Project 1: White Paper

Jason Kremhelmer

Southern New Hampshire University

CS370: Current/Emerging Trends in CS

Roland Morales

9/29/2024

# Neural Networks

Neural networks are a type of Machine Learning. They are an algorithm that attempt to simulate the human brain. They can be used for a variety of applications to include natural language processing, image recognition, as well as voice recognition. “An intelligent system (1) operates in an environment with other agents, (2) possesses cognitive abilities such as perception, action control, deliberative reasoning or language use, (3) follows behavioral principles based on rationality and social norms and (4) has the capacity to adapt through

learning.” (Sheldon, 2022)

Neurons, layers of interconnected nodes, are what makes up a neural network. The artificial neurons were inspired by biological processes according to Gulli and Paul (Antonio Guli, 2017) Both BNN (Biological Neural Network) and ANN (Artificial Neural Network) see inputs or signals. “**Signals**: an action potential is either triggered or not — biological synapses either carry a signal or they don’t. Perceptrons work somewhat similarly, by accepting binary inputs, applying weights to them and generating binary outputs depending on whether the sum of these weighted inputs have reached a certain threshold (also called a step function).” (Nagyfi, 2018)

There are multiple layers to the neural network. The first layer, known as the input layer, is responsible for receiving the data that the network will be trained on. From here the data is passed through hidden layers, where data is then processed and transformed. The output layer produces the networks classifications and predictions based on the data that was input.

In a neural network each neuron receives inputs from multiple other neurons, then applies a mathematical function to the sum of those inputs to produce the output. The weights, or strength of the connection between neurons, is adjusted while the training is taking place to optimize the network’s performance. For example, in image recognition the input layer may receive a pixelated image. At this point the hidden layers process the data, identify patterns, then the output layer would then produce a prediction of what the image is.

Neural networks learn to classify objects by iteratively adjusting connections between the neurons, this is in response to the feedback regarding how their predictions matched the correct answer.

Neural networks are used in multiple ways in the personalization of a user’s experience. Below are some examples:

* Recommender systems: A user’s past behaviors can be used by neural networks to generate personalized recommendations. “YouTube’s recommendations are powered by deep neural networks, which have been trained on human preferences to predict what videos people will like. These Deep Neural Networks work much like the brain in that they can process enormous amounts of data with a single connection and then make predictions based on these connections. The more we watch YouTube, the better it knows us and our tastes!” (Kiran, 2021)
* NLP (Natural Language Processing): The use of text and voice commands can be used by neural networks to understand and analyze a user’s natural language.
* Image and Video recognition: Photos and videos can be analyzed and used by the neural network to identify patterns and personalize recommendations.

Neural networks often are used to analyze large amounts of data to generate personalized recommendations. This personalization however can raise some ethical questions. Below are a couple examples:

* Data Privacy: A neural network relies on large amounts of personal data to train and personalize the recommendations. There are some ethical concerns around the use of this data. Personal information may be collected, analyzed, and used without the consent of the user. This leads to concerns over data privacy and the potential misuse of personal information. One example is Uber’s routing info exposes information without user’s consent. (News, 2017)
* Transparency: With the difficulty in interpreting the neural network, they are sometimes considered “black boxes”. The lack of transparency can lead to ethical concerns about hidden biases in the system. A user may not be aware that recommendation and decision-making is taking place. Without knowing this, it is difficult to assess and address any potential biases.

It is crucial that the ethical issues in the system design be addressed. Systems need to be designed that respect user’s privacy, are explainable, ensure that users have sufficient control, and monitored for potential bias. Responsible Research and Innovation is a step in the right direction to achieving this goal. RRI “...is a term used by the European Union's Framework Programmes to describe scientific research and technological development processes that take into account effects and potential impacts on the environment and society".

“Right to be forgotten” which is very similar to the ideas of General Data Protection Regulation (GDPR) which seeks to codify this "right". This movement calls for companies to allow people to control their data, especially PII. This allows people to choose whether a company can keep their data or delete it from their files.

[The General Data Protection Regulation (GDPR) is a European Union regulation that sets guidelines for information privacy in the EU and the European Economic Area (EEA)](https://www.bing.com/ck/a?!&&p=033b5f3eaf162a83JmltdHM9MTcyNzU2ODAwMCZpZ3VpZD0wZDc3ZTMxYi1jZjUyLTY3YWUtMWNiZS1mN2E4Y2UzZTY2NjkmaW5zaWQ9NTk0MA&ptn=3&ver=2&hsh=3&fclid=0d77e31b-cf52-67ae-1cbe-f7a8ce3e6669&psq=GDPR&u=a1aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvR2VuZXJhbF9EYXRhX1Byb3RlY3Rpb25fUmVndWxhdGlvbg&ntb=1). [It is the toughest security and privacy law in the world, governing the collection and processing of personal information from individuals both within and outside the EU](https://www.bing.com/ck/a?!&&p=0758de708e188d8cJmltdHM9MTcyNzU2ODAwMCZpZ3VpZD0wZDc3ZTMxYi1jZjUyLTY3YWUtMWNiZS1mN2E4Y2UzZTY2NjkmaW5zaWQ9NTk0Ng&ptn=3&ver=2&hsh=3&fclid=0d77e31b-cf52-67ae-1cbe-f7a8ce3e6669&psq=GDPR&u=a1aHR0cHM6Ly93d3cuaW52ZXN0b3BlZGlhLmNvbS90ZXJtcy9nL2dlbmVyYWwtZGF0YS1wcm90ZWN0aW9uLXJlZ3VsYXRpb24tZ2Rwci5hc3A&ntb=1).

