NOVEMBER 2023

Raising the red flag

The role of Artificial Intelligence (AI) in benefit fraud detection

CONTENTS

INTRODUCTION

Not only does benefits fraud affect health insurance companies, it also financially impacts plan members and plan sponsors, resulting in higher premiums for everyone. Even though fraudulent transactions represent a small fraction of activity within an organization, they can cause significant financial losses.[1]

Alberta Blue Cross® is embracing the future of technology. We pride ourselves in keeping up to date with solutions that allow us to provide sustainable, cost-effective plans to our customers.

With advancements in digital technology, the opportunities for fraudulent transactions have grown.

AI makes it easier to detect benefits fraud. Traditional rule-based systems and manual processes struggle to keep up with evolving fraud strategies. AI models continuously learn and adapt, making it highly effective in detecting known and emerging fraud schemes.

> "
>
> *With its ability to analyze vast amounts of data, identify patterns and anomalies and make decisions faster, AI has the power to transform the fraud detection process for the better.*
>
> **Nazanin Tahmasebi**
> Manager, Analytics & Reporting, Claims Audit & Investigation Services

WHAT IS AI AND WHAT IS MACHINE LEARNING?

AI stands for **Artificial Intelligence**. AI technology allows machines to do things that typically only humans could do, making them smarter and more capable.[2]

Machine learning is a subset of AI that refers to teaching computers to identify patterns from historical data, without direct human intervention. Machine learning trains algorithms to make decisions and predictions without being directly programmed to do so.[3]

Machine learning also includes developing models that can analyze data to help computer systems become more accurate over time. This continuous improvement on a given task represents the learning in machine learning. Think of it like training a dog— the more times you practice a trick, the better the dog becomes. The same goes for machine learning, the more data a machine learning algorithm encounters, the more effective and accurate it becomes at completing a task.

Machine learning methods are particularly good at helping computers look at a complex set of data and model the underlying patterns that generated it. The models generated through machine learning can then be applied to new data to predict future outcomes.

MACHINE LEARNING VERSUS TRADITIONAL PROGRAMMING

Traditional programming, unlike machine learning, is a rule-based approach. The programmer accounts for each step required to solve a problem or complete a task. Machine learning, on the other hand, is inspired by how humans learn—the programmer feeds data to the algorithm and lets the machine figure out how to solve the problem by itself.

Many organizations still rely on rule-based systems as their primary tool for fraud detection. While rules are effective in uncovering known patterns, they may not be as efficient in detecting unknown fraud schemes or adapting to new patterns.[4]

Fraud and the people who commit it are constantly evolving. This means we tend to rely more on machine learning than traditional programming. By learning from and modelling historical data, machine learning algorithms can identify abnormal and risky activities and apply rules better than human beings and traditional programming can.

Machine learning is inspired by how humans learn—the programmer feeds data to the algorithm and lets the machine figure out how to solve the problem by itself.
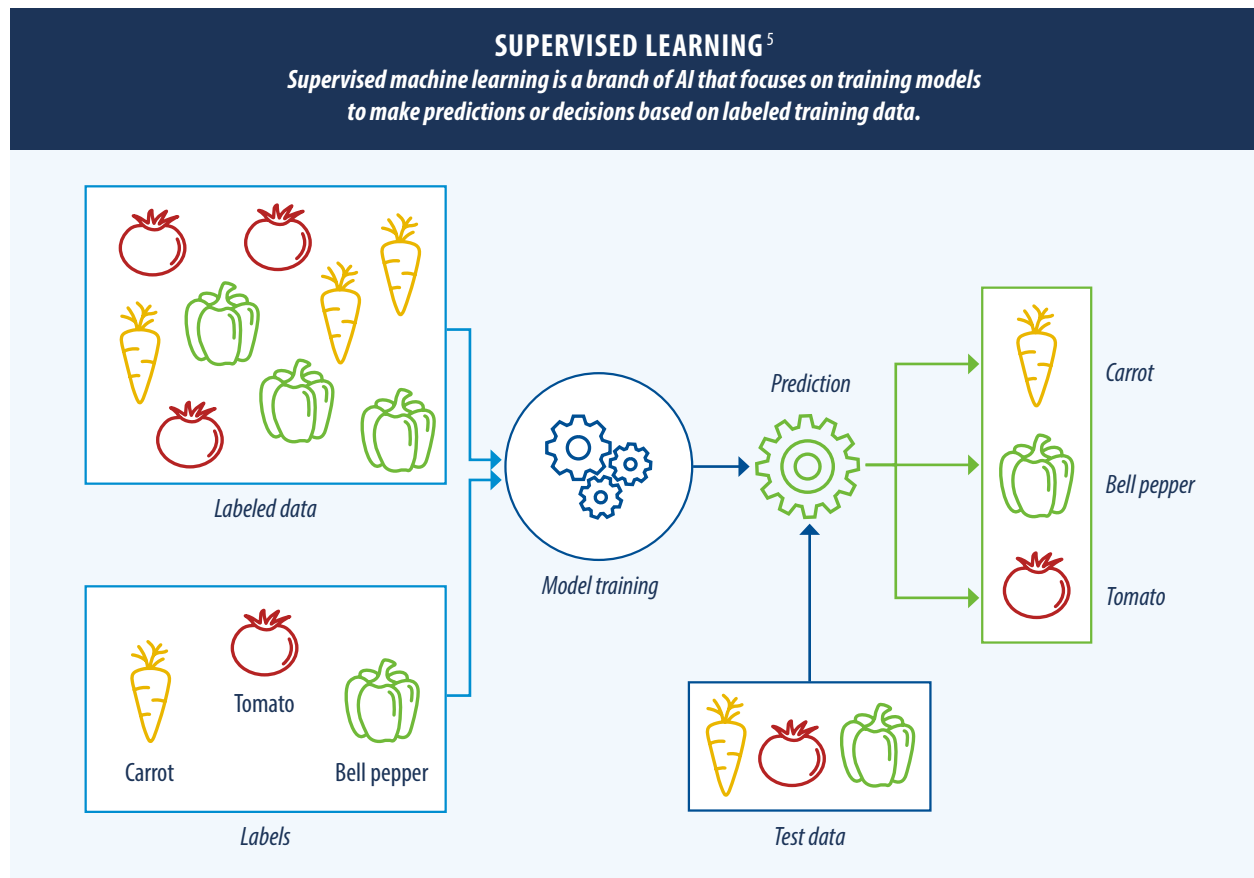
MACHINE LEARNING METHODS

