J Inf Process Syst, Vol.21, No.1, pp.1~12, February 2025
https://doi.org/10.3745/JIPS.04.0331
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

RAE-SVM based Webpage Tamper-Resistant Detection Algorithm

Changjian Zhou[1], Yutong Zhang[2], Yunfu Liang[3], and Jinge Xing[3,*]

Abstract

Cybersecurity has become a key component of national strategy in recent years. Traditional cybersecurity technology such as network traffic-based intrusion detection and threatening intelligence sensing are designed to focus on the traffic features of network, which are no doubt effective defense technologies. However, these methods required decent amount of domain knowledge and massive training data, which brought a significant barrier for cybersecurity research. In this work, we propose a novel residual autoencoder and support vector machine combined approach (RAE-SVM) for webpage tamper-resistant detection using high-level webpage image features. This method, inspired by the Chinese proverb "mend the fold after the sheep have been stolen." The web crawler technology is used for website screenshot within limited domain names, and input them into autoencoder architecture and SVM for feature extraction and invaded webpage detection. This method combines the advantages of deep residual network, convolutional autoencoder and SVM, and the interdisciplinary intersection between cybersecurity and high-level image features. The experimental results demonstrate that the proposed method achieves an accuracy of 95%, significantly higher than other models, which proves the validity of the proposed method.

Keywords

Cyber Security, Deep Autoencoder, Image Features, Support Vector Machine, Tamper-Resistant Detection

1. Introduction

As the Internet continues to provide unparalleled convenience, the urgency of addressing cybersecurity issues has grown exponentially. It also has been designated as a national territorial security topic in many countries. Since the symptoms of intrusion are mainly visible on webpages, the majority of cybersecurity incidents are displayed through webpages. It is an important responsibility of cybersecurity personnel to protect webpages from being tampered. Recently, with the wide use of machine learning approaches by defenders and attackers, especially the rapid application of deep convolutional neural networks (deep CNN), the deep architecture models have pushed the automated cyber-threats detection technique to a new level. However, regardless of traditional machine method or deep learning method for cyber network, a large amount of training data is necessary. When building a specific application case, such as colleges, hospitals etc., it's hard to get enough data for training a classifier.

Manuscript received February 16, 2022; first revision June 21, 2022; second revision August 18, 2022; accepted September 9, 2022.

* **Corresponding Author:** Jinge Xing (xingjinge@neau.edu.cn)
[1] Department of Modern Educational Technology, Northeast Agricultural University, Harbin, China. (zhouchangjian@neau.edu.cn)
[2] College of electrical & information, Northeast Agricultural University, Harbin, China (zhangyutong@neau.edu.cn)
[3] Department of Modern Educational Technology, Northeast Agricultural University, Harbin, China (yfliang@neau.edu.cn; xingjinge@neau.edu.cn)

Recently, machine learning based cybersecurity techniques have been further improved for proactive defense and detection of cyber-attacks, and these studies have achieved excellent performance in different tasks. Machine learning technique can automatically extract valuable features in massive datasets and make decisions based on them [1]. Machine learning-based cybersecurity methods can obtain satisfactory results when given massive training data, making it possible to detect attack variants, which are mainly divided into the following aspects.

(1) Content based webpage tamper-resistant detection method. This method attends to concentrate the file content and information of the website, which is necessary to read and write files continuously. He et al. [2] proposed a unified modeling language-based connected and autonomous vehicle (CAV) cyber-security framework. They designed two classifier models based on naive Bayes and decision tree, respectively. When identifying each type of communication-based attacks tasks, the decision tree model is more appropriate for communication attack detection since it requires a shorter runtime. Jaber and Rehman [3] focused on the internet pay-per-use system, the authors proposed a fuzzy k-means clustering algorithm-based intrusion detection system, which can detect the anomalies with low false positive rate and high detection accuracy compared with existing mechanisms. Kumar et al. [4] deeply analyzed the security of social networks and found that there are a great number of users were unaware of the privacy concerns. The authors investigate the evolution of online social networks and discuss various security models using machine learning and deep learning methods. Finally, the authors gave a better solution for protecting personal privacy.

