Classification accuracy of the methods

Non-Sensitive Data	Accuracy	Rand	PCA	PLS	LDA	Proposed Method
		0.6000	0.6150	0.6200	0.6200	**0.6250**
Sensitive Data		0.4700	0.4750	0.4850	0.4850	0.4900

The data in the Table 1 shows that with the application of the method to the data, the algorithm identifies the sensitive data with low accuracy, while it identifies the non-sensitive data with high accuracy.

REFERENCES

1. Ojagveriyeva S.S. Some actual problems of data sanitization// Institute of Information Technology of ANAS, 2019, no 1, pp. 99–108.

2. Anandan B., Clifton Ch., Jiang W., Murugesan M., Pastrana-P.Camacho, Luo Si. t-Plausibility: Generalizing Words to Desensitize Text// TRANSACTIONS ON DATA PRIVACY, 2012, 5, pp.505–534

3. Krizhevsky I.S., G. E. Hinton. Imagenet classification with deep convolutional neural networks//Advances in Neural Information Processing Systems, 2012, pp. 1097–1105.

UDC 004

R. M. Alguliyev, Y. N. Imamverdiyev, L. V. Sukhostat
e-mail: r.alguliev@gmail.com, yadigarimam@gmail.com,
lsuhostat@hotmail.com

Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan

DETECTION OF CYBER-ATTACKS ON CYBER-PHYSICAL SYSTEMS USING DEEP NEURAL NETWORK

This paper proposes and evaluates the application of a deep neural network to detection of cyber-attacks on cyber-physical systems.

Cyber-physical systems (CPSs) consisting of distributed computing elements that interact with physical processes have become ubiquitous in modern life [1-2].

Cyber-physical systems (CPSs) consisting of distributed computing elements that interact with physical processes have become ubiquitous in modern life [1-2]. The rapid growth of CPS applications leads to the necessity of ensuring the information security of such systems.

Cyber-attacks affect the normal functioning of physical processes and may lead to devastating consequences. Therefore, to reduce their impact, it is necessary to analyze and develop approaches to minimize the damage to the CPS.

Deep learning is a state-of-the-art technique of artificial intelligence, consisting of algorithms and solutions that significantly expand the scope and effectiveness of neural networks [3]. A large number of layers allows the neural network to build the concept of the object under study from simple features, gradually moving to more complex ones.

The paper proposes an approach that combines the advantages of GANs (Generative Adversarial Networks) and CNN (Convolutional Neural Network) to detect CPS failures. Due to the imbalance of datasets containing information about the system condition, GAN was applied to improve the accuracy of the CNN model. The proposed approach provides high accuracy of cyber-attacks detection. Testing of CPS is carried out on a dataset that represents the work of a real industrial network to evaluate the machine learning algorithms.

The experiments were conducted on Intel Xeon (R), CPU X5670 @ 2.93GHz * 4 with 10GB of RAM machine. The proposed approach was evaluated in Python 2.7.13 using various libraries, including Tensorflow and Keras.

A large dataset Secure Water Treatment (SWaT) collected at the Singapore University of Technology and Design was considered for the experiments [4]. It contains information about attacks (e.g., attack with the intention of overflowing the tank by shutting pump, attack with the intention to underflow the tank and damage pump, etc.) and the normal operation of the system from 25 sensors and 26 actuators. Recovery from these attacks can take up to several hours, or even damage the system and lead to its failure.

The resulting accuracy and cross-entropy loss depending on the iteration number are shown in the following figure.

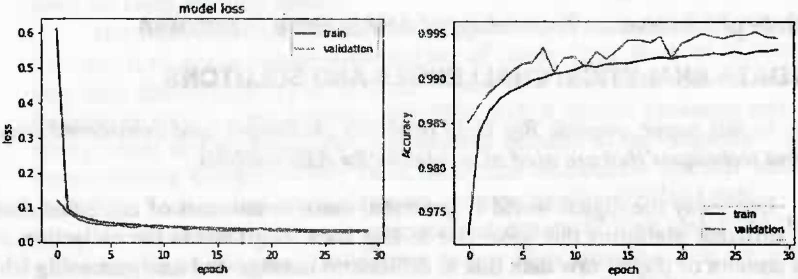

Fig. Dependences of accuracy and cross-entropy loss from iteration number

The proposed approach is compared with logistic regression (LR) and support vector machines (SVM). The results of the experiments according to the precision, recall and F-measure metrics are shown in the table.

Method	Metrics	Class	
		Normal	Attack
LR	Precision	97.09%	27.83%
	Recall	69.91%	84.72%
	F-measure	81.29%	41.89%
SVM	Precision	96.74%	97.86%
	Recall	99.77%	75.45%
	F-measure	98.23%	85.20%
Proposed approach	Precision	98.53%	98.85%
	Recall	99.86%	89.15%
	F-measure	99.19%	93.75%

REFERENCES

1. Zeadally S., Jabeur N. Cyber-physical system design with sensor networking technologies. The Institution of Engineering and Technology. London, UK, 2016, 368 p.

2. Lun Y. Z., D'Innocenzo A., Smarra F., Malavolta I., Di Benedetto M. D. State of the art of cyber-physical systems security: an automatic control perspective // Journal of Systems and Software. 2019. Vol. 149. P. 174–216.

3. Shin J., Baek Y., Lee J., Lee S. Cyber-physical attack detection and recovery based on RNN in automotive brake systems // Preprints. 2018. P. 1-21.

4. Secure Water Treatment (SWaT). URL: http://itrust.sutd.edu.sg/research/testbeds/secure-water-treatment-swat/, acc.: February 2019.

UDC 004.93

M. Sh. Hajirahimova, A. S. Aliyeva

e-mail: aliyeva.a.s@mail.ru

Institute of Information Technology of ANAS, Baku, Azerbaijan

BIG DATA ANALYTICS: CHALLENGES AND SOLUTONS

In this paper, provide Big Data analytics challenges, and considered some current techniques that are used as a solution for data analysis.

Every day the digital world is generated massive amounts of unlabeled data from different platforms that gave rise to Big Data. Big Data is the collection of huge amount of digital raw data that is difficult to manage and analyses using traditional tools. Big Data brings big opportunities and transformative potential for various sectors. On the other hand, it also presents big challenges to harnessing