# Application of Deep Learning in Software Security Detection

**Lin Li[1, 2], Ying Ding[1, 2] and Jiacheng Mao[1, 2]**

College of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan, Hubei, China

Hubei Province Key Laboratory of Intelligent Information Processing and Real-time Industrial System, Wuhan, Hubei, China

**Keywords:** Deep learning; Software security; Detection; RNN.

**Abstract:** Machine learning is knowledge of learning rules from data through computational models and algorithms. It has been applied in various fields that require mining rules from complex data, and has become one of the most core technologies in the field of artificial intelligence in the broad sense. In recent years, a variety of deep neural networks have made remarkable achievements in a large number of machine learning problems, forming a new branch of machine learning, deep learning, and also raising a new climax of machine learning theory, method and application research. Software security is a highly concerned issue at present. Vulnerability detection technology is an important measure to improve software security. In order to make software application more secure, it is necessary to discuss the application of deep learning in software security detection.

## 1. Introduction

Discovering laws from phenomena is one of the most core abilities of human intelligence, and people have long started to study how to analyze laws in data by mathematical methods. Starting from Fisher's linear discrimination in the 1930s and perceptron algorithm in the 1950s, the discipline of pattern recognition was born, and the mathematical method of learning classified information from data was studied, forming the earliest machine learning research. The term "machine learning" was also coined in the late 1950s. Initially it did not specifically refer to learning from data, but rather to classic artificial intelligence problems such as machine reasoning. Now, the meaning of these two terms is very close. Pattern recognition refers to the classification of data, while machine learning refers to the rules of data, especially the rules of classification.

Many pattern recognition methods and statistical learning methods, such as linear discrimination, neighbor method, Rogers's regression, decision tree, support vector machines, have been successful on a wide range of issues, such as advertising click-through prediction, hag's sub-signal recognition, and disease typing based on gene expression. These statistical learning methods tend to classify the samples directly according to the features, without feature transformation or only once feature transformation or selection. Compared with deep learning methods, these methods have less feature transformation or rely on upstream processing to transform features, so some people call them "shallow model" or "shallow learning method".

These shallow models have been successful in a number of applications, but there are also significant limitations, where the effects of the models depend heavily on the features provided upstream. On the one hand, the process of constructing feature is very difficult, which requires abundant prior knowledge and detailed understanding of original data. On the other hand, in the case of insufficient prior knowledge, the number of features that need to be constructed by human is huge, such as the number of feature dimensions constructed by human in some AD click-through rate prediction algorithms is up to hundreds of millions of dimensions.

Deep learning is a deep machine learning model, whose depth is reflected in the multiple transformations of features. The commonly used deep learning model is a multi-layer neural network. Each layer of the neural network will conduct nonlinear mapping for input. By stacking the

DOI: 10.25236/iccse.18.089

multi-layer nonlinear mapping, very abstract features can be calculated in the deep neural network to help classify. Such as the convolution neural network is used for image analysis, will directly enter the pixel values of the original image, the first layer neural network can be regarded as the edge of the detector, while the second layer neural network can detect the edge of the combination, get some basic module, then deep network will these basic module combination, finally tested to identify the target. The emergence of deep learning makes people no longer need to select and transform the features alone in many applications, but input the original data into the model, and the model gives the characteristic representation suitable for classification through learning.

Cyclic neural network (RNN) is a kind of neural network used to process sequential data. Compared with the feed forward neural network (BP), which only allows the signal to be sent forward from input to output, RNN allows the signal to be transmitted forward and backward. They introduce loops in the network and allow internal connections to hide unit queries. With the help of this internal connection, RNN is better suited to use information from past data to predict future data. Here is a typical RNN cell. □