(2) Low level features-based webpage tamper-resistant detection methods. Al-Eidi et al. [5] proposed an automated covert temporal channels detection using image processing method. This method can detect the malicious part automatically in covert channels and reduce the quality-of-service degradation caused by blocking the entire traffic in the hidden channel. It achieves detection accuracy and covert traffic accuracy of 95.83% and 97.83%, respectively. Nowroozi et al. [6] gave a survey of adversarial image forensics using machine learning models to enhance the robustness of machine learning binary operation detector in various confrontation scenarios. Sarker et al. [7] proposed an intrusion detection decision tree security model by ranking the security features in the order of their importance, and building an intrusion detection decision tree based on the order of important features. Experimental results showed that this model is better than the existing models. Dehghani et al. [8] proposed a false data injection attacks detection method. The factors and wavelet features were adjusted and extracted, defining the input indexes based on deep learning, and a cyber-protection method was proved a high accuracy. Yavuz et al. [9] proposed an Internet of Things (IoT) routing attacked detection method based on deep learning. Since the Cooja IoT simulator generated high-fidelity attack data within 10 to 1,000 nodes of IoT networks, a highly scalable IoT routing attacked detection methodology was designed. The accuracy and precision of the proposed method is satisfactory in IoT cybersecurity area. Ko et al. [10] analyzed the DDoS attack vector of malware facilitated, the infection of 5 new devices per minute attracted by DDoS, and proposed a stacked self-organizing map method based on deep learning. Yuan et al. [11] proposed a byte level malware classification method based on Markov image, which adopted bytes transfer probability matrix, and then input them into deep architecture models. It achieved the 99.264% and 97.364% accuracy on the datasets of the Drebin and Microsoft.

Most of the above works have achieved a high-level performance in specific areas. However, the content-based webpage tamper-resistant detection method needs frequent read and write operations

[12,13], which has a waste of time and no guarantee of timeliness. Low level features-based webpage tamper-resistant detection methods pay more attention to traffic characteristics, which needs rich network security knowledge reserve. Unfortunately, there is a shortage of such talents in society [14]. Since the network environments change quickly, traditional machine learning methods are difficult to adapt to the various attacks [15]. Deep learning methods may be effective tools for protecting information systems from attacks, however, due to the constantly evolving hacker attacks, preventing information systems from being invaded is still a great challenge for cybersecurity researchers [16,17].

To address the high frequently read and write requirements of traditional low level based webpage tamper-resistant detection methods, this work thought in a different way and proposed a deep residual auto-encoder and SVM combined intrusion detection algorithm named RAE-SVM. The RAE-SVM method detects webpage anomaly using the image features based on deep and shallow learning and without large training data. In addition, the RAE-SVM requires fewer professional network security knowledge to achieve a high detection accuracy. The main contributions of this work are as follows.

- A novel residual attention based auto-encoder and SVM combined approach for webpage tamper-resistant detection is proposed, which takes advantage of the residual network and SVM.
- The proposed model only needs a small amount of training data to get excellent performance.
- The residual attention block is proposed to adjust the weight value of residual connection adaptively.

The rest of this article is organized as follows. The related works are stated in Section 2. Section 3 discusses the proposed method. The experiment result analysis and discussion are detailed in Section 4. Section 5 provides the conclusions.

2. Related Works

In this study, the two different machine learning methods are combined for webpage tamper-resistant detection task. The deep learning method is used for feature extraction and the shallow learning methods such as SVM is introduced for feature classification. This work contrasted various deep learning methods and adopted deep residual autoencoder and support vector machine combined method for feature extraction and classification, respectively. A brief review of the two branches is given as follows.

