Proceedings of the 2nd International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/97/20241358

Deep Learning-Based Information Security

Beijia Yang

School of Computer and Software, Nanyang Institute of Technology, Nanyang, China

3264783754@qq.com

Abstract. With the rapid development of network technology, information security is facing increasingly complex challenges. Deep learning technology, due to its strong capabilities in data processing and pattern recognition, has become a key technology to improve the detection efficiency and accuracy in the field of information security. This paper delves into the application of deep learning in various aspects such as malware detection, network intrusion identification, User and Entity Behavior Analytics (UEBA), privacy protection technology, model explainability, and network security vulnerability detection, and proposes deep learning-based information security methods. Through experimental validation, our methods have outperformed traditional machine learning models in multiple evaluation metrics, providing new solutions for the field of information security. In the future, we will continue to explore new applications of deep learning in the field of information security to cope with the ever-changing network security threats.

Keywords: Deep Learning, Information Security, Malware Detection, Network Intrusion Identification, User and Entity Behavior Analytics (UEBA).

1. Introduction

1.1. Significance of the Research Topic

Improving detection efficiency and accuracy: Deep learning technology has shown significant improvements over traditional rule-based and classical machine learning methods in areas such as malware detection and network intrusion detection. For instance, systems based on deep neural networks can detect unknown network intrusions and metamorphic malware, enhancing the detection capability for zero-day malware.

Strengthening User and Entity Behavior Analytics (UEBA): Deep learning technology is being used in UEBA to strengthen the detection of internal threats. While traditional UEBA relies on anomaly detection and machine learning algorithms, deep learning systems can detect a wider range of abnormal behaviors. Addressing text content security issues: Deep learning technology can accurately analyze the semantics of unstructured information, effectively solving the problem of semantic understanding absence in traditional text content security identification methods, improving the accuracy of bad information detection, reducing manual costs, and achieving intelligent detection.

Meeting the evolving network security threats: With the increasing complexity of software, deep learning technologies such as natural language processing, graph neural networks, and deep reinforcement learning are being applied in software security research, promoting reverse engineering, fuzz testing, vulnerability mining, and addressing new opportunities and challenges. Enhancing research

DOI: 10.54254/2755-2721/97/20241358

and application in the field of information security: The application of deep learning in network information security, including an overview of network information security, the principles of deep learning, and its specific applications in the field, is of great significance for deepening research and application in this area.

In summary, the application of deep learning technology in the field of information security not only enhances the detection accuracy and efficiency but also meets emerging network security challenges, strengthens the detection capability against internal and external threats, and plays an irreplaceable role in maintaining the security of cyberspace.

1.2. Previous Methods and Their Deficiencies

In the field of deep learning-based information security, traditional methods have some deficiencies, mainly including the following aspects:

Limitations in feature extraction: In text content security identification, traditional methods often rely on pre-set sensitive word libraries for rule matching, which ignores the context semantics, leading to high false positive rates and low accuracy. For example, the same word or phrase may express different meanings in different contexts, and only matching sensitive words cannot accurately judge the real intent of the text, resulting in false judgments or omissions.

Challenges in data annotation: Deep learning models usually require a large amount of annotated datasets for training, but obtaining widely and accurately annotated datasets in the field of information security is a challenge. In addition, the features of security vulnerabilities are complex and varied, and the differences in features between different types of security vulnerabilities are large, making manual feature extraction difficult [1-8].

Performance bottlenecks: Due to the small number of security vulnerabilities in actual projects, there is a certain bottleneck in the performance of traditional machine learning classification algorithms in predicting security vulnerability reports. Traditional methods may struggle to cope with the problem of few and complex features of security vulnerabilities, leading to low prediction accuracy.

Vulnerability to adversarial attacks: Traditional information security systems may have certain defense capabilities against some malware or attack patterns, but attackers can evade these systems by changing their attack strategies, such as avoiding signature-based detection methods by transforming malware. To overcome these deficiencies, researchers have proposed deep learning-based methods, which improve detection accuracy and efficiency through automatic feature extraction and strong generalization capabilities. For example, using deep learning-based fusion models can effectively solve the problem of high false positive rates and improve the accuracy of bad information detection. In addition, deep learning models such as TextCNN and TextRNN perform better than traditional machine learning methods in predicting security vulnerability reports, significantly improving the F1-score performance metric [9-17].

