Chapter 4
Applications of Machine Learning in Cyber Security Domain

Sailesh Suryanarayan Iyer
R. B. Institute of Management Studies, India

Sridaran Rajagopal
Marwadi University, India

ABSTRACT

Knowledge revolution is transforming the globe from traditional society to a technology-driven society. Online transactions have compounded, exposing the world to a new demon called cybercrime. Human beings are being replaced by devices and robots, leading to artificial intelligence. Robotics, image processing, machine vision, and machine learning are changing the lifestyle of citizens. Machine learning contains algorithms which are capable of learning from historical occurrences. This chapter discusses the concept of machine learning, cyber security, cybercrime, and applications of machine learning in cyber security domain. Malware detection and network intrusion are a few areas where machine learning and deep learning can be applied. The authors have also elaborated on the research advancements and challenges in machine learning related to cyber security. The last section of this chapter lists the future trends and directions in machine learning and cyber security.

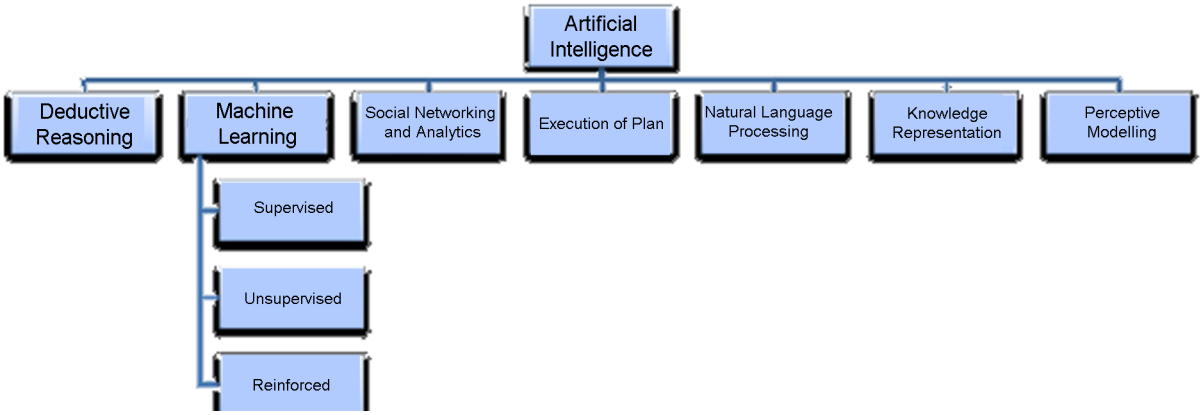
INTRODUCTION

The digital revolution is transforming the global scenario. Desktop are being replaced by Laptops and Laptops by Mobiles and Tablets. Internet which was considered a luxury before a few decades has become the necessity of the hour. Social Media and online transactions are transforming ordinary people to smart people through Smart devices. The Information Technology is touching the life of the urban as well as rural population. Digi-Farming has become a reality with Companies and Government implementing Sensors to help identify type of Soil, Soil moisture, temperature, humidity and leaf wetness.

DOI: 10.4018/978-1-5225-9611-0.ch004

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Figure 1. Artificial intelligence/machine learning classification



Water Conservation can be increased by spraying water only where required. Smart Devices are replacing mundane tasks bringing about a 360° transformation in the way business and social networking is done. Technical concepts like Cyber Crime, Cyber Security, Artificial Intelligence, Machine Learning and Deep Learning are soon invading workplaces. Artificial Intelligence is the ability of machine to behave like a human being, Machine Learning can be considered an AI variant wherein learning and improving from previous experience takes place.

Figure 1 shows the classification of AI and Machine Learning. AI can be classified into Deductive Reasoning, Machine Learning, Social Analysis, Natural Language Processing (NLP), Knowledge Representation and Perceptive Modeling (Sanjeevi, 2017).

Intelligent people can be defined as those possessing important qualities as knowing, learning, understanding, communicate, judge, think etc. Artificial Intelligence is the application of human qualities to solve real life problems which previously only humans solved. Artificial Intelligence is used for solving problems like Computer Vision and Image Processing, Robotics, etc. to name a few. AI's goal is to make computers/computer programs smart enough to imitate the human mind behavior. Vertical Artificial Intelligence concentrates on one job only. Horizontal Artificial Intelligence concentrates on many tasks at the same time (Maruti Tech Labs, 2019).

Machine Learning (Maruti Tech Labs, 2019) can be considered as a subset of Artificial Intelligence. Machine Learning consists of designing and applying algorithms capable of learning from historical occurrences. Some of the major applications of Machine Learning are Self Driving Cars, face detection and recognition, Marketing Campaigns, Credit card or banking fraud detection. The world's finest player of Chess Gary Kasparov was defeated in his own turf by IBM's product Deep Blue. Machine Learning also has various applications in product recommendations e.g. Book recommendations.

Figure 2. represents the classification of machine learning (InfoTechLead, n.d.)

Machine Learning can further be classified into three (3) categories:

1. **Supervised Learning:** In Supervised Learning, rules are provided to the system. The Supervised algorithm analyzes the data and produce inferences. e.g. Credit Card fraud detection is Supervised Learning application. Trained data is required for Supervised Learning. Some of the examples of Supervised Learning include Speech automated system in mobile captures voice and trains to

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/applications-of-machine-learning-in-cyber-security-domain/235037

Related Content

Accuracy in Parallel Dynamic Task Allocation for Multi-Robot Systems Under Fuzzy Environment
Teggar Hamza, Senouci Mohamedand Debbat Fatima (2021). *International Journal of Fuzzy System Applications (pp. 1-20).*
www.irma-international.org/article/accuracy-in-parallel-dynamic-task-allocation-for-multi-robot-systems-under-fuzzy-environment/277108

Applications of Machine Learning in Food Safety
Rakesh Mohan Pujahariand Rijwan Khan (2022). *Artificial Intelligence Applications in Agriculture and Food Quality Improvement (pp. 216-240).*
www.irma-international.org/chapter/applications-of-machine-learning-in-food-safety/307427

Statistical Study of Machine Learning Algorithms Using Parametric and Non-Parametric Tests: A Comparative Analysis and Recommendations
Vijay M. Khadse, Parikshit Narendra Mahalleand Gitanjali R. Shinde (2020). *International Journal of Ambient Computing and Intelligence (pp. 80-105).*
www.irma-international.org/article/statistical-study-of-machine-learning-algorithms-using-parametric-and-non-parametric-tests/258073

The Impact of Federated Learning on AI-Enhanced Healthcare Delivery
Archana Shahiand Amit Mittal (2024). *Pioneering Smart Healthcare 5.0 with IoT, Federated Learning, and Cloud Security (pp. 57-66).*
www.irma-international.org/chapter/the-impact-of-federated-learning-on-ai-enhanced-healthcare-delivery/339427

Optimal Tuning Strategy for MIMO Fuzzy Predictive Controllers
Adel Taeiband Abdelkader Chaari (2015). *International Journal of Fuzzy System Applications (pp. 87-99).*
www.irma-international.org/article/optimal-tuning-strategy-for-mimo-fuzzy-predictive-controllers/133127