2.1 Deep Residual Autoencoder

Auto-encoder is one of the classic artificial neural networks, which consists of encoder unit and decoder unit [18]. Consider $X = \{x_1, x_2, \dots, x_n\}$ as the input features space, and Y as the feature representation space. The autoencoder aims to find a mapping function f, which finds the minimum loss of X and Y. To improve the feature encoder capability, the state-of-the-art deep architecture residual network is employed in the encoder unit, which takes advantage of the strong feature expression ability and makes the encoded feature more representative. Deep residual autoencoder has achieved strong feature representation and dimensionality reduction in various tasks [19].

2.2 Support Vector Machine

SVM is one of the most powerful and robust approaches in the advance of limited training data [20],

which aims to find a Decision Hyperplane as indicated in Fig. 1.

After extracting the features of captured screenshots images, we pass them into SVM classifier to calculate the maximum value of d, which can effectively satisfy the classification in Eq. (1). Since the SVM classifier principle is very familiar to us, the detailed derivation will not be repeated in this paper.

$$y \cdot (w^T \cdot x_i + \gamma) \geq 1, \tag{1}$$

where y is the labels, x is the input feature, The parameter d is calculated in Eq. (2):

$$d = \frac{\hat{\gamma}}{\| w \|} = \frac{y_i \cdot (w^T \cdot x_i + \gamma)}{\| w \|} = \frac{1}{\| w \|}, \tag{2}$$

where d represents the distance from the vector points to hyperplane. The Lagrangian function is introduced as shown in Eq. (3):

$$L(w, b, a) = \frac{1}{2} \cdot \| w \|^2 - \sum_{1}^{n} a_i \cdot (y_i \cdot (w^T \cdot x_i + b) - 1) \text{ s.t. } y_i(w^T \cdot x + b) \geq 1, \tag{3}$$

where the factor $a_i \geq 0$, and the optimal approach is shown in Eq. (4):

$$\theta(w) = \max_{a_i \geq 0} L(w, b, a) = \frac{1}{2} \| w \|^2. \tag{4}$$

Thus, the parameter d is maximized while $\frac{1}{2} \| w \|^2$ is minimized.

The SVM classifier is used for calculating the maximum value of d and generating the webpage images, which are not in the baseline category, and we believe that the generated webpages are tamper-resistant.

To reduce the amount of calculation, numerous kernel functions such as Sigmoid, Anova, Gaussian, and liner kernel function are employed in various downstream tasks. The Gaussian kernel function is most widely used because it maps finite dimensional data to high-dimensional space.

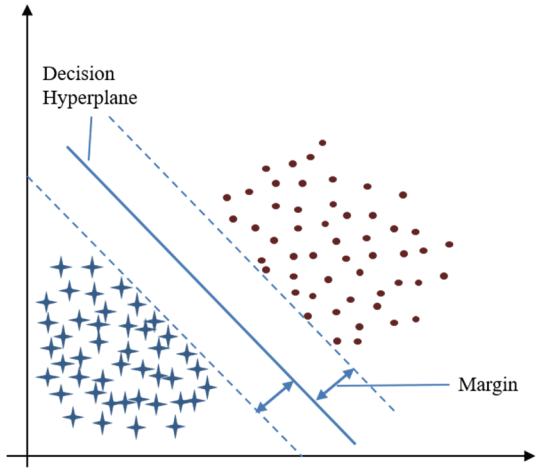


Fig. 1. The diagram of support vector machine.

3. Proposed Method

Although there are many variants and novel ways of protecting information systems from intrusion, there are still countless attacks every day. In this paper, we had taken another way, drew our inspiration from the perspective of network user behavior, and proposed a deep and shallow learning combined method for webpage tamper-resistant detection.

3.1 Model Architecture

To improve the feature representation ability, a robust deep learning architecture for feature extraction is necessary. In this work, a residual attention auto-encoder and SVM combined architecture for feature learning and extraction is proposed, as demonstrated in Fig. 2. The deep residual attention autoencoder approach RAE-SVM is presented for detecting the anomalous webpages. Firstly, the web crawler tools are employed for grabbing all the webpages screenshots within the preset domain name and establishing index marks with the domain name. Then the model identifies whether this domain name appears for the first time and checks whether it is abnormal. If not, put it into the classifier for feature extraction, and the extracted features are used as the baseline features. If the domain name does not appear for the first time, then input them into the classifier for prediction. Once the prediction results indicate that the webpage is abnormal, an alarm will be sent automatically.

