UDC 004.056.5;343.72:[336.7+351.853]
JEL: L86; G21; G28
DOI: https://doi.org/10.32983/2222-4459-2023-7-140-145

THE USE OF MACHINE LEARNING FOR THE PURPOSE OF COMBATING BANK FRAUD

©2023 **CAPRIAN Iu.**

UDC 004.056.5;343.72:[336.7+351.853]
JEL: L86; G21; G28

Caprian Iu. The Use of Machine Learning for the Purpose of Combating Bank Fraud

Machine learning is a specific field of artificial intelligence that allows an information system to learn and improve itself autonomously using neural networks and deep learning, without the need for explicit programming, by ingesting large amounts of data. With the deepening of banking activity at the global level in cyberspace, the problems of a different kind, which are considered bank frauds, have become substantially more acute. Combating them required the examination of a gigantic volume of information, which as a task can only be achieved with artificial intelligence solutions, including the use of automatic learning technologies. Systems based on automatic learning are capable not only of analyzing the available information, but also of making certain predictions and self-learning conclusions, which allows not only the detection of existing forms of bank fraud, but to a certain extent to prevent it by detecting anomalies in customer behavior. At the moment, the global information industry has developed different forms of automatic learning, which can be adapted to the detection of fraud in different forms of banking activity. The development, implementation and further development of banking information systems based on automatic learning requires the completion of certain stages and the observance of mandatory rules.

Keywords: *machine learning, bank, customer, fraud.*
Bibl.: *13.*

Caprian Iurie *– Postgraduate Student, State University of Moldova (60 Alexei Mateevici Str., Kishinev, MD-2009, Moldova)*
E-mail: *iuriecaprian@gmail.com*
ORCID: *https://orcid.org/0000-0001-5484-3087*

УДК 004.056.5;343.72:[336.7+351.853]
JEL: L86; G21; G28

Капріан Ю. Використання машинного навчання для боротьби з банківським шахрайством

Машинне навчання – це специфічна галузь штучного інтелекту, яка дозволяє інформаційній системі самостійно навчатися та вдосконалюватися за допомогою нейронних мереж і глибинного навчання, без необхідності спеціального програмування, шляхом обробки великих обсягів даних. З активізацією банківської діяльності на глобальному рівні в кіберпросторі суттєво загострилися проблеми, що прийнято класифікувати як види банківського шахрайства. Боротьба з ними вимагає вивчення гігантського обсягу інформації, що може бути досягнуто тільки за допомогою рішень на базі штучного інтелекту, в тому числі з використанням технологій автоматичного навчання. Системи на основі автоматичного навчання здатні не тільки аналізувати наявну інформацію, а й робити певні прогнози та самонавчальні висновки, що дозволяє не тільки виявляти існуючі форми банківського шахрайства, але й певною мірою запобігати йому, виявляючи аномалії в поведінці клієнтів. На даний момент світова інформаційна індустрія розробила різні форми автоматичного навчання, які можуть бути адаптовані до виявлення шахрайства в різних формах банківської діяльності. Розробка, впровадження та подальший розвиток банківських інформаційних систем на основі автоматичного навчання вимагає проходження певних етапів та дотримання обов'язкових правил.

Ключові слова: *машинне навчання, банк, клієнт, шахрайство.*
Бібл.: *13.*

Капріан Юрій *– аспірант, Державний університет Молдови (вул. Олексія Матеєвича, 60, Кишинів, MD-2009, Молдова)*
E-mail: *iuriecaprian@gmail.com*
ORCID: *https://orcid.org/0000-0001-5484-3087*

Wikipedia defines machine learning (ML) as follows: "...is an umbrella term for solving problems for which development of algorithms by human programmers would be cost-prohibitive, and instead the problems are solved by helping machines 'discover' their 'own' algorithms, without needing to be explicitly told what to do by any human-developed algorithms" [8].

In James Bassey's definition, ML is "a technology that allows computers to learn without being explicitly programmed" [2].

The IBM experts consider ML as "is a branch of artificial intelligence (AI) and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy" [13].

A particular form of ML is considered deep learning (DP), which mimics how people acquire certain types of knowledge and is an element of data science, which includes statistics and predictive modeling [12].

The main purpose of using ML is the technological development of human knowledge.