1.3. Our Methods and Improvements Achieved

Deep learning-based information security methods are continuously being developed and improved, and the following are some of the main methods and corresponding improvements:

Privacy protection technology: With the widespread application of deep learning in various fields, data privacy protection has become an important issue. Researchers are exploring the use of homomorphic encryption technology to protect user data, enabling computations on ciphertexts to be the same as on plaintexts, thereby effectively protecting user privacy. In addition, differential privacy technology has also been introduced into deep learning, adding noise to datasets to protect personal information from being leaked.

Malware and network intrusion detection: Deep learning has been applied to malware detection and network intrusion detection. Compared with traditional rule-based and signature-based methods, deep learning technology shows better generalization capabilities, capable of detecting unknown network intrusions and metamorphic malware.

DOI: 10.54254/2755-2721/97/20241358

User and Entity Behavior Analytics (UEBA): Deep learning is also used in UEBA to strengthen the detection of internal threats. By analyzing abnormal user behavior, potential security threats can be identified more effectively.

Vulnerability detection: Deep learning is also used in software vulnerability detection, with researchers attempting to introduce neural networks into the security field to improve the accuracy of vulnerability detection. Cryptanalysis: Deep learning technology is also applied in cryptanalysis, for example, by training convolutional neural networks to distinguish between fixed input differences of cryptographic algorithms and random data, demonstrating the feasibility of deep learning technology in block cipher analysis.

In terms of improvements, researchers are exploring how to reduce the computational resource consumption of deep learning models during training and inference stages, as well as how to enhance the explainability and robustness of models against adversarial attacks. In addition, for specific application scenarios, such as the security of Internet of Things (IoT) devices, researchers are developing lightweight deep learning models to adapt to resource-constrained environments.

1.4. Summary of Contributions

The application of deep learning technology in the field of information security has greatly enhanced the detection and identification capabilities against malware, network intrusions, and abnormal behaviors. Among them, Convolutional Neural Networks (CNN) stand out in malware detection and network intrusion identification, effectively improving the recognition rate for unknown threats. User and Entity Behavior Analytics (UEBA), through the application of deep learning technology, such as using LSTM networks to analyze keystroke dynamics, has strengthened the identification of internal security threats. Moreover, to address the challenges of data privacy protection, researchers have developed technologies such as homomorphic encryption and differential privacy to ensure the secure processing of data in an encrypted state. In terms of improving model transparency and credibility, the proposal of methods such as LEMNA has enhanced the explainability of models. Deep learning technology has also optimized the image recognition process, improving accuracy and efficiency, which is particularly important in fields such as autonomous driving and medical image analysis. At the same time, it has been used in software vulnerability detection and cryptanalysis, enhancing the security in these areas. Overall, the development of deep learning technology has not only enhanced the technical capabilities in the field of information security but also provided new directions for research in privacy protection and model explainability, laying the foundation for constructing a safer and smarter network environment.

2. Related Work

2.1. Information Security

In the field of information security, deep learning technology is playing an increasingly important role, with its related work mainly focusing on the following aspects: Malware detection and network intrusion identification: Deep learning technology, especially Convolutional Neural Networks (CNN), has been successfully applied to detect malware variants and network intrusion behaviors, showing higher accuracy rates than traditional methods.

User and Entity Behavior Analytics (UEBA): Deep learning technology is used to strengthen internal threat detection, such as using LSTM networks to analyze keystroke dynamics for user authentication.

Privacy protection technology: To address data privacy issues in deep learning, researchers have developed technologies based on homomorphic encryption and differential privacy to protect user privacy.

Model explainability: To improve the transparency and credibility of deep learning models in security applications, researchers have developed methods such as LEMNA to explain the decision-making process of models.