Compared to other deep learning methods, the deep residual autoencoder considers the relationships between the features, eliminating irrelevant and visual attention redundant features, makes it accomplish strong feature representation and ensures to preserve the features spatial locality. This method largely resolves the network degradation and gradient vanishing problem, allowing it to maintain an excellent performance in feature representation stage.

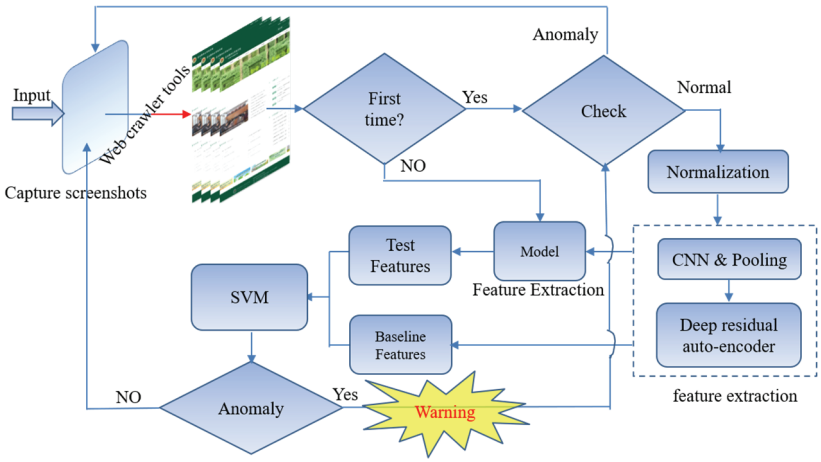


Fig. 2. The architecture of RAE-SVM.

3.2 CNN and Pooling Block

CNN and pooling block undertakes the task of dimension reduction and feature fusion. The convolution layer with Conv(1×1) is employed for feature integration and the $Pooling$is introduced for dimensionality

reduction. In this work, we proposed a novel $Pooling$ method, as shown in Eq. (5):

$$Pooling = Concate(maxpooling, averagepooling), \tag{5}$$

where $Pooling$ means the proposed pooling operation, $Concate$ means concatenating $maxpooling$ and $averagepooling$ methods on the channel dimension.

3.3 Attention Block

The architecture of attention based deep residual autoencoder is illustrated in Fig. 3. The attention block in RAE-SVM model is defined as Eq. (6):

$$F_k = f(I * \mathrm{W}(x_L) + r_L), \tag{6}$$

where $*$ represents the convolution operation, I denotes the output of the L-th layer. $W \in [0,1]$ denotes the weight matrix $f(\cdot)$ is the residual connection operation, r_L denotes the residual block features of the L-th layer. This architecture works well as the attention based feature monitors which suppress the redundant features to improve the weight of valuable features. The decoding approach is represented as shown in Eq. (7):

$$\mathrm{Z} = f\left(F_L * X_L^T + r_L^{'}\right), \tag{7}$$

where T is the matrix transposition unit.

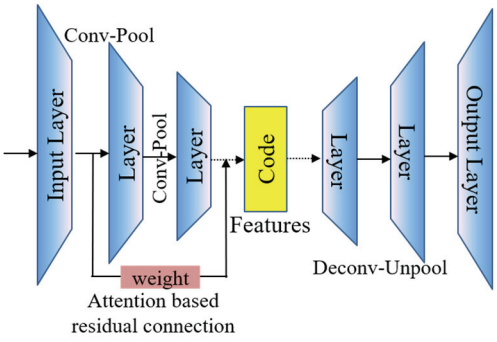


Fig. 3. The architecture of attention based deep residual autoencoder.