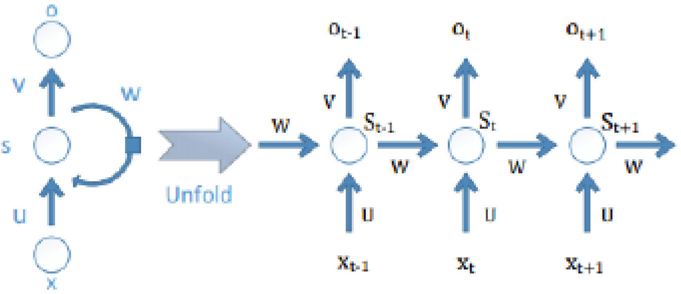

Figure 1 RNN unit

## 2. Organization of the Text

### 2.1 The status quo.

At present, information technology is in rapid development, and computer is gradually widely used in various fields. Computer software has become an important tool for informatization management and production in various fields, which is also an indispensable part in social life, and the frequency of use is gradually increased. The software brings convenience to people's production and life, but it also gives many opportunities for criminals to make profits. By taking advantage of the loopholes in the software, hacking into people's computers without anyone's authorization, or carrying out damage or stealing information, people will suffer losses. Therefore, software security is a highly concerned issue at present. Vulnerability detection technology is an important measure to improve software security. In order to make software application more secure, it is necessary to discuss. According to the nature of analysis, at present the software vulnerabilities are mainly security vulnerabilities and functional vulnerabilities. Security vulnerability is a design that is vulnerable to attack and attack. If these points are breached, the software will not work properly. Functional vulnerabilities affect the functioning of the software. If it is used, the software will not work properly, or there will be an error. First is the human factor is more clear, either way, what is certain is most of the holes is due to software developers, in the process of software design and development, some problems caused by human factors, developers in the error in calculating Settings or logic errors, formed the loophole, logic errors are common, not a single linear thinking mode makes overall software logic errors, calculation errors are appearing in some small and medium-sized module. The second is the persistence of vulnerabilities. On the one hand, software logic becomes more and more complex, so designers inevitably face the problem of improving the probability of logical error. On the other hand, if the environment in which the software is running changes, or changes the means of attack, new vulnerabilities will emerge. After fixing the original bug, there are new ones. Therefore, the software vulnerability basically exists for a long time, which requires real-time monitoring in the software operation and repair at any time to ensure that the software can be in normal operation. Finally, the vulnerability and the system lost contact. Software vulnerabilities emerge in the actual operation of a problem, and security vulnerabilities and running environment have been linked, different environment to produce holes completely different effects, such as security loophole, in some extremely high safety coefficient of environment, may be little impact, running environment and software compatibility is also affect the influence of the hole.

Why deep neural networks should be adopted is a representational problem of machine learning. The representation of multilayer perceptron neural networks has been studied theoretically in the last century: almost any function can be represented by an artificial neural network model of appropriate scale. This conclusion indicates that no matter how complex the classification or regression model can be represented by a specific neural network, as long as the neural network used has enough nonlinear nodes and enough hidden layers. Subsequently, Barron proposed a theorem, which further proved that the single hidden layer of nonlinear neural network can be used to represent almost any function. The theorem tells us that deeper neural networks are not more functional representations than shallow neural networks. In other words, as long as the number of nodes of the single hidden layer is large enough, the function of the multi-hidden layer neural network can also be represented. However, the conclusion about representativeness only indicates that there is a certain network structure capable of implementing arbitrarily complex function mapping, but does not mean that such a structure can be obtained or easy to obtain. It is pointed out that the representation ability of shallow neural network and deep neural network is still different, which is reflected in the relative relation between representation and number of parameters.

## 2.2 Looking forward to.

This detection technology is the entire section of the program for small pieces of segmentation, combined with the standard of these small pieces for testing, so we can determine whether there is the emergence of loopholes in the small section of this method is equivalent to in the article to test the lexical, therefore has the name, this method detection rate is relatively high, but the workload is very big, the feasibility of the implementation is limited.

This method starts very early. It is to verify the characteristics of the software by means of model calculus and by means of invisible calculation of fixed point and dominant search. This technology is more intuitive and more complicated to operate at the same time.

Non-execution stacks technique. Software data is stored on the current stack, but the stack is vulnerable to intrusion and attack, such as hackers planting code will form vulnerability. In recent years, this kind of attack often appears, the organization of this kind of attack, using this technology. This technology can effectively block hacker attacks by terminating the stack and allowing the intruder to continue access while making illegal access, but it can also negatively affect the computer operation and reduce the smoothness of the computer system.

Most of the time, an intruder USES a null character in memory to invade. This technique maps software code to different memory areas at any time, which makes it difficult for the intruder to find the code, but it is also difficult for the intruder to modify the system kernel itself.

The technology is the premise of the comprehensive definition on the computer, restrictions related to the attack, such as the preparation of the software with C language, all kinds of function has been defined, which is not the SYSTEM function, using the technology can be to limit of unknown function, this technology has not stopped within the definition of attack, so still need to improve. When the software is interpreted and executed, it can protect the program, protect related programs in real time and block intruders.