Machine learning can be broken down into 3 major categories.

SUPERVISED LEARNING

Supervised learning is when a computer is provided with a set of input data (for example, images of cars) and taught how to create a desired output (such as identifying a car from a bus). The computer learns as it goes and adjusts its approach to reduce its number of errors.

In supervised learning, the learning process is supervised by the existence of desired labels (for example, labels for cars and buses) from the historical data. The computer learns by minimizing the difference between the actual and predicted outputs. The final model is used to predict future unlabelled data.
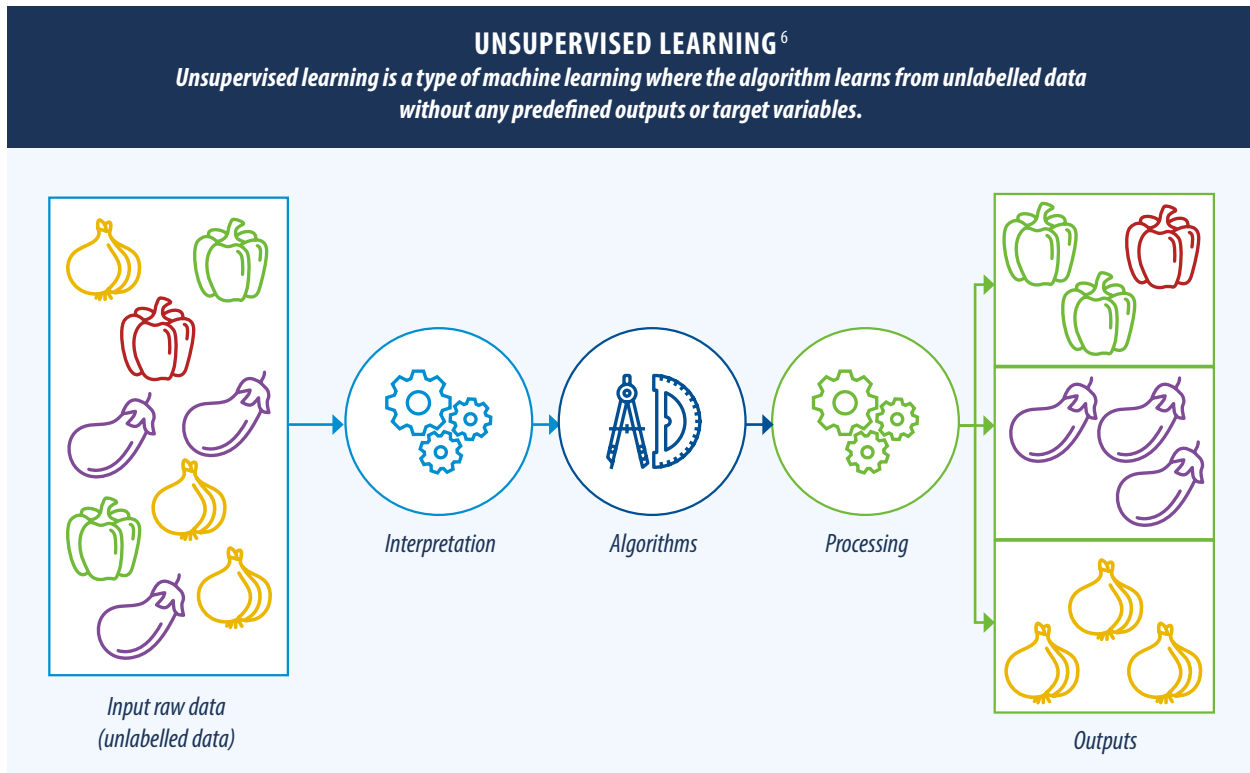
This method is used when historical data and the correct labels are available. Examples of supervised learning include programs that can identify spam emails or categorize images.

