UDC 004.032.26:004.056

THE USE OF NEURAL NETWORKS IN INFORMATION SECURITY

Sedun M.S., Nardinov R.R.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Lazarenko A.M. – senior lecturer of the department of foreign languages

Annotation. This text provides an overview of the applications and benefits of neural networks and deep learning techniques for information security. It explains how different types of neural networks, such as deep belief networks, generative adversarial networks, recurrent neural networks, convolutional neural networks, and self-organizing maps can be used to enhance the detection and prevention of cyberattacks, malware, phishing, fraud, and other threats. It also discusses the challenges and limitations of neural networks, such as high computational complexity, lack of interpretability, vulnerability to adversarial attacks, and ethical and legal issues.

Keyword: neural networks, datasets, information security

Introduction. Neural networks are a type of artificial intelligence that can learn from data and perform tasks, such as classification, regression, clustering, anomaly detection, etc. Neural networks can be used in information security to enhance the detection and prevention of cyberattacks, malware, phishing, fraud, and other threats.

Main part. Some examples of neural network applications in information security are considered below:

Deep Belief Networks (DBNs) are sophisticated artificial neural networks used in the field of deep learning, a subset of machine learning. They are designed to discover and learn patterns within large sets of data automatically. Imagine them as multi-layered networks, where each layer is capable of making sense of the information received from the previous one, gradually building up complex understanding of the overall data [1].

DBNs work in two main phases: pre-training and fine-tuning. In the pre-training phase, the network learns to represent the input data layer by layer. Each layer is trained independently as an RBM, which allows the network to learn complex data representations efficiently. During this phase, the network learns the probability distribution of the inputs, which helps understand the underlying structure of the data.

In the fine-tuning phase, the DBN adjusts its parameters for a specific task, like classification or regression. This is typically done using a technique known as backpropagation, where the network's performance on a task is evaluated, and the errors are used to update the network's parameters. This phase often involves supervised learning, where the network is trained with labelled data [2] (Figure 1):

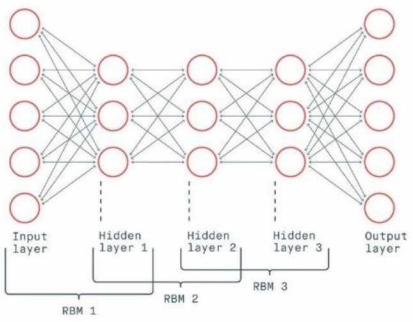


Figure 1 – An Overview of Deep Belief Network (DBN)

Generative adversarial networks (GANs) can be used to generate realistic and diverse synthetic data for training and testing security models, as well as. A generative adversarial network (GAN) is a class of machine learning frameworks and a prominent framework for approaching

generative AI. The concept was initially developed by Ian Goodfellow and his colleagues in June 2014. In a GAN, two neural networks contest with each other in the form of a zero-sum game, where one agent's gain is another agent's loss. Given a training set, this technique learns to generate new data with the same statistics as the training set. For example, a GAN trained on photographs can generate new photographs that look at least superficially authentic to human observers, having many realistic characteristics. Though originally proposed as a form of generative model for unsupervised learning, GANs have also proved useful for semi- supervised learning, fully supervised learning, and reinforcement learning.The core idea of a GAN is based on the "indirect" training through the discriminator, another neural network that can show how "realistic" the input seems, which itself is also being updated dynamically. This means that the generator is not trained to minimize the distance to a specific image, but rather to fool the discriminator. This enables the model to learn in an unsupervised manner [3] (Figure 2):

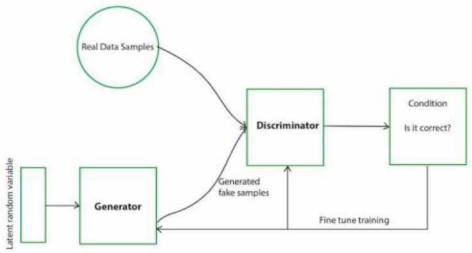


Figure 2 - Generative Adversarial Network (GAN)

RA recurrent neural network (RNN) is a type of artificial neural network which uses sequential data or time series data. These deep learning algorithms are commonly used for ordinal or temporal problems, such as language translation, natural language processing (nlp), speech recognition, and image captioning; they are incorporated into popular applications such as Siri, voice search, and Google Translate.