4. Experiment Analysis and Discussion

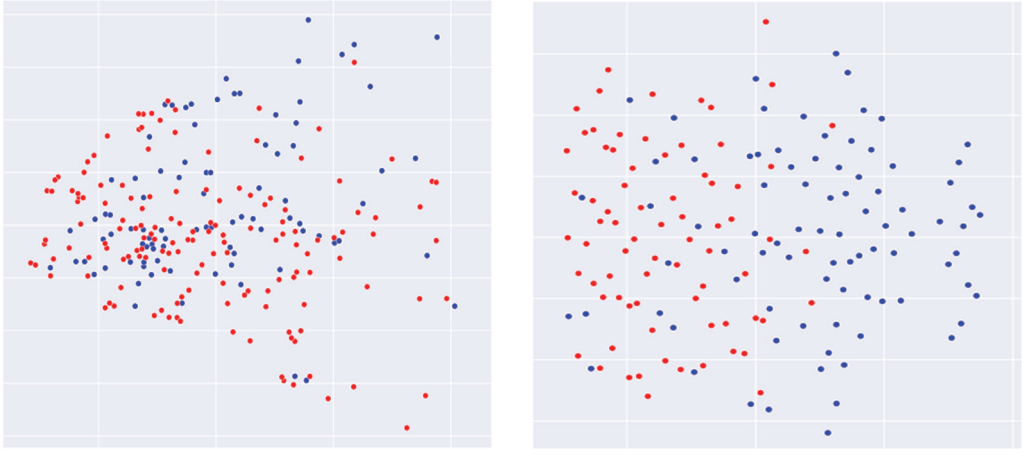
4.1 Experimental Environment

This study employs the high-performance computing (HPC) platform with Cent OS 8 Linux operating system, where 2×NVIDIA 2080 Ti graphics processing units (GPU) are adopted for accelerating calculation speed. In this work, 1,291 screenshots of second-level images were captured site under more than 50 websites within the domain name of Northeast Agricultural University. Part of the captured webpage images are shown in Fig. 4(a). The invaded web images are annotated manually by adding random

images, and part of them are shown in Fig. 4(b). The distribution of positive and negative samples can be visualized by t-Distributed Stochastic Neighbor Embedding (t-SNE) in Fig. 5, where the blue dots denote the normal web images and the red ones denote the tampered web images. It is obvious that the normal and tampered webpage images are hardly distinguished from each other.

(a) (b)

Fig. 4. (a) Part of the captured webpages images and (b) part of the tampered web images.



(a) (b)

Fig. 5. (a) Original training data visualization and (b) the visualization extracted features.

4.2 Training Details

In this work, there are 1,291 positive instances and 2,000 negative instances collected. All of the raw data was curated into three classes, 60% for training, 20% for validation, and 20% for testing. All of the simple images are resized to 512×512 pixels, the batch size is set as 8, and the RMSProp and Binary crossentropy functions are adopted as optimizer and loss function respectively. The two-activation functions such as Sigmoid and ReLU are introduced in this work as shown in Eqs. (8) and (9):

$$\text{Sigmoid}(t) = \frac{1}{1+e^{-t}}, \tag{8}$$

$$\text{ReLU}(t) = \begin{cases} t, & \text{if } t > 0 \\ 0, & \text{if } t \leq 0' \end{cases} \tag{9}$$

where t is the original prediction probability value. Sigmoid function is adopted in full connection layer, which aims to map variables in [0,1]. And ReLU function is utilized in the residual block to alleviate gradient disappearance.

In this work, the webpage image features were extracted before being passed into SVM classifier. Through comparative analysis, we extracted the codes in deep residual autoencoder as the features of samples. The distribution of extracted features can be shown by t-SNE in Fig. 5(b). It can be seen that the features present a clustering trend but less than ideal. Therefore, the SVM classifier with powerful classification ability introduced in this work is necessary. The radial basis function (RBF) kernel function in SVM is the mapping gap between low and high dimension which is detailed in Eq. (10):

$$K(x, x_i) = \exp\left(-\frac{\|x - x_i\|^2}{2\sigma^2}\right), \tag{10}$$

where K is the kernel function, σ is the constant parameter and x is the vector.