SUPERVISED LEARNING[5]
Supervised machine learning is a branch of AI that focuses on training models to make predictions or decisions based on labeled training data.

Imagine you want to create a model to identify spam emails. To train an algorithm, you give it a special collection of past emails, some of which are known to be spam, while others are legitimate emails. These emails have been marked as either spam or not by people who checked them before. The algorithm uses these examples to learn and understand the characteristics of a spam email. Once the algorithm has learned from these examples, it's then ready to make predictions. As new emails come into your inbox, the model can flag the email as spam.

UNSUPERVISED LEARNING

Unsupervised learning is when a computer is not provided with labelled data, which means the computer must look for patterns by organizing and clustering similar data together.

UNSUPERVISED LEARNING [6]
Unsupervised learning is a type of machine learning where the algorithm learns from unlabelled data without any predefined outputs or target variables.

Interpretation   *Algorithms*   *Processing*

Input raw data (unlabelled data)

Outputs

Instead of using labelled examples, unsupervised learning trains algorithms on data with no assigned labels. Imagine teaching a computer to recognize spam emails without providing any historically labelled data. Through a method called clustering, algorithms group similar transactions based on common features or behaviour patterns. Clustering sorts through a collection of emails and identifies groups of messages that exhibit common characteristics, such as sender information or language patterns. By identifying these clusters, the model can pinpoint emails that don't fit the usual patterns, which may indicate risky activity.

Overall, unsupervised learning can be a powerful tool for fraud detection, especially when used alongside supervised learning and other techniques, and can help organizations stay ahead of ever-evolving threats in the fight against fraud.

REINFORCEMENT LEARNING

Reinforcement learning is a type of machine learning where an algorithm learns through a series of trial-and-error experiences. The "learner" is called an agent and is tasked with performing actions in an environment.

Through positive or negative feedback (rewards and punishments), the agent learns to adjust its actions to maximize its future rewards. This approach has proven to be incredibly useful in a variety of fields, including gaming, cyber security, robotics, supply chain management and more.

USING MACHINE LEARNING TO DETECT SUSPICIOUS ACTIVITIES

Various industries such as banking, insurance, health care and e-commerce use machine learning to detect fraud. Machine learning helps identify anomalies, patterns and suspicious activities that indicate potential fraud, which allows for timely intervention and prevention.[7] Machine learning can identify potential money laundering, claims and credit card fraud, spam emails and cyber security attacks.

Machine learning helps identify anomalies, patterns and suspicious activities that indicate potential fraud, which allows for timely intervention and prevention.

HOW AI HELPS KEEP EVERYONE'S COSTS DOWN

At Alberta Blue Cross, we use a dynamic and adaptive multi-layered approach that combines AI and machine learning technologies, to identify abnormal and suspicious claiming patterns and connections. With a dedicated team of data scientists, we use technologies to proactively identify abnormal transactions. Our machine learning models are trained using historical data to identify patterns of abnormal and risky claiming. The models analyze large volumes of data from multiple sources to identify suspicious activity. The models then flag cases that require further investigation. This helps us allocate our resources more efficiently, resulting in improved quality and service for our customers.

MODEL → PREDICTION → EXPLANATION → HUMAN[8]

Probability of fraud

%

> " *The strategic use of AI and machine learning empowers Alberta Blue Cross to not just detect benefits fraud but stay ahead of evolving schemes, ensuring proactive intervention, heightened service quality, and cost-effectiveness for our customers.*
>
> **Vivianna Botticelli**
> Vice President & Chief Audit Executive

ABOUT THE AUTHOR

Naz Tahmasebi is currently the manager of Analytics and Reporting at Alberta Blue Cross. She holds a PhD in mathematics from the University of Alberta, which she received in 2015. Naz was ranked at the top of her class among M.Sc. graduates and has several publications in peer reviewed journals.

Naz is an accomplished mathematician with a focus on machine learning and deep learning and their applications in fraud detection, medical science, marketing and insurance. She has presented her work at various international conferences and contributed to several leading academic journals.

In her current role at Alberta Blue Cross, Naz leverages her mathematical and AI expertise to lead the Analytics team in providing critical business insights into risk and to inform strategic decision-making.

REFERENCES

[1] https://www.sas.com/en_us/insights/articles/risk-fraud/fraud-detection-machine-learning.html#/

[2] https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp

[3] https://www.futurelearn.com/info/blog/what-is-machine-learning-a-beginners-guide

[4] https://www.sas.com/en_us/insights/articles/risk-fraud/fraud-detection-machine-learning.html#/

[5] https://databasetown.com/supervised-learning-algorithms/

[6] https://databasetown.com/unsupervised-learning-types-applications/

[7] https://www.coursera.org/articles/machine-learning-in-finance

[8] https://www.sas.com/en_us/insights/articles/risk-fraud/fraud-detection-machine-learning.html

QUESTIONS?
If you have any questions about this topic, please don't hesitate to contact your Alberta Blue Cross representative.