PROSPECTS FOR FURTHER IMPROVEMENT OF MACHINE LEARNING SYSTEMS

Vladimir MKRTCHYAN
Ph.D. in Economics
Artur OGHLUKYAN
MA, SE at Polytechnic Institute of Bragança, Portugal (IPB)
& National Polytechnic University of Armenia (NPUA)

Key words: machine learning, machine learning systems algorithms, data, collectives.

Introduction. The rapid development and widespread use of machine learning methods in the last decade is caused by:

a) The growth of computing power.
b) The amount of accumulated information.
c) Development of the mathematical base used in these algorithms.

Machine learning enables computers or robots to make data-driven decisions. These programs or algorithms are designed to learn and improve over time as new data is introduced. Machine learning models are classified into the following categories:

1. Supervised learning
2. Unsupervised Learning
3. Reinforcement Learning Use Cases

i. Product recommendation on a shopping site.
ii. Spam email filter.
iii. Chat-bots.

Machine learning is the most important branch of artificial intelligence. Without the assistance of training, it is highly unlikely that a human would be able to create any kind of intelligent system capable of any of the abilities we associate with intelligence, such as language or vision. These responsibilities would be impossible to carry out otherwise. Furthermore, because learning is the foundation of intelligence, we would not consider a system truly intelligent if it was incapable of learning. Automated procedures are heavily emphasized in machine learning. In other words, the goal is to develop learning algorithms that can learn on their own without the assistance of humans. Machine learning is often referred to as "programming by example." We frequently have a specific goal in mind, such as checking for spam. Rather than directly programming a computer to solve a problem, machine learning looks for methods to allow the computer to generate its own program based on provided examples.

Economic significance. Machine learning is practically everywhere today, from a pilot car on the road to Siri talking to us and Coursera offering us courses, all thanks to machine learning. It is possible to reach ideas that were proposed two or three years ago, and which change the reality that surrounds us today, using machine learning. It is possible to apply machine learning knowledge in virtually any field, including economics, where we can, for example, predict the client's solvency or spending for the next month. And this is critical knowledge; machine learning will largely determine the development of humanity for at least a few years, and it is critical for us to know, understand, and be able to work with these tools without fear.

Methodology. The primary goal of machine learning research is to develop universal algorithms that are applicable in real situations. This type of algorithm must be efficient. We are interested in the efficient use of time and space as computer scientists. However, in the context of learning, we are also concerned with another valuable resource: the amount of data that the learning algorithm necessitates. Learning algorithms should be as versatile as possible. We are looking for algorithms that can be used to solve a wide range of learning problems, including those mentioned above. There are numerous machine learning applications to consider. The majority of this article is about classification problems, in which the goal is to categorize things into a predefined set of categories. Below are a few examples:

- Optical Character Recognition: Sorts photos of handwritten characters into categories based on the letters they represent.
- Face detection is the process of identifying people in photographs (or indicating if a face is present)
- Filtering: Determine if an email message is spam.
- Topic Definition: Classifies news into categories: politics, sports, entertainment.
- Determine the meaning of what the speaker is saying in the context of a limited area, to the extent that it can be placed in one of a fixed set of categories.
- The term "medical diagnosis" refers to the process of determining the cause of a patient's illness.
- Predict which customers will respond to a particular promotion, for example, using customer segmentation.
- Fraud detection (i.e., identifying potentially fraudulent credit card transactions).
- Forecasting the weather, whether it will rain tomorrow.

There will be a lot of discussion about classification problems in the long run, but there will also be other important learning issues. In a classification, we want to group items into fixed categories. Regression, on the other hand, attempts to predict a real number. For instance, we might want to forecast how much rain will fall tomorrow. Alternatively, we can make an educated guess as to how much the house will sell for.