4.3 Result Analysis and Discussion

4.3.1 Evaluation metrics

To verify the effect of the proposed RAE-SVM model in a more comprehensive way, it is essential to compare the model with the traditional classical models and the results published recently. The selected evaluation index is shown in Eqs. (11)–(14):

$$Precision = \frac{True\ positive}{True\ positive + False\ positive}. \tag{11}$$

Precision is mainly used to measure the prediction results, and predict the correct probability in the positive sample.

$$Recall = \frac{True\ positive}{True\ positive + False\ negative}. \tag{12}$$

Recall is mainly used to measure the index of the sample, which is used to show how many positive examples in the sample are predicted correctly.

$$F1 - score = \frac{2(Precision * Recall)}{Precision + Recall}. \tag{13}$$

F1-score is an important indicator of the model to evaluate the binary classification, which takes both precision and recall into account.

$$Accuracy = \frac{True\ positive + True\ negative}{N}. \tag{14}$$

Accuracy is a common indicator mainly for all samples, and it is one of the important indicators for

comprehensive evaluation of the model.

4.3.2 Ablation study and comparison

To verify the superiority of the proposed method and the basic components, this work adopted the classic state-of-the-art models such as ResNet-50, SVM, k-nearest neighbor (KNN), AlexNet, DenseNet-121 for comparison. In addition, the recently released webpage tamper-resistant detection approaches such as PCA+SVM method [21], Autoencoder & SVM [22], SnapCatch [5], IntruDTree [7], and Dehghani [8] are also employed for comparison. The metrics of all methods are shown in Table 1.

Table 1. Experimental results

Approach	Precision	Recall	F1-score	Accuracy
Deep ResNet-50	0.72	0.67	0.69	0.71
SVM	0.81	0.83	0.82	0.85
KNN	0.68	0.61	0.64	0.65
AlexNet	0.73	0.64	0.68	0.68
DenseNet-121	0.76	0.66	0.7	0.7
PCA + SVM	0.92	0.85	0.88	0.89
Auto-encoder + SVM	0.97	0.87	0.92	0.92
SnapCatch	0.9	0.92	0.91	0.92
IntruDTree	0.89	0.94	0.91	0.94
Dehghani	0.91	0.94	0.92	0.93
Proposed method	0.96	0.94	0.94	0.95

It shows that the KNN method has the lowest accuracy compared with the deep set and the combined models; this is mainly because the deep learning models can generally achieve a better performance than the traditional machine learning models. As the classic deep learning model, deep CNN and ResNet-50 achieved 68% and 71% accuracy, respectively, which are lower than expected. The main reason is that the limited training samples and the negative samples are various, which made the deep-set classifier model cannot learn strong feature representation. The accuracy of PCA+SVM based method is 3% lower than that of the autoencoder & SVM approach. The best performance of the proposed method is predictable, and it is also proven that the deep residual auto-encoder has a great advantage in feature extraction.

4.3.3 Discussion

The proposed method breaks through the limitations of conventional thinking in cybersecurity, and detects network intrusion from the perspective of high-level image semantics, which is an effective supplement to the traditional cybersecurity methods. By comparison with other methods, the experimental results of the proposed approach proves that it can make a better performance.

The difference between deep autoencoder and the deep residual auto-encoder method is mainly as follows. One is that the deep residual autoencoder constructs a short residual connection between input layer and code layer, so the gradient vanishing phenomenon is limited by optimization and can obtain a good training result to improve the image features representation ability. The other is that the decoding

evaluation standard is different. The purpose of autoencoder is to restore image, while the task of proposed deep residual autoencoder is to find the features to identify abnormal images. In addition, the proposed method has strong learning capacity on small samples, which combines the advantages of deep residual network, deep autoencoder and SVM methods, and shows strong ability of feature representation and feature classification. However, when the webpage has picture carousel or color change magic effect, the proposed method might encounter the false negative phenomenon, which needs to be improved in future work.