The rationale behind the application of ML is laid out in the following vision from Techopedia: "Machine learning allows computers to deal with new situations through analysis, self-training, observation and experience. Machine learning facilitates continuous computational progress by exposure to new scenarios, testing and adapting, while using pattern and trend detection for improved decisions in subsequent (though not identical) situations." [3].

ML has become an important element of progress in the sphere of the banking industry.

In this context, James Bassey mentions: "Machine learning is machine-based artificial intelligence that can learn and improve without being explicitly programmed. Machine learning has been implemented in banking, financial services and investments for the last few decades. It has been used in credit assessment, fraud detection and risk assessment." [2].

According to the expert Swati Sharma, at once fraud has become an important problem for banking institutions and one of the main opportunities for the use of ML in banking.

According to the same author: "Machine learning systems can detect fraud by using various algorithms to sift through massive volumes of data. Banks can monitor transactions, keep an eye on client behavior, and log information to extra compliance and regulatory systems to help minimize overall risk when it comes to regulatory compliance." [9].

The main purpose of this article is to present the possibilities of ML application to combat bank fraud.

RESEARCH METHODOLOGY

The research was carried out in the form of a screening of recent bibliographic sources on trends in the both ML development and taking advantage of its use in banking worldwide. As a result, it was outlined in the summary table of the content of the given topic, which examined the essence and technological particularities of ML application in the banking industry.

THE PARTICULARS OF USING MACHINE LEARNING IN THE BANKING INDUSTRY

In banking, ML can be used to generate practical insights using the enormous databases that banks collect. The collected data is very diverse, it is about transaction history, chat logs with bank workers, and corporate documentation. The ML models can be intended to process and analyze this data to give the bank a deeper understanding of customer needs (interests) and the organization of internal processes within banking institutions. Using ML in banking can streamline fraud detection, optimize the lending process, improve compliance with banking regulations, and strengthen customer engagement [10].

Regarding the purposes of using ML in banking, James Bassey points out predicting fraud, identifying customers at risk of default, optimizing trading strategies, and lot and reputation risk management [2].

The Fayrix experts presented the seven main benefits of using ML in banking [1]:

1. *Improving decision-making.* ML can provide an objective assessment without any bias. The ability to process a huge volume of collected data helps banks make better decisions.

2. *Better risk management.* Applying ML reduces risks for both customers and banks through accurate reporting. With the help of ML, predictions can be made based on transaction history to examine customer creditworthiness. Early detection of errors and availability of potential future risks help banks prepare early.

3. *Fraud prevention.* ML for banking can significantly reduce the number of fraudulent activities in various ways.

4. *Improved customer experience.* With the help of ML banks can offer more security and a personalized experience to customers. They demand digital banking products that are easy to use. ML improves the overall experience and service by reducing the time it takes to make credit decisions and banking operations. Applying for a loan, which used to take weeks, can now be done in a few days. ML can do an unbiased analysis based on several credit factors.

5. *Obtaining internal operational solutions.* ML in the banking sector perfected internal operations. Automation reduces staff time spent on redundant tasks. Robots perform routine tasks with minimal risk of error. As a result, a bank can provide efficient solutions, while automation gives employees the chance to pay more attention to the most important tasks.

6. *Obtaining marketing solutions.* The ML systems collect data and also look for specific patterns that help banks make better marketing predictions. The data collected helps a bank decide where to invest, thereby increasing revenue. It also provides more accurate information about the possibilities of attracting new customers.

7. *Offer higher customization.* Banks can benefit from ML as it helps to adopt better management, increase customer satisfaction and provide more personalized and simplified operations and support.

The expert Pavlo Sidelov presented a wide spectrum of ML application in the banking industry [11]:

- *Fraud prevention* through ML is among the most effective applications of the technology today. Dedicated innovative algorithms analyze huge volumes of data, transaction parameters and consumer behavior patterns in real-time to detect security threats and potential cases of fraud. Unlike traditional systems based on static rules, which apply the same logic to most consumers, the ML fraud prevention is customized from customer to customer. As a result, ML enables banks to detect fraudulent transactions quickly and accurately to prevent any unnecessary losses. Likewise, ML can be the key to solving the false positive problem.
- *Anomaly detection.* The technology simultaneously tracks and processes transaction size, location, time, device, purchase data, consumer behavior and many other variables. Modern anomaly detection is successfully applied to anti-money laundering (AML) and know your client (KYC) as

well as financial fraud, as it provides clear binary responses to complex inputs. ML in anti-money laundering enables banks to pinpoint events and correlations in customer behavior that may signal fraud. By automating the complex process of detecting anomalies, banks can process much more data much faster than systems based on human rules. The machine learning KYC process relies on anomaly detection to find irregularities in the documents customers submit for verification, saving companies from taking unnecessary risks. Real-time anomaly detection allows banks to respond immediately to deviations from the norm, potentially saving funds that would otherwise have been lost to fraudulent behavior. By eliminating the delay between problem identification and resolution, banks can maximize the effectiveness of their anti-fraud strategies.