Literature review. In [5], one can find data on the applicability of various methods for detecting attacks, which based on various machine learning methods (Bayes classifier, k nearest neighbors, neural networks, random forest, support vector machine, decision trees and ensemble methods) made it possible to achieve a classification accuracy of more than 95%. The work [6] notes the applicability of fuzzy systems for traffic analysis, which allows not only classifying, but also trying to interpret the factors that led to the result, trying to explain it. We may conclude that machine learning and deep learning methods have a high potential for solving cybersecurity problems. Learning methods such as decision trees, SVMs, and KNNs are the most common and are being studied to increase their effectiveness in solving cybersecurity problems. Also, one of the main opportunities for machine learning in 2022 is secure multilateral computing (BMC) - one of the most important areas for the development of modern cryptography. Recall the statement of the BMW problem [1]. Consider a multilateral cryptographic protocol in which each participant has their own individual secret. It is necessary to calculate the given function, the arguments of which are these secrets, so that the result of the calculations is known to all members of the group, but the secrets themselves are not disclosed by the protocol participants to each other or to any third party. A special case of BMW can be considered the problem of confidential machine learning (CML). The purpose of the KMO is to ensure the confidentiality of the data of each of the participants in the machine learning system in conditions when the persons providing the training sample at the stage of training the model (training) or queries to the model at the stage of its operation (inference) and waiting for answers to their requests (clients) remotely interact with provider capable of performing calculations with the model (server)[2].

Scientific novelty. Initially, the field of machine learning appeared to be a work of science fiction. However, machine learning is now being used in real-world industries. In 2022, the most recent advancements in this field have enabled many problems to be solved more efficiently and accurately than ever before. The combination of machine learning methods and algorithms allows for the detection of hidden dependencies, predictive analysis of information, real-time responses, and the implementation of artificial intelligence algorithms. In fact, the methods of collaboration with machine learning technologies (such as the use of neural networks) are based on graph embedding. This technology enables us to conduct a thorough, in-depth, and intelligent analysis of data.

Analysis. Based on literature review, at present, theoretical and applied research in the field of development and implementation of CMO systems is carried out by at least 10 research teams dispersed around the world. Due to the high rate of scientific research in the field of CMO systems, only systems created in the last three years (2019-2021) were considered. The following is a brief summary of the work of each group.

1. Team of the international research division of Microsoft Corporation. The efforts of the team are focused on creating two-level architecture KMO systems, in which client components allow interpreting descriptions of machine learning models performed using the TensorFlow library tools into an internal representation, and server

components automatically execute BMW protocols that implement calculations using modules with a set of universal two-way and tripartite secure computing protocols [3].

The main work of the team:

- SecureNN system (2019) [8];
- EzPC system (2019) [4];
- CrypTFlow system (2020) [2];
- CrypTFlow2 system (inference, 2020) [6].

2. Research group of the Darmstadt University of Technology (Germany). The main area of work of the team in the field of CMO systems is the implementation of universal means for executing bilateral protocols for secure computing based on a combination of representation of calculated functions in the form of arithmetic, Boolean and distorted circuits (garbled circuits), which can be used as a ready-made kernel when creating individual applications, including federated training, processing of medical images using machine learning methods, etc.

The main work of the team:

- module ABY (2015) [7];
- MP2ML system (2020) [8];
- ABY 2.0 module (2020);
- FLGuard system (2021).

3. Research group of the University of California at Berkeley (UC Berkeley, US). The team is working on the creation of CMO systems for obtaining responses to requests containing confidential information to already trained models based on two-way secure computing protocols with enhanced properties, including the most "strong" intruder model - the malicious client model. The main work of the team:

- Delphi system (2018);
- experimental systems and prototypes of Visor, Bost, Cerebro (2019-2021);
- Muse system (2021).

4. Research group of the Indian Institute of Sciences in Bangalore. The activity of the scientific group is focused on the creation of CMO systems mainly for deep neural networks based on 4-way secure computing with the possibility of implementing some systems on three-way protocols. The main work of the team:

- Trident (2020).
- FLASH (2020);
- Blaze (2020);
- SWIFT (2021);
- Tetrad (2021).

Together with the University of Darmstadt, members of the research team participated in the development of the ABY 2.0 module [9].

5. A team of Facebook and Visa Research researchers. The team members' activities are focused on developing a universal module for trilateral secure computing protocols based on a combination of arithmetic, Boolean, and distorted schemes, as well as applying it to CMO systems. Currently, the emphasis is on secure clustering protocols and systems. The main work of the team:

- SecureML (2017).
- ABY3 (Anthmetic-Bmary-Yao) framework (2018);
- K-means clustering (2020).