5. Conclusion

With the increasingly severe situation of cybersecurity, despite the variety of cybersecurity measures and devices, the cybersecurity staff are required to be on duty day and night, which greatly increases the cost of manpower. An unattended system is an urgent demand for the network security staff. This work is committed to address this issue. We analyzed the deep and shallow learning models, and modified the model architecture to achieve the purpose. A deep residual autoencoder based feature extraction method was proposed, combined with the SVM method to detect the invaded webpage images. Experimental results showed that the accuracy of the proposed RAE-SVM method achieves 95%, which meets our satisfaction performance and provides a novel approach for cybersecurity based on machine learning and computer vision.

Conflict of Interest

The authors declare that they have no competing interests.

Funding

None.

References

[1] D. Michie, D. Spiegelhalter, and C. Taylor, *Machine Learning, Neural and Statistical Classification*. Englewood Cliffs, NJ: Prentice Hall, 1994.

[2] Q. He, X. Meng, R. Qu, and R. Xi, “Machine learning-based detection for cyber security attacks on connected and autonomous vehicles,” *Mathematics*, vol. 8, no. 8, article no. 1311, 2020. https://doi.org/10.3390/math8081311

[3] A. N. Jaber and S. U. Rehman, “FCM–SVM based intrusion detection system for cloud computing environment,” *Cluster Computing*, vol. 23, no. 4, pp. 3221-3231, 2020. https://doi.org/10.1007/s10586-020-03082-6

[4] C. Kumar, T. S. Bharati, and S. Prakash, “Online social network security: a comparative review using

machine learning and deep learning," *Neural Processing Letters*, vol. 53, no. 1, pp. 843-861, 2021. https://doi.org/10.1007/s11063-020-10416-3

[5] S. Al-Eidi, O. Darwish, Y. Chen, and G. Husari, "SnapCatch: automatic detection of covert timing channels using image processing and machine learning," *IEEE Access*, vol. 9, pp. 177-191, 2021. https://doi.org/10.1109/ACCESS.2020.3046234

[6] E. Nowroozi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A survey of machine learning techniques in adversarial image forensics," *Computers & Security*, vol. 100, article no. 102092, 2021. https://doi.org/10.1016/j.cose.2020.102092

[7] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "Intrudtree: a machine learning based cyber security intrusion detection model," *Symmetry*, vol. 12, no. 5, article no. 754, 2020. https://doi.org/10.3390/sym12050754

[8] M. Dehghani, A. Kavousi-Fard, M. Dabbaghjamanesh, and O. Avatefipour, "Deep learning based method for false data injection attack detection in AC smart islands," *IET Generation, Transmission & Distribution*, vol. 14, no. 24, pp. 5756-5765, 2020. https://doi.org/10.1049/iet-gtd.2020.0391

[9] F. Y. Yavuz, D. Unal, and E. Gul, "Deep learning for detection of routing attacks in the Internet of Things," *International Journal of Computational Intelligence Systems*, *12*(1), 39-58, 2018. https://doi.org/10.2991/ijcis.2018.25905181

[10] I. Ko, D. Chambers, and E. Barrett, "Feature dynamic deep learning approach for DDoS mitigation within the ISP domain," *International Journal of Information Security*, vol. 19, pp. 53-70, 2020. https://doi.org/10.1007/s10207-019-00453-y

[11] B. Yuan, J. Wang, D. Liu, W. Guo, P. Wu, and X. Bao, "Byte-level malware classification based on Markov images and deep learning," *Computers & Security*, vol. 92, article no. 101740, 2020. https://doi.org/10.1016/j.cose.2020.101740

[12] T. Qi, B. Wang, and S. J. Zhao, "The research of website tamper-resistant technology," *Advanced Materials Research*, vol. 850-851, pp. 475-478, 2014. https://doi.org/10.4028/www.scientific.net/AMR.850-851.475

[13] J. Huo, H. Qu, and L. Liu, "Design and implementation of automatic defensive websites tamper-resistant system," *Journal of Software*, vol. 7, no. 10, pp. 2379-2386, 2012.

