to express my gratitude to my distinguished colleagues whose knowledge and perspectives enhanced the caliber of this study. Their assistance and cooperation were really helpful.

I also want to thank my parents from the bottom of my heart for their constant support and help with the schoolwork. Their support and considerate input have been invaluable to me throughout my academic career.

1) INTRODUCTION

The foundation of machine learning is the development of statistical models that, given more data to work with, may learn from the data and become more predictive over time. When a machine learning algorithm is given enough examples from a data source (referred to as training data), it may predict a property of interest. It can also predict a property of interest when it is given a new, unseen example. This can be done by employing several methods or by calibrating internal parameters based on well-known examples.

Thus, "the ability for computers to learn without being explicitly programmed" is a straightforward definition of machine learning. Machine learning algorithms create behavioral models and use those models as a foundation for future predictions based on fresh incoming data through mathematical methods.

Whether we realize it or not, machine learning plays a crucial role in our daily lives. You interact with machine learning every time you visit websites like YouTube and Amazon.com, which provide tailored suggestions. This implies that ML algorithms determine which things to show you on websites depending on your interests. Not only that, but ML-based comment moderation is available for flagging spam or harmful remarks and more. ML is used to generate translations and captions on websites such as YouTube.

The advancement of self-driving cars is frequently tied to machine learning. They would predict different situations along the route, such heavy traffic or crossing paths, using the information gathered by the automobile.

A number of industries, including finance, commerce, and medical diagnostics, are also profiting from this new trend. Machine learning aims to assist companies in the security domain by enhancing their threat analysis and incident response capabilities. The software of today is based on data and machine learning algorithms.

2) OVERVIEW OF MACHINE LEARNING

2.1.Opportunities It Brings To Developers?

1) Threat anticipation

- One of the core features of machine learning, as previously said, is the ability of machine learning models to analyze enormous amounts of data, both structured and unstructured. This can dramatically improve analytical capabilities in risk management and compliance by empowering risk managers across many institutions to identify risks more quickly and effectively, make more informed decisions, and reduce the likelihood of events. Using machine learning techniques will enable businesses to identify harmful activities more rapidly and prevent attacks before they begin.

2) Enhance human learning.

- The fundamental tenet of machine learning in security is that it assists human analysts in all facets of their work, such as vulnerability assessment, network analysis, and the detection of malicious assaults. Since the model will supply pre-analyzed data, machine learning will enable the human brain to conduct further analysis. As such, human learning will begin at a earlier stage than it typically does.

3) Automation of tasks

- The advantage of machine learning is that it can automate tedious and repetitive jobs, freeing up personnel to concentrate on more crucial work. The goal of machine learning should be to eliminate the need for humans to perform routine, Significant decision-making tasks. Give the machine the repetitive tasks, like opening doors, so that people can spend more time on important and strategic tasks.

4) Finance

- Machine learning has also been extremely beneficial to the banking industry. It is employed in algorithmic trading, fraud detection, and credit scoring. According to a recent survey, 56% of global executives claimed that financial crime compliance processes had used machine learning and artificial intelligence.

2.2.What threats does it pose to society?

1) Adversarial attacks

- A traditional adversarial strategy entails providing inputs designed to fool a machine learning model that has been trained. It entails meticulously modifying the source image so that the changes are barely perceptible to the unaided eye. They can be viewed as optical illusions by machines. An adversarial image is a modified image that is classified wrongly by a classifier while the original image is classed properly.

- The possibility of performing adversarial attacks on various systems, including CCTV footage, presents security problems. Incidents may go unreported only by introducing a certain amount of noise into the photos, since they would not be appropriately categorized. That can be executed even in the event that the attacker is unable to access the underlying model, which increases its risk.

2) Data poisoning

- Data poisoning targets the data used for machine learning training, in contrast to traditional adversarial attacks. Data poisoning purposefully introduces undesirable correlations into the model by altering the training data, as opposed to searching for them in the parameters of the trained model. It would be quite difficult to identify any tainted data within the sets immediately, which could lead to misunderstanding of the data, because machine learning frequently works with vast amounts of data.

3) High error-susceptibility

- Although autonomous, machine learning is prone to mistakes. Imagine using tiny enough data sets to train an algorithm that cannot be inclusive. From a biased training set, you obtain biased predictions. As a result, clients see irrelevant advertisements. For a considerable amount of time, these mistakes in machine learning might initiate a series of mistakes that are difficult to discover. Furthermore, when they are detected, it takes a while to identify the problem's origin and much longer to fix it.

4) CONCLUSION

- Machine learning, like many other cutting-edge developing technologies, has benefits and drawbacks depending on how and by whom it is used. There's no denying that technological advancement and adaptation will pick up steam in the upcoming years. Consequently, rather than rejecting it, the best course of action for moving forward may be to train people to avoid the vast majority of potential hazards.

5) CRITICAL EVALUATION

- Machine learning is a two-sided coin. Its remarkable ability to recognize patterns, automate procedures, and improve continuously offers opportunities for a variety of industries. The opacity of complex models and the field's over-reliance on high-quality data pose serious issues. Ethical problems including discrimination, privacy violations, and employment displacement are also insurmountable. While machine learning has great promise, its development and implementation must be done responsibly to maximize its benefits and minimize its drawbacks.

REFERENCES

Chang, S. S. (n.d.-b). Machine learning interviews. O'Reilly Online Learning. https://learning.oreilly.com/library/view/machine-learning-interviews/9781098146535/preface01.html

Machine Learning: opportunity or threat? (2022, September 13). https://www.entelec.eu/machine-learning-opportunity-or-threat

https://data-flair.training/blogs/advantages-and-disadvantages-of-machine-learning/

Cameron, I., Engell, S., Georgakis, C., Asprion, N., Bonvin, D., Gao, F., Gerogiorgis, D. I., Grossmann, I. E., Macchietto, S., Preisig, H. A., & Young, B. R. (2019b). Education in Process Systems Engineering: Why it matters more than ever and how it can be structured. Computers & Chemical Engineering, 126, 102–112. https://doi.org/10.1016/j.compchemeng.2019.03.036