- *Document integration and processing*. The ML technology can be used for back-office tasks. First, there is document classification, which is an important process that requires considerable time and resources. ML can significantly reduce processing time for tagging, classifying, and organizing documents. By first running the documents through the Optical Character Recognition (OCR) process, machine learning algorithms can then digitize the text on the scanned documents to read, process and analyze the context. Using this information, the ML model can classify the document and index it for future search for easy access by bank employees. The ML-based document processing is just as useful for traditional banks that still rely on paper forms for customers, as it is for non-banks that require customers to send electronic documents. When ML is part of the integration and document recognition processes, customers can perform complex operations like opening a new bank account in minutes, from anywhere and on any device.
- *Assessment of creditworthiness*. Although most banking institutions collect valuable data with every transaction their customers make, most cannot use the information to its full potential. Credit scoring ML can use big data, transaction details and behavioral patterns to determine hidden customer characteristics. The ML models can generate highly personalized offers to different categories of customers. Unlike human credit scorers, the ML algorithms can rate borrowers without emotion or bias. According to the Harvard Business Review, banks can make the lending process more equitable by eliminating racial, gender, and other biases. Unbiased risk understanding enables banks to make better decisions and serve a wider audience.
- *Use within the payment system*. The ML technology enables banks to reduce transaction costs within the payment system through conversion, connectivity, invoicing and payments. ML can help optimize payment routing based on multiple parameters, such as performance, functionality, and price. By processing multiple data sources in real time, the ML algorithms can dynamically allocate traffic to the best performing combination of variables at any given time. This unlocks a new level of service customization, as banks can deliver the best results for merchants based on their individual goals.
- *Process automation*. From automating repetitive tasks by automating robotic processes such as processing documents, training employees, tracking customer inquiries, banks can completely replace time-consuming manual work and generate more value in the process. With every online action that leaves a footprint, the ML algorithms have a wealth of data to work with that they can use to interpret behaviors and recognize patterns. This is particularly useful for customer support systems, which assist in categorizing, narrowing and eventually resolving customer issues without any human intervention.
- *Application in the investment process*. The ML technology has been used to optimize the way the investment process is organized. This is algorithmic trading based on ML to closely monitor financial news, trading results, prices and hundreds of other data sources simultaneously to detect patterns that move the prices of financial instruments. Algorithms can make placements at the best possible prices using this information, eliminating human error, which sometimes leads to heavy losses. Similarly, ML has increased the accessibility of financial markets with automated robo-advisors that make investment decisions automatically based on the client's risk profile and preferences. Robo-advisors create customized portfolios to help consumers achieve their investment goals.
- *Customer retention*. ML in the payments and other banking industry helps to understand and respond to the interests of their customers with personalized services and offers. ML technology enables companies to extract nuanced insights from how their customers interact with banking products and services. Importantly, ML can help banks monitor and forecast customer churn based on behavioral changes. Given the fact that attracting new customers is much more expensive than keeping existing ones, ML helps banks identify customers they are at risk of losing and quickly take steps to keep them. For example, if a customer who had a bad experience, does not

know or has forgotten about a certain banking service and stopped using it, ML can help build loyalty and keep customers interested for longer.

- *Support services and chatbots*. Chatbots have created new useful features for customers. When connected to a payment system, the ML-based chatbots allow customers to ask and receive answers about their accounts and transactions. The sophisticated algorithms on which chatbots operate can solve many everyday queries that would otherwise be passed on to traditional customer support. Unlike most call centers, chatbots are available 24/7/365 and provide near-instant responses. If a chatbot cannot resolve a problem, the request should be forwarded to a human customer support representative. But before that, the algorithm will automatically categorize the query and present all the relevant details so that the human operator can solve the problem efficiently.