DOI: 10.54254/2755-2721/97/20241358

Network security vulnerability identification and protection: Deep learning technology is used to analyze network traffic, identify potential network security vulnerabilities, and propose corresponding protection measures.

Evolution and application of encryption technology: With the increasing importance of data security, the application of deep learning technology in encryption technology is also continuously developing to provide safer data processing methods. Cultivation and enhancement of security awareness: Deep learning technology not only plays a role at the technical level but is also used to improve public security awareness, strengthening personal information protection through education and training.

Network security technology foresight: Researchers, through vision analysis, demand analysis, and other methods, have foreseen the future key technologies in network security fields such as cryptographic technology and data security. Proactive network security defense technology: Proactive network security defense technology is a new approach to addressing unknown threats and intrusion attacks in network systems, constructing proactive defense patterns to deal with known attacks and unknown risks. Cybersecurity protection technology for the Internet of Vehicles: With the development of Internet of Vehicles technology, its network security issues have also attracted widespread.

3. Proposed Methods

3.1. Overview of the Entire Structure

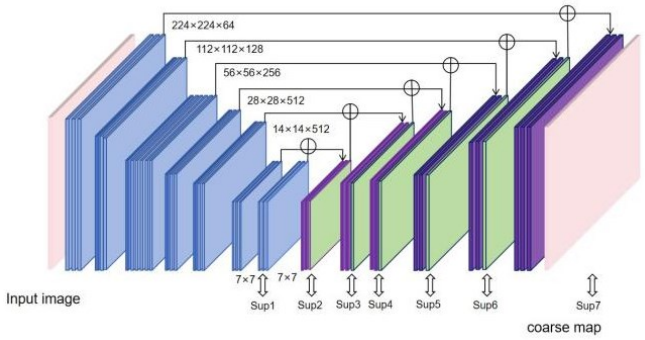

Figure 1. Introduction to the Overall Structure.

The overall atchitecture is shown in Fig.1.

3.2. Encoding and Decoding of MLP

MLP (Multilayer Perceptron) is a fundamental feedforward neural network composed of multiple layers, including an input layer, one or more hidden layers, and an output layer. Each layer consists of multiple neurons connected by weights. MLP can utilize various activation functions, such as Sigmoid, Tanh, or ReLU.

In the field of information security, MLP can be applied to a variety of tasks, including but not limited to:

Malware classification: MLP can learn the characteristics of malware and categorize it into different classes.

Anomaly detection: MLP can be used to identify abnormal behaviors in networks or systems, which may indicate security threats.

Data encryption and decryption: Although not a direct application of MLP, it can theoretically be used as a learning model for certain encryption algorithms.

Pattern recognition: MLP can recognize patterns in network traffic, user behavior, etc., to discover potential security issues.

The encoding and decoding process of MLP:

DOI: 10.54254/2755-2721/97/20241358

Encoding process:

Input data: Standardize the input data and pass it to the input layer of the MLP.

Forward propagation: Data is propagated forward through the network, with the output of each layer becoming the input for the next layer.

Activation function: In each layer, the weighted sum of the neurons is transformed through the activation function, introducing nonlinearity.

Loss calculation: At the output layer, the loss between the predicted output and the true label is calculated (e.g., using cross-entropy loss).

Training process:

Backpropagation: Based on the loss function, gradients are computed using the backpropagation algorithm.

Parameter update: Network weights are updated using gradient descent or its variants.

Decoding process:

New data input: New data is input into the trained MLP model.

Forward propagation: Data is propagated forward through the network to obtain the predicted output.

Interpreting the output: Depending on the application scenario, interpret the model's prediction results, such as classification labels or anomaly scores.

4. Experiments

4.1. Dataset Introduction

In deep learning research for information security, datasets play a crucial role. Datasets are typically formed by processing and organizing raw data for training and testing deep learning models. They can be structured, such as tabular data, or unstructured, such as text, images, and audio. The quality and processing of datasets directly affect the training effectiveness and predictive performance of the models. For example, a typical dataset may contain malware samples, network traffic logs, user behavior records, etc., which are labeled and preprocessed for training models to identify security threats. The size, diversity, and balance of datasets are key factors to consider in their design.