The region candidate network takes an image of any size as input and outputs a set of rectangular target suggestion boxes to select the best frame. Regional candidate networks have become an important part of some of the best target detection methods. RPN architecture of r-cnin method is combined with feature learning network layer and convolution middle layer to form an end-to-end full convolution network. The architecture of the network is shown in figure 1. The loss of feature information of the target through convolution and processed by BN layer and ReLU layer is very detailed, so the positioning result is not accurate. Therefore, the results obtained from the third convolution are processed by using the force formula of upper sampling, and the results of the first and second convolution are also sampled by using the idea of multi-layer feature fusion, and the data with the same multiple size as the result of the fourth layer is obtained. The final fusion result is used as the input of the classification layer and the border regression layer

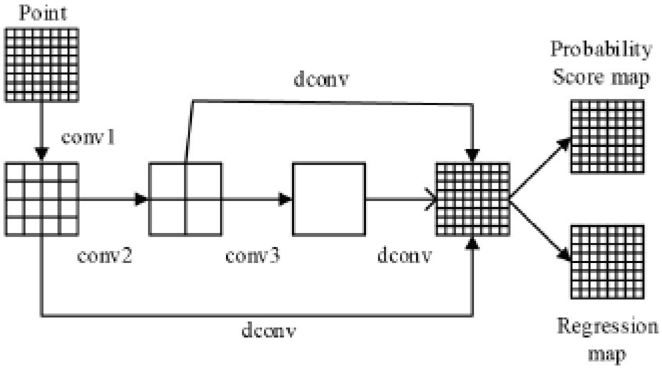

Figure 2 network structure

## 3. Conclusions

For traditional machine learning, the process of constructing features is very difficult in some complex problems. However, the performance of many traditional machine learning methods has strict theoretical guarantee under certain conditions. Deep learning can automatically extract features and gradually combine simple features into more complex features. By solving problems through these complex features, excellent application results have been achieved in many fields. However, the existing mathematical theories cannot give a good quantitative explanation, including the problem of generalization, representation and optimization. The future progress of theoretical research will further accelerate the development of deep learning and better guide the application of deep learning. Deep learning is the most cutting-edge field of machine learning methods at present. Deep learning is used to simulate human brain to analyze and summarize data. Combining Android application detection with deep learning methods is the future research direction. According to the above discussion, to obtain better optimization results, we need to start from three aspects: design of neural network structure, optimization algorithm and initialization method. Recently, many theoretical and experimental methods have emerged to analyze and discuss these three aspects. It is expected that people can have a deeper understanding of their advantages and application scope while showing a large number of successful application examples in deep learning.

## Acknowledgements

This work was supported by the Scientific Research Project of Hubei Provincial Department of Education (Grant No. B2018554); Hubei Province Key Laboratory of Intelligent Information Processing and Real-time Industrial System Open Fund(Grant No.2016ZNSS25C); National Natural Science Foundation of China (Grant No. 61472293); National College Students' innovation and entrepreneurship training project Construction of platform for popularizing programming thinking of AI in the age of youth.

## References

[1] Pei, Kexin, Cao, Yinzhi, Yang, Junfeng, et al. DeepXplore: Automated Whitebox Testing of Deep Learning Systems[J]. 2017:1-18.

[2] Yoo Y, Brosch T, Traboulsee A, et al. Deep Learning of Image Features from Unlabeled Data for

Multiple Sclerosis Lesion Segmentation[C]// International Workshop on Machine Learning in Medical Imaging. Springer International Publishing, 2014:117-124.

[3] Xiao B, Xiong J, Shi Y. Novel applications of deep learning hidden features for adaptive testing[C]// Asia and South Pacific Design Automation Conference. IEEE, 2016:743-748.

[4] Ding J, Kang X, Hu X H. Validating a Deep Learning Framework by Metamorphic Testing[C]// International Workshop on Metamorphic Testing. IEEE Press, 2017:28-34.

[5] Psuj G, Biernacki M, Kruczyński K. Application of deep learning procedure to magnetic multi-sensor matrix transducer data for the need of defect characterization in steel elements[C]// International Symposium on Electromagnetic Fields in Mechatronics, Electrical and Electronic Engineering. IEEE, 2017:1-2.

[6] Hangl S, Stabinger S, Piater J. Autonomous skill-centric testing using deep learning[C]// Ieee/rsj International Conference on Intelligent Robots and Systems. IEEE, 2017:95-102.