Another expert, James Bassey, mentioned two important areas of application of ML in banks [2]:

- *Risk management*. Banks can use ML to determine the probability of loan default. ML can make banking more efficient and safer. By applying ML, banks can ensure that they are not taking unnecessary risks that could lead to money losses or even bankruptcy. An ML algorithm uses a set of rules to learn from data and then make model-based predictions from the data without any human intervention.
- *Managing the reputation of banking institutions*. The ML algorithms can detect patterns in online reviews and identify negative reviews before they become too widespread, prompting banks and institutions to take action before the damage becomes too great.

Some experts point to ML's contribution to complying with banking regulations. Among the most important use cases of ML in finance are regulatory technology (RedTech) applications. The ML algorithms can scan and learn from regulatory documents and easily recognize correlations between guidelines. They can track and monitor regulatory changes as they come into effect. With the help of the ML systems, banking institutions can identify anomalies, monitor transaction data and ensure that all transactions comply with regulatory requirements [6].

THE USE OF MACHINE LEARNING FOR COMBATING BANK FRAUD

ML come to enhance the capabilities of banking institutions to prevent and combat bank fraud, complementing traditional fraud detection methods that are based on rule-based systems and may be limited in their ability to detect new and sophisticated fraud schemes. ML provides a more powerful and accurate approach to fraud detection by analyzing large amounts of data and identifying patterns that may indicate fraudulent behavior [7].

The expert Jenn Jeffers points out two advantages of applying ML to combat bank fraud [7]:

- ML has its ability to adapt to new and evolving fraud patterns. ML algorithms can learn from past fraud cases, estimate probability, and adapt to new patterns as they emerge.
- ML algorithms can reduce false positives by identifying patterns that indicate fraud, taking into account each customer's individual behavior.

ML in banking can evaluate substantial data sets of simultaneous transactions in real time. At the same time, ML can minimize human input by learning from results and updating models. With ML, banking institutions can label historical data as fraudulent or non-fraudulent and continue to improve their ability to detect potential fraud by learning from past patterns of behavior. ML can help banks quickly identify customer activity. Likewise, it is important that ML is able to check and respond quickly and effectively to cyber attacks [6].

ML enables the examination of a large amount of data in real time and the minimization of human intervention. In addition, it improves the customer experience by simplifying identity verification measures.

Examining the bibliographic sources related to the topic addressed, suggests that the main mission of the ML in combating bank frauds is detection.

According to the Binariks experts: "Fraud detection is using security measures to prevent third parties from obtaining funds or property through fraud. This process involves a manual check and/or automated verification of transaction details to spot any unusual activity that may be a sign of attack and block it. Fraud detection is the most widely used in banking and finances, insurance, healthcare, eCommerce, and other industries that collect lots of personal information and handle transactions." [5].

Fraud detection using ML is related to the following activities [6]:

- Finding hidden and implicit correlations in data;
- Automatic detection of fraud scenarios;
- Reduced number of verification steps, resulting in a better user experience;
- Real-time data processing.

It should be noted that fraudulent activities in the banking industry can take many forms with different levels of complexity. Detecting these fraudulent activities with the application of ML requires some adaptation, as the following examples illustrate [5; 7]:

- *Identity theft* is a threat that often leads to credit card fraud. It occurs when a fraudster steals the bank customer's personal data. This information is then used to open accounts or make unauthorized payments. The ML algorithms can detect identity theft by analyzing customer behavior and spotting any unusual activity, such as a spike

in transactions or changes to account information.

- *ATM skimming* occurs when a fraudster places a skimming device on an ATM, which records the bank customer's card information when they use the device. The ML algorithms can detect the ATM skimming by analyzing transaction data and spotting any unusual activity, such as a spike in the ATM transactions or transactions occurring outside of the customer's typical location.
- *Money laundering* involves presenting the proceeds of illegal activities as legitimate monetary means. The ML algorithms can detect money laundering by analyzing transactional data and spotting any unusual patterns or behaviors, such as a large number of small transactions, transactions between unrelated parties, or transactions that take place in countries with a money laundering profile.
- *Email phishing* consists of fraudsters emailing bank customers fake messages and URLs that invite them to visit a website controlled by the attackers and steal their personal information. ML performs classification and regression analysis to remove such messages.
- *Bank card fraud* occurs when fraudsters steal bank card numbers over an unsecured Internet connection to siphon off funds. ML enables the detection of unusual transactions or changes in user behavior to automatically alert banks about the threat.
- *Mobile fraud*. ML enables the detection of bank fraud by identifying unusual payment activities, regardless of the end user's device. Therefore, ML is used to secure mobile payments by protecting the personal information transmitted.