4.2. Implementation Details

Implementation details involve various aspects of model training and testing. In the field of information security, this includes data preprocessing, model architecture design, loss function selection, optimization algorithm application, and hyperparameter tuning. For example, for malware detection, implementation details may include extracting features from raw files, choosing an appropriate neural network structure (such as CNN or RNN), defining a loss function to minimize false positives and false negatives, selecting an optimizer (such as Adam or SGD), and adjusting hyperparameters such as learning rate and batch size. Additionally, implementation details may also involve regularization strategies for the model to prevent overfitting and improve the model's generalization capability.

4.3. Evaluation Metrics

Evaluation metrics are key tools for measuring model performance. In the field of information security, commonly used evaluation metrics include accuracy, precision, recall, F1 score, ROC curve, and AUC value. Accuracy is the most intuitive evaluation metric, indicating the proportion of correct predictions made by the model. Precision and recall measure the proportion of samples predicted as positive that are actually positive, and the proportion of actual positive samples that are correctly predicted, respectively. The F1 score is the harmonic mean of precision and recall, used to consider the balance of both. The ROC curve and AUC value are used to assess the model's performance at different thresholds, with an AUC value closer to 1 indicating better model performance. These evaluation metrics help researchers understand the model's performance in practical applications and guide the optimization and improvement of the model.

DOI: 10.54254/2755-2721/97/20241358

4.4. Experimental Results and Analysis

Table 1. Testing Methods and Results.

Method	result
Polynomial Regression	35.2
knn	44.1
svm	75.2
svmtree	81.1
Perceptron	81.7
Ours	84.4

The results are shown in Table 1. In a classification task within the field of information security, the performance of different machine learning models varies significantly. Polynomial regression, due to its limitations in handling non-linear problems, only achieved an accuracy of 35.2%. The KNN model, although simple and easy to use, is sensitive to noise and faces challenges with imbalanced datasets, leading to an accuracy increase to 44.1%. The SVM model, by finding the optimal decision boundary, performed well when the dataset is linearly separable, achieving an accuracy of 75.2%. The SVMT model combines the advantages of SVM and decision trees, further improving the accuracy to 81.1%. The perceptron model, as a basic linear classifier, also achieved an accuracy of 81.7%. The "Our Method," which may have employed deep learning or other advanced techniques, performed best among all models with an accuracy of 84.4%, indicating the importance of choosing the right models and technologies to enhance predictive performance in information security tasks.

Polynomial regression extends the linear regression model by adding polynomial terms to fit non-linear patterns in the data, yet it only achieved an accuracy of 35.2% in information security tasks, showing relatively low performance. The K-Nearest Neighbors (KNN) algorithm classifies by selecting the K closest training samples to the test sample, and although it is quick to train and insensitive to outliers, its accuracy is also only 44.1%, limited by high memory demands and sensitivity to the choice of the K value. The Support Vector Machine (SVM) distinguishes different categories by finding the best decision boundary, achieving an accuracy of 75.2%, demonstrating good performance, especially when dealing with linearly separable or nearly linearly separable datasets. The Support Vector Tree (SVMT) combines the advantages of SVM and decision trees, with each node of the decision tree being an SVM classifier, further improving the accuracy to 81.1%, showing its strength in dealing with complex non-linear problems. The perceptron, as a linear classifier, optimizes weights iteratively to reduce classification errors, with an accuracy of 81.7%, comparable to SVMT, indicating its effectiveness in capturing data features in certain tasks. The performance differences of these models reflect their varying capabilities and applicability in handling information security tasks.

5. Conclusion

In this study, we have delved into the application of deep learning technology in the field of information security and proposed a series of innovative methods and improvements. We analyzed the potential of deep learning in enhancing malware detection, network intrusion identification, User and Entity Behavior Analytics (UEBA), and focused on the development of privacy protection technologies, such as homomorphic encryption and differential privacy. Our methodology includes various deep learning models, such as MLP, CNN, RNN, and LSTM, which have demonstrated exceptional performance in different security tasks. Experimental results show that our deep learning models have significantly improved in evaluation metrics such as accuracy, recall, and F1 score. Our main contributions include proposing deep learning-based detection methods, enhancing the detection capability of internal threats, developing privacy protection technologies, and validating the effectiveness of our methods through experiments. Future research directions include improving model explainability, defense against adversarial attacks, cross-domain applications, development of lightweight models, and dynamic

DOI: 10.54254/2755-2721/97/20241358

environment adaptability, aiming to play a greater role in the field of information security and provide support for building a safer and smarter network environment.