5. A research group at Princeton University (USA) is developing CMO systems based on tripartite secure computing protocols with increasingly stringent adversary models. The main work of the team:

- SecureNN (2019, with Microsoft);
- FALCON (2021);
- Ponytail (2012-2021);

6. International research group of the National Institute of Industrial Science and Technology of Japan, NTT Corporation and the University of St. Gallen (Switzerland). There is information about one development of this team - the Adam CMO system for deep neural networks, which supports extended functionality in comparison with the known ones when training and applying neural networks [4]. The system is based on tripartite secure computing protocols.

7. Research Group of the Massachusetts Institute of Technology (USA). There is information about one development of this group - the Gazelle system (2018) based on bilateral protocols. Currently, some of the ideas of this development are used in newer KMO systems, and the Gazelle system itself is of historical interest.

8. Aalto University Research Group (Finland). There is information about one development of this group - the MiniONN system (2017) [26], which is only of historical interest, since it is inferior to newer KMO systems in all main indicators.

9. Research group of the University of Paris (France). There is information about one development of this group - the AriaNN system, which is also of only historical interest, since it is inferior to newer KMO systems in all major indicators.

Conclusions. An analysis of the work of research teams allows us to identify several criteria that are essential for evaluating the developed and implemented CMO systems based on BMW protocols. Below we describe them in more detail:

1. Number of parties in BMW protocols implementing functionality of CMO:

1.1. Bilateral:

1.2. Tripartite:

1.3. Quadripartite.

Some CMO systems allow functionality to be implemented through protocols with varying numbers of participants. At the same time, systems with more than four participants in the calculations were not found in the course of this study.

2. Cryptographic primitives used to implement the system.
3. The model of the intruder, under the assumption of which the CMO system was developed and in which its cryptographic strength is ensured.
4. Support for machine learning lifecycle stages.
5. Suitability for use in various communication architectures.
6. Neural network architectures for which KMO systems have been tested:

During the course of the work, an exploratory study was conducted, as well as a review of existing CMO systems, which were mostly implemented in the form of prototypes and laboratory samples.

References.

1. Bryuxina N.G., Reva P.V., Barannikov V.A. Intelektualnaya avtomatizaciya kak drayver ekonomiki v usloviyax pandemii // Resursosberejenie. Effektivnost. Razvitie. 2020. 443-450pp.
2. Idei mashinnogo obucheniya. Ot teorii k algoritmam / M.: DMK Press, 2019, - 438p.
3. Mashinnoe obuchenie // pod. red. Brink X., Feverolf M., Richards D. - P.: Piter, 2017 – 336p.
4. Mashinnoe obuchenie bez lishnix slov // pod. red. Burkov A. – P.: Piter, 2020 – 192p.
5. Otkritiy kurs mashinnogo obucheniya. 7. Obuchenie bez uchitelya: RSA i klasterizaciya 2017.
6. Kostas K. Anomaly Detection in Networks Using Machine Learning / 2018. 23p.
7. Morocho-Cayamcela, M. Machine learning for 5G/B5G mobile and wireless communications: potential, limitations, and future directions / IEEE Access. - 2019. - V.7. - 137184-137206 pp.
8. Mahfouz A.M. Comparative Analysis of ML Classifiers for Network Intrusion Detection / A.M. Mahfouz, D. Venugopal, S.G. Shiva / 2020. - 193-207pp.
9. Zapechnikov S., Scherbakov A. Konfidencialnoe mashinnoe obuchenie na osnove dvustoronnix protokolov besopasnix vicheslenij. Besopasnost inform. texnologiy, [S.I.], t. 28, № 4, 2021,

Vladimir MKRTCHYAN, Artur OGHLUKYAN

Prospects for further improvement of machine learning systems

Key words: Machine learning, machine learning systems, algorithms, data, collectives.

Machine learning is a catalyst for productivity growth. Its methods are the main tools of artificial intelligence, the use of which allows to automate the processing and analysis of big data, identify hidden or non-obvious patterns on this basis, and extract new knowledge. Those methods have many practical implementations in such tasks as processing graphic and speech information, organizing the safe movement of unmanned vehicles, predicting the development of a disease, forming financial strategies, medicine abuse detection, useful and fascinating advertisement prediction, etc. This article is devoted to the analysis of the possibilities of machine learning, after general information about the formulation of problems of secure multilateral computing and confidential machine learning, an overview of the existing systems of confidential machine learning and the prospect for their development is given. An analysis of the work of leading foreign research teams worldwide allows us to identify several criteria that are essential for evaluating confidential machine learning systems based on multilateral secure computing protocols.