Likewise, this author presents the use of DP in the detection of bank fraud. The DP algorithms analyze large data sets to identify patterns and anomalies that may indicate fraudulent activity. Neural networks are a core component of DP because they allow machines to use self-learning algorithms for data mining, pattern recognition, and natural language processing.

There are the following groups of methods of using ML for the purpose of bank fraud detection [5]:

- *Supervised learning* is the predictive analysis of the data, and its accuracy depends on the accuracy of the training data. Therefore, its main disadvantage is that if a fraud case is not present in the historical data used for training, the model will not detect it.
- *Unsupervised learning* involves the use of algorithms, which continuously process and analyze new unlabeled data to detect patterns and build an appropriate model. This pattern can cause unusual behavior when transaction data is limited or missing. It works completely autonomously, meaning no human intervention is required.
- *Semi-supervised learning* provides that a fraud detection algorithm processes a small amount of labeled data with a large volume of unlabeled information. The semi-supervised approach can be used when information cannot be labeled for any reason or labeling is too expensive.
- *Reinforcement learning* is based on the reinforcement learning approach. The system learns the optimal behavior in a specific environment for maximum reward and interacts with the environment to determine how it responds and evaluate the feedback for further learning.

Supervised machine learning has become increasingly prevalent in building bank fraud detection systems, as they can learn from labeled data and detect patterns that indicate fraudulent activity, taking the following forms [7]:

- *Logistic regression* is a statistical technique, which is applied to analyze the relationship between a dependent variable and one or more independent variables. In fraud detection, logistic regression can be used to predict the probability that a transaction is fraudulent based on a complex of factors such as transaction value, location, and time.
- *Decision trees* use a tree-like model to represent decisions and their possible consequences. In fraud detection, decision trees can be used to identify the most important factors that contribute to fraudulent activities, such as transaction value, frequency, and location.
- *Random forest* is an ensemble learning method that combines multiple decision trees to improve accuracy and reduce the risk of overfitting. In fraud detection, random forest can be used to analyze large amounts of transactional data and detect patterns, which may not be apparent using traditional rule-based systems.
- *Support vector machines* (*SVM*) are used for classification and regression analysis. In fraud detection, SVMs can be used to detect fraudulent activity by analyzing transactional data and identifying patterns that indicate fraud.

Binariks experts presented the process of bank fraud detection using the ML algorithms [5]:

- *Information collection*. The ML technology involves collecting a large volume of data to have a basis for learning. Therefore, within the bank, a database of customer records must be formed, which should be permanently updated.
- *Abnormal patterns selection*. Then customer behaviors to be classified as good and suspicious must be determined. Anomalous information on financial transactions allows the system to learn how to assess risky customer activity. Patterns

may include customer identity, location, payment methods, number of transactions, average transaction value, and other characteristics.

- *Training an algorithm*. It is necessary to set the rules to training the algorithm on differentiating normal customer activity from fraudulent activity.
- *Creating a fraud detection model*. After training, the ML model intended for fraud detection is obtained. It is important to keep updating the system as long as it is in use to ensure its accuracy and adapt it to new security threats.

Some experts say, that at the moment there is not an universal and reliable ML algorithm for bank fraud detection. In practice, one usually tests several techniques or their combinations, calculates the predictive accuracy of the model, and selects the optimal approach. The main characteristic of efficient fraud detection systems is the rapid adaptation to the dynamic evolution of fraud and the methods used by criminals, as well as the rapid discovery of new fraudulent schemes [4].