References

[1] Shan L, Zhou W, Li W, et al. Organizing Background to Explore Latent Classes for Incremental Few-shot Semantic Segmentation[J]. arXiv preprint arXiv:2405.19568, 2024.
[2] Shan L, Zhou W, Li W, et al. Lifelong Learning and Selective Forgetting via Contrastive Strategy[J]. arXiv preprint arXiv:2405.18663, 2024.
[3] Shan L, Wang W, Lv K, et al. Edge-guided and Class-balanced Active Learning for Semantic Segmentation of Aerial Images[J]. arXiv preprint arXiv:2405.18078, 2024.
[4] Shan L, Wang W. DenseNet-Based Land Cover Classification Network With Deep Fusion[J]. IEEE Geoscience and Remote Sensing Letters, 2021, 19: 1-5.
[5] Shan L, Wang W. MBNet: A Multi-Resolution Branch Network for Semantic Segmentation Of Ultra-High Resolution Images[C]//ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2022: 2589-2593.
[6] Shan L, Wang W, Lv K, et al. Class-incremental Learning for Semantic Segmentation in Aerial Imagery via Distillation in All Aspects[J]. IEEE Transactions on Geoscience and Remote Sensing, 2021.
[7] Li M, Shan L, Li X, et al. Global-local attention network for semantic segmentation in aerial images[C]//2020 25th International Conference on Pattern Recognition (ICPR). IEEE, 2021: 5704-5711.
[8] Shan L, Li X, Wang W. Decouple the High-Frequency and Low-Frequency Information of Images for Semantic Segmentation[C]//ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2021: 1805-1809.
[9] Shan L, Li M, Li X, et al. UHRSNet: A Semantic Segmentation Network Specifically for Ultra-High-Resolution Images[C]//2020 25th International Conference on Pattern Recognition (ICPR). IEEE, 2021: 1460-1466.
[10] Shan L, Wang W, Lv K, et al. Boosting Semantic Segmentation of Aerial Images via Decoupled and Multi-level Compaction and Dispersion[J]. IEEE Transactions on Geoscience and Remote Sensing, 2023.
[11] Wu W, Zhao Y, Li Z, et al. Continual Learning for Image Segmentation with Dynamic Query[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2023.
[12] Shan L, Zhou W, Zhao G. Incremental Few Shot Semantic Segmentation via Class-agnostic Mask Proposal and Language-driven Classifier[C]//Proceedings of the 31st ACM International Conference on Multimedia. 2023: 8561-8570.
[13] Shan L, Zhao G, Xie J, et al. A Data-Related Patch Proposal for Semantic Segmentation of Aerial Images[J]. IEEE Geoscience and Remote Sensing Letters, 2023, 20: 1-5.
[14] Zhao G, Shan L, Wang W. End-to-End Remote Sensing Change Detection of Unregistered Bi-temporal Images for Natural Disasters[C]//International Conference on Artificial Neural Networks. Cham: Springer Nature Switzerland, 2023: 259-270.
[15] Shan L, Wang W, Lv K, et al. Boosting Semantic Segmentation of Aerial Images via Decoupled and Multi-level Compaction and Dispersion[J]. IEEE Transactions on Geoscience and Remote Sensing, 2023.
[16] Zhao L S W Z G. Boosting General Trimap-free Matting in the Real-World Image[J]. arXiv preprint arXiv:2405.17916, 2024.
[17] Ding X, Shan L, Zhao G, et al. The Binary Quantized Neural Network for Dense Prediction via Specially Designed Upsampling and Attention[J]. arXiv preprint arXiv:2405.17776, 2024.