* Transparency: GDPR requires that organizations provide individuals with clear and concise information about the personal data that is being collected, processed, and stored. This includes information about how the data will be used for personalization purposes.
* Transparency: GDPR requires that organizations provide individuals with clear and concise information about the personal data that is being collected, processed, and stored. This includes information about how the data will be used for personalization purposes.
* Data minimization: GDPR requires personal data to be adequate, relevant, and limited to what is necessary for the purposes for which it is processed. Organizations must ensure that they are not collecting more data than is necessary for personalization, and that the data they collect is accurate and up to date.
* Storage limitation: GDPR requires that personal data be kept in a form that permits identification of individuals no longer than is necessary for the purposes for which the data is processed. Organizations must ensure that they are not storing personal data for longer than is necessary for personalization purposes.
* Confidentiality: GDPR requires that personal data be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage. Organizations must ensure that personal data used for personalization purposes is kept confidential and secure.
* Accountability: GDPR requires that organizations be able to demonstrate compliance with the GDPR's principles and obligations. This includes maintaining records of personal data processing activities, conducting data protection impact assessments, and implementing appropriate technical and organizational measures to ensure the security of personal data used for personalization purposes.

GDPR brings several legal concerns to the company. The concerns may include the following:

* Data protection and privacy: The use of personal data to train the neural network and personalize the user experience may raise concerns around data protection and privacy. We must comply with relevant data protection laws, such as the GDPR, to ensure that the collection, processing, and storage of personal data is lawful and transparent.

For compliance purposes our internal auditing team should become aware of, trained for, and measuring our GDPR compliance for any of our business teams operating in the European Bloc.

* Discrimination and bias: Neural networks can be prone to perpetuating biases and discrimination. We need to make sure our company has a diverse team, helping to train, test, and validate our models before being released to the public.
* Intellectual property: The use of neural networks may raise questions around intellectual property, particularly if the neural network is trained on copyrighted or proprietary data. Legal should be involved in the vetting of any new data set.
* Liability: Companies may be held liable for any harm caused using the neural network. This liability is another reason to have our company’s auditing team begin to monitor our usage and creation of ANN technologies.

The GDPRs principles of transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, and accountability. Our Auditing team will make sure these principles are followed. The team must obtain consent from the users to use their personal information. If we fail to comply with the GDPR the company could face fines and be legally liable.

The auditing team needs to be evaluating the engineering team’s adherence to industry’s best practices.

* Differential privacy: Differential privacy is a machine learning (ML) model technique that adds noise to data to prevent the identification of individual users, enhancing privacy, while still allowing for accurate statistical analysis.
* Federated learning: Federated learning is a decentralized approach to ML that allows data to be trained locally on user devices, rather than being centralized in one location – helpful in mitigating the damage of data breaches.
* Homomorphic encryption: Homomorphic encryption is a technique that allows computations to be performed on encrypted data without decrypting it. This technique can be used in ML models to protect user privacy while still allowing for accurate analysis of the data.
* Privacy-preserving data sharing: Privacy-preserving data sharing techniques allow multiple parties to share data while still maintaining the privacy of individual users.

The trend in AL and ML is towards a greater focus on ethics and privacy. Increasingly companies are recognizing the importance of protecting user privacy and ensuring their models are transparent and fair.

# References

Antonio Guli, S. P. (2017). *Deep Learning with Keras.* Birmingham - Mumbai: Packt Publishing Ltd.

Kiran, J. (2021, August 25). *YouTube Recommendations: How YouTube uses Deep Neural Networks to recommend videos*. Retrieved from ReelnReel: https://reelnreel.com/how-youtube-uses-deep-neural-networks/

Nagyfi, R. (2018, September 4). *The differences between Artificial and Biological Neural Networks*. Retrieved from Medium: https://towardsdatascience.com/the-differences-between-artificial-and-biological-neural-networks-a8b46db828b7

News, B. (2017, February 12). *Cheating Frenchman sues Uber for tipping off wife about affair*. Retrieved from BBC News: https://www.bbc.com/news/world-europe-38948281

Sheldon, R. (2022, June). *Intelligent System*. Retrieved from WhatIs: https://www.techtarget.com/whatis/definition/intelligent-system