Like feedforward and convolutional neural networks (CNNs), recurrent neural networks utilize training data to learn. They are distinguished by their “memory” as they take information from prior inputs to influence the current input and output. While traditional deep neural networks assume that inputs and outputs are independent of each other, the output of recurrent neural networks depend on the prior elements within the sequence. While future events would also be helpful in determining the output of a given sequence, unidirectional recurrent neural networks cannot account for these events in their predictions (Figure 3):

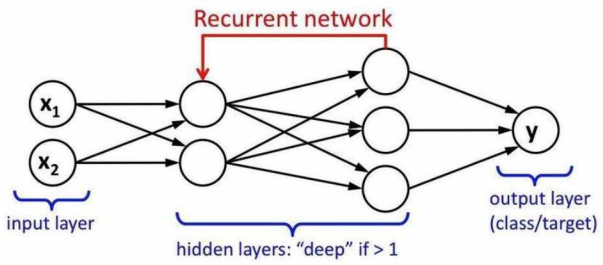
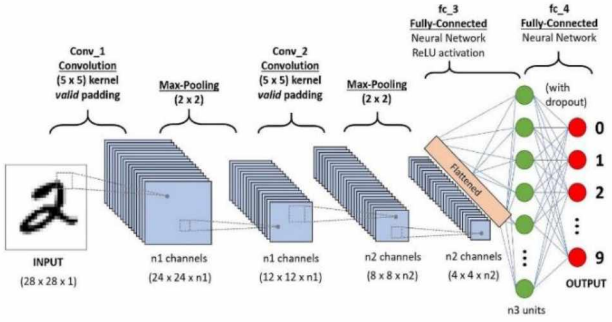


Figure 3 – Recurrent neural network(RNN) or Long Short Term Memory(LSTM)

Neural networks are a subset of machine learning, and they are at the heart of deep learning algorithms. They are comprised of node layers, containing an input layer, one or more hidden layers, and an output layer. Each node is connected to another and has an associated weight and threshold. If the output of any individual node is above the specified threshold value, that node is activated, sending data to the next layer of the network. Otherwise, no data is passed along to the next layer of the network. While we primarily focused on feedforward networks in that article,

there are various types of neural nets, which are used for different use cases and data types. For example, recurrent neural networks are commonly used for natural language processing and speech recognition whereas convolutional neural networks (ConvNets or CNNs) are more often utilized for classification and computer vision tasks. Prior to CNNs, manual, time-consuming feature extraction methods were used to identify objects in images. However, convolutional neural networks now provide a more scalable approach to image classification and object recognition tasks, leveraging principles from linear algebra, specifically matrix multiplication, to identify patterns within an image. However, they can be computationally demanding, requiring graphical processing units (GPUs) to train models [1] (Figure 4):



Figuree 4 - Convolutional Neural Networks (CNNs)

A self-organizing map (SOM) or self-organizing feature map (SOFM) is an unsupervised machine learning technique used to produce a low-dimensional (typically two-dimensional) representation of a higher-dimensional data set while preserving the topological structure of the data. For example, a data set with (p) variables measured in (n) observations could be represented as clusters of observations with similar values for the variables. These clusters then could be visualized as a two-dimensional "map" such as observations in proximal clusters have more similar values than observations in distal clusters. This can make high-dimensional data easier to visualize and analyze.

An SOM is a type of artificial neural network but is trained using competitive learning rather than the error-correction learning (e.g., backpropagation with gradient descent) used by other artificial neural networks. The SOM was introduced by the Finnish professor Teuvo Kohonen in the 1980s and therefore is sometimes called a Kohonen map or Kohonen network. The Kohonen map or network is a computationally convenient abstraction building on biological models of neural systems from the 1970s and morphogenesis models dating back to Alan Turing in the 1950s. SOMs create internal representations reminiscent of the cortical homunculus, a distorted representation of the human body, based on a neurological "map" of the areas and proportions of the human brain dedicated to processing sensory functions, for different parts of the body [3].

Conclusion. Neural networks can provide many benefits for information security, such as high accuracy, scalability, adaptability, and robustness. However, they also pose some challenges, such as high computational complexity, lack of interpretability, vulnerability to adversarial attacks, and ethical and legal issues [2]. Therefore, neural networks should be used with caution and proper evaluation in information security applications.

References

1. *Marukhlenko A.L., Plugatarev A.V., Bobyntsev D.O. / Complex evaluation ofinformation security of an object with the application of a mathematical model for calculation of risk indicators. Lecture Notes in Electrical Engineering. – 2020. – Vol. 641 LNEE. – P. 771–778.*

2. *M. Kang and J. Kang. / A novel intrusion detection method using deep neural network for in-vehicle network security. – 2016 IEEE 83rd , – Vehicular Technology Conference (VTC Spring). – P. 1–5.*

3. D.Y. Yeung and Y. Ding. / Host-based intrusion detection using dynamic and static behavioral models, Pattern Recognition. – Vol. 36, – Issua 1 – 2003. – P. 229–243.