CONCLUSIONS

The machine learning technologies have become an important element in the work of modern banks. Along with its application for other purposes, ML has become an important tool in preventing and combating bank fraud, which has become an important threat to the financial condition and reputation of banking institutions as well as customer confidence. Fraudulent activities can lead to significant financial losses, not only for banks but also for their customers. Fraud detection helps banks identify and prevent unauthorized activity in various forms. Likewise, fraud detection contributes to improving the operational efficiency of banking institutions. By identifying and mitigating fraudulent activity, banks can reduce false positives and improve fraud detection accuracy. In implementing fraud detection techniques using ML, it is important for banks to stay ahead of fraudulent activities. ■

BIBLIOGRAPHY

1. 4 Best Practices of Machine Learning Application in the Banking Sector. URL: https://fayrix-software.medium.com/4-best-practices-of-machine-learning-application-in-the-banking-sector-20c7aed6dad4
2. Bassey J. Ghidul complet pentru învățarea automată în domeniul bancar, al serviciilor financiare și al investițiilor. URL: https://stayinformedgroup.com/ro/machine-learning-in-banking/
3. Ce este învățarea automată? – definiție din techopedia. URL: https://ro.theastrologypage.com/machine-learning
4. Data Science in Banking: Fraud Detection. URL: https://www.datacamp.com/blog/data-science-in-banking
5. Financial Fraud Detection Using ML and Measures to Prevent It. URL: https://binariks.com/blog/financial-fraud-detection-machine-learning/
6. How Machine Learning is Used in Finance and Banking. URL: https://exadel.com/news/how-machine-learning-is-used-in-finance-and-banking/
7. Jeffers J. Fraud Detection in Banking Using Machine Learning. URL: https://securityboulevard.com/2023/04/fraud-detection-in-banking-using-machine-learning/
8. Machine learning. URL: https://en.wikipedia.org/wiki/Machine_learning
9. Sharma S. Applications of Machine Learning and AI in Banking and Finance in 2023. URL: https://www.analyticsvidhya.com/blog/2023/03/machine-learning-and-ai-in-banking-and-finance/#:~:text=Machine%20learning%20systems%20can%20detect,it%20comes%20to%20regulatory%20compliance
10. Shmat D. Machine learning in banking: 8 use cases and implementation guidelines. URL: https://www.itransition.com/machine-learning/banking
11. Sidelov P. Machine Learning in Banking: Top Use Cases. URL: https://sdk.finance/top-machine-learning-use-cases-in-banking/
12. What is deep learning? URL: https://www.techtarget.com/searchenterpriseai/definition/deep-learning-deep-neural-network#:~:text=Deep%20learning%20is%20a%20type,includes%20statistics%20and%20predictive%20modeling
13. What is machine learning? URL: https://www.ibm.com/topics/machine-learning

REFERENCES

"4 Best Practices of Machine Learning Application in the Banking Sector". https://fayrix-software.medium.com/4-best-practices-of-machine-learning-application-in-the-banking-sector-20c7aed6dad4

Bassey, J. "Ghidul complet pentru invatarea automata in domeniul bancar, al serviciilor financiare si al investitiilor". https://stayinformedgroup.com/ro/machine-learning-in-banking/

"Ce este invatarea automata? – definitie din techopedia". https://ro.theastrologypage.com/machine-learning

"Data Science in Banking: Fraud Detection". https://www.datacamp.com/blog/data-science-in-banking

"Financial Fraud Detection Using ML and Measures to Prevent It". https://binariks.com/blog/financial-fraud-detection-machine-learning/

"How Machine Learning is Used in Finance and Banking". https://exadel.com/news/how-machine-learning-is-used-in-finance-and-banking/

Jeffers, J. "Fraud Detection in Banking Using Machine Learning". https://securityboulevard.com/2023/04/fraud-detection-in-banking-using-machine-learning/

"Machine learning". https://en.wikipedia.org/wiki/Machine_learning

Sharma, S. "Applications of Machine Learning and AI in Banking and Finance in 2023". https://www.analyticsvidhya.com/blog/2023/03/machine-learning-and-ai-in-banking-and-finance/#:~:text=Machine%20learning%20systems%20can%20detect,it%20comes%20to%20regulatory%20compliance

Shmat, D. "Machine learning in banking: 8 use cases and implementation guidelines". https://www.itransition.com/machine-learning/banking

Sidelov, P. "Machine Learning in Banking: Top Use Cases". https://sdk.finance/top-machine-learning-use-cases-in-banking/

"What is deep learning?" https://www.techtarget.com/searchenterpriseai/definition/deep-learning-deep-neural-network#:~:text=Deep%20learning%20is%20a%20type,includes%20statistics%20and%20predictive%20modeling.

"What is machine learning?" https://www.ibm.com/topics/machine-learning