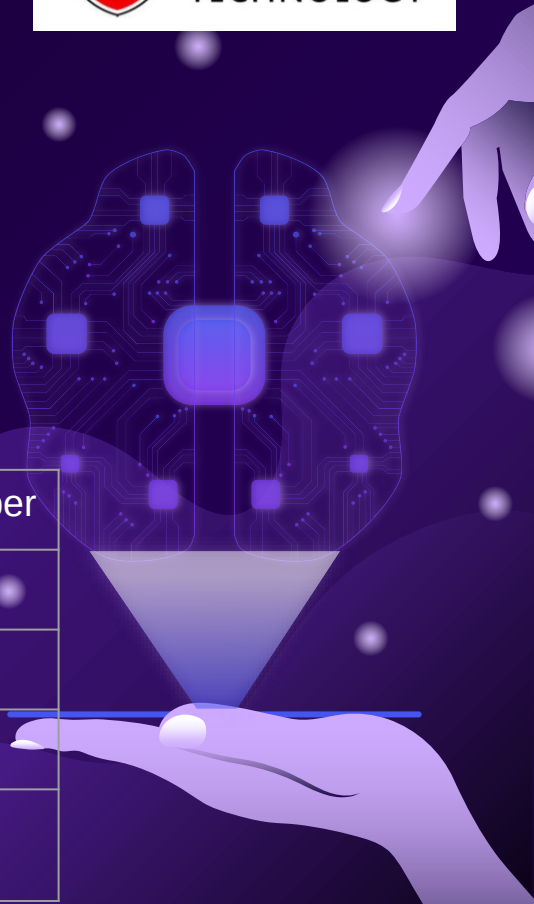
UNIVERSITY OF WESTMINSTER

INFORMATICS INSTITUTE OF TECHNOLOGY

Trends In Computer Science

4COSC008C

Machine Learning Threats And Opportunities



Group No-7

Full Name	UOW Number	IIT Number	Sub-Topic Number
Disandu Perera	W2052093	20220794	2.d.
Yuthmika Gamage	W2053137	20220952	2.b.
Banusha Kalhara	W2052094	20220801	2.a.
Tharusha Jayawardena	W2052103	20220910	2.c.

01. Introduction

- Machine learning (ML) is the process by which computers pick up knowledge from data without explicit programming.
- Rather than using hardcoded rules, algorithms use training data to predict outcomes.
- It is described as the capacity of computers to learn without explicit programming, whereby algorithms make hard-coded rule-based predictions based on training data.
- Machine learning is a revolutionary technology that is changing entire sectors and having a significant impact on day-to-day living
- Machine learning is present in everything we do on a daily basis, from personalized suggestions to driverless automobiles.
- In order to promote wise decision-making, our mission is to investigate the many effects of machine learning on security and society.

02. Opportunities

1) Task Automation:

- Security experts may concentrate on high-value work since machine learning automates tedious and repetitive jobs.
- Security operations become more efficient overall when workflows are streamlined and manual errors are decreased thanks to automation.

2) **Enhanced Risk Management**:

- Organizations can evaluate large amounts of organized and unstructured data thanks to machine learning, which enhances risk management and compliance.
- Businesses can improve their risk management and compliance procedures by using sophisticated algorithms.
- **Businesses can more quickly and effectively identify hazards by utilizing sophisticated algorithms and making well-informed decisions.**

3) **Industry-Specific Applications**:

- Better patient outcomes are achieved in the healthcare industry with machine learning, which also enhances medical imaging accuracy, anticipates disease outbreaks, and customizes treatment regimens.
- With machine learning in algorithmic trading, fraud detection, and credit scoring, the finance industry may improve operational effectiveness and risk management.

4) **Innovation in Transportation**:

- Transportation technology is advancing thanks to machine learning, which makes it possible to create driverless cars and optimize transportation networks.
- Road infrastructure management is safer and more effective when machine learning experts work together with transportation authorities.

3. Threats

1)Adversarial Attacks:

- Machine learning models are the target of adversarial attacks, which alter inputs to provide false results.
- These assaults have the potential to undermine machine learning systems' integrity, producing inaccurate results and judgments.

2)Data Poisoning:

- In order to affect the behavior of machine learning models, maliciously altering training data is known as data poisoning.
- Attackers can introduce false or biased data into training datasets, which can distort predictions and jeopardize system integrity.

3)High Error-Susceptibility:

- Errors can occur in machine learning systems, particularly when they are trained on incomplete or biased datasets.
- Decision-making fairness and dependability can be negatively impacted by biases in training data that produce discriminating results.

4)Privacy Concerns:

- Privacy concerns arise because machine learning algorithms frequently rely on enormous datasets that contain sensitive information.
- Insufficient data security protocols may result in unapproved access or improper use of personal information, jeopardizing individuals' right to privacy.

4. Critical Evaluation

- Technology and society are shaped by a dual reality of opportunities and risks, which is embodied in machine learning. Achieving a balance between utilizing its innovative potential and reducing its inherent hazards is crucial. A thorough grasp of the moral, societal, and security ramifications of machine learning technology is necessary for responsible innovation.

- Effective navigation of the complicated world of machine learning requires cooperation amongst stakeholders, including developers, legislators, and end users. In this quickly changing area, it is critical to continuously adapt and improve in order to handle new threats and problems.

- Not withstanding these difficulties, machine learning's revolutionary potential is extremely promising for promoting progress in a variety of fields. We can fully utilize machine learning to build a more safe, just, and prosperous future for everybody if we seize opportunities and take early measures to mitigate threats.

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

- 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