[14] S. Dwivedi, M. Vardhan, and S. Tripathi, "Defense against distributed DoS attack detection by using intelligent evolutionary algorithm," *International Journal of Computers and Applications*, vol. 44, no. 3, pp. 219-229, 2022. https://doi.org/10.1080/1206212X.2020.1720951

[15] M. A. Baig, "An analysis of North Korean cyber warfare capabilities and impact on USFK and USINDOPACOM," *Journal of Cyber Security Technology*, vol. 3, no. 4, pp. 219-248, 2019. https://doi.org/10.1080/23742917.2019.1663990

[16] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19-31, 2016. https://doi.org/10.1016/j.jnca.2015.11.016

[17] M. Elhoseny, M. M. Selim, and K. Shankar, "Optimal deep learning based convolution neural network for digital forensics face sketch synthesis in internet of things (IoT)," *International Journal of Machine Learning and Cybernetics*, vol. 12, pp. 3249-3260, 2021. https://doi.org/10.1007/s13042-020-01168-6

[18] X. Guo, A. A. Minai, and L. J. Lu, "Feature selection using multiple auto-encoders," in *Proceedings of 2017 International Joint Conference on Neural Networks (IJCNN)*, Anchorage, AK, USA, 2017, pp. 4602-4609. https://doi.org/10.1109/IJCNN.2017.7966440

[19] J. Masci, U. Meier, D. Cireşan, and J. Schmidhuber, "Stacked convolutional auto-encoders for hierarchical feature extraction," in *Artificial Neural Networks and Machine Learning–ICANN 2011.* Heidelberg, Germany: Springer, 2011, pp. 52-59. https://doi.org/10.1007/978-3-642-21735-7_7

[20] B. M. Aslahi-Shahri, R. Rahmani, M. Chizari, A. Maralani, M. Eslami, M. J. Golkar, and A. Ebrahimi, "A hybrid method consisting of GA and SVM for intrusion detection system," *Neural Computing and*

Applications, vol. 27, pp. 1669-1676, 2016. https://doi.org/10.1007/s00521-015-1964-2

[21] G. Liu, X. Gao, D. You, and N. Zhang, "Prediction of high power laser welding status based on PCA and SVM classification of multiple sensors," *Journal of Intelligent Manufacturing*, vol. 30, pp. 821-832, 2019. https://doi.org/10.1007/s10845-016-1286-y

[22] A. Tellaeche Iglesias, M. A. Campos Anaya, G. Pajares Martinsanz, and I. Pastor-Lopez, "On combining convolutional autoencoders and support vector machines for fault detection in industrial textures," *Sensors*, vol. 21, no. 10, article no. 3339, 2021. https://doi.org/10.3390/s21103339

Changjian Zhou **https://orcid.org/0000-0002-2094-6405**

He received M.S. degree in Harbin Engineering University in 2012, China. Since March 2012, he is as a teacher in Department of Modern Educational Technology from Northeast Agricultural University. His current research interests include artificial intelligence and computer vision.

Yutong Zhang **https://orcid.org/0000-0003-1012-3621**

She is currently pursuing the B.S. degree in college of electrical & information, Northeast Agricultural University. She is also the member of High-Performance Computing and Artificial Intelligence Laboratory. Her research interests include image processing and agricultural artificial intelligence.

Yunfu Liang **https://orcid.org/0000-0003-3414-2886**

He received B.S. degree in Northeast Agricultural University, China. Now he is as the director of Department of Modern Educational Technology, Northeast Agricultural University. His current research interests include cyberspace security and educational informatization.

Jinge Xing **https://orcid.org/0000-0001-8764-0673**

He received B.S. degree in Harbin Engineering University in 1996, China. Now he is as a senior engineer in Northeast Agricultural University. His current research interests include cyberspace security and artificial intelligence.