ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803/tg-20230219213151

Original scientific paper
Received: 2023-02-19, Accepted: 2023-05-26

Design of Efficient Phishing Detection Model using Machine Learning

Bong-Hyun Kim

Abstract: Recently, there have been cases of phishing attempts to steal personal information through fake sites disguised as major sites. Although phishing attacks continue and increase, countermeasures remain in the form of defense after identifying the attack. Therefore, in this paper, we designed a phishing detection model using machine learning that provides knowledge and prediction by learning patterns from data input to a computer. For this, an analysis model was built using sklearn logistic regression, and the phishing probability was visualized using a heatmap. In addition, a graph was used to visually indicate the result, and a function for attribute information of a phishing website was provided.

Keywords: ensemble method; heatmap; machine learning; phishing detection; random forest; sklearn

1 INTRODUCTION

Many victims occur every year as a result of deceiving others over the phone or the Internet, or stealing identity or financial information through phishing, pharming, and smishing. Until recently, there have been cases of phishing attempts to steal personal information through fake sites disguised as major sites. Although phishing attacks continue and increase, countermeasures remain in the form of defense after identifying the attack [1]. A phishing site refers to a malicious web site that requests personal and financial information from users through a web page similar to the real thing and causes various attacks, particularly financial damage. The attacker composes and sends an attack email or message to the user, convincing the user to connect to a spoofed server [2]. If the page displayed by the spoofed server is mistaken for the real server and personal information is entered, the information is delivered to the attacker who manages the spoofed server. Actual phishing attack methods and routes vary by phone call and text message.

In computing, phishing is the act of using e-mail or messenger to deceive by pretending to be a message from a trusted person or company. This deception is a form of social engineering that attempts to fraudulently obtain confidential information such as passwords and credit card information. As reports of phishing incidents increase, methods to prevent phishing are needed. These methods include law, user training, and technical tools. Recently, in addition to phishing using a computer, phishing using a phone is also called voice phishing. There are many different types of phishing.

To prevent and minimize this damage, we are working to eradicate phishing scams worldwide. Korea stipulates punishment for fraud under the "Criminal Act", punishment for telecommunication financial fraud under the "Special Act on Prevention of Damages from Telecommunication Financial Fraud and Refund of Damages", and penalties for falsification and false display of phone numbers under the Telecommunications Business Act. Since 2012, a comprehensive government-wide response system has been prepared and operated [3, 5].

The US federal government has the "Identity Fraud and Impersonation Prevention Act" and the "Identity Fraud Enforcement Punishment Act" to protect personal information. In addition, states such as California, Florida, and Illinois have state-level phishing fraud prevention laws. Currently, the "Fraud and Scam Prevention Act" to protect the elderly who are susceptible to fraud has passed the US House of Representatives and is before the Senate [4].

Similar to Korea's legal system, Japan is governed by the Act on the Prevention of Illegal Use of Mobile Voice Communication Services and Identification of Contractors by Mobile Voice Communication Operators, and the Payment of Damages Recovery Contributions with Funds from Criminal Use Accounts, etc. In addition, phishing fraud prevention policies are being strengthened for the elderly, such as making alert calls to the elderly or subsidizing the purchase cost of a preventive phone equipped with an automatic recording function. In Europe, central banks and payment system operating organizations are publicizing the risk of phishing scams by disclosing information that analyzes payment method fraud data. As the criminal methods and means of phishing scams become more sophisticated and complex, a comprehensive and continuous response is required in the future. In particular, it is necessary to strengthen individual preventive measures for the elderly, who are vulnerable to phishing scams such as the United States and Japan. In addition, telecommunication companies, platform companies, and banks should actively respond to new phishing scams due to technological advancements and changes in communication usage methods [6].

Deep learning achieves higher levels of recognition accuracy than ever before. This accuracy can meet user expectations in consumer electronics and is critical in safety-critical applications such as driverless vehicles. Recently, advances in deep learning have advanced to the level of outperforming humans in some tasks, such as classifying objects in images through deep learning. In this paper, fraud detection and sales prediction were performed using deep learning. To this end, the performance of each model that can be used for data analysis was investigated and a machine learning model suitable for the situation was adopted.

Therefore, in this paper, we designed a phishing detection model using machine learning that provides knowledge and prediction by learning patterns from data input to a computer. For this, an analysis model was built using sklearn logistic regression, and the phishing probability was visualized using a heatmap. In addition, a graph was used

to visually indicate the result, and a function for attribute information of a phishing website was provided.

2 RELATED WORKS

2.1 Phishing

Phishing is an attack method that has been in use since the mid-1990s. It started with a group of young people designing AOL's chat room feature to impersonate an AOL administrator. AOL's 'New Member Chat Room' is designed to provide users with site access assistance. The hackers created valid AOL admin screens like 'BillingAccounting' and alerted users to an account problem. Phishing was created to understand illegal and similar attacks. However, it is currently mainly used in connection with fraudulent activities using e-mail. Also, these illegal phishing scams continue to this day [7, 8].

First, an attack using social engineering is a way to convince users to do something they wouldn't normally do. It is to install a malicious program on a computer using an external device and cause a security problem. Next, an attack using a general e-mail is a method of attacking using a generally frequently used e-mail address [9, 10].

A phishing attack is a set of actions taken by hackers to take advantage of users. Email phishing scams are often easy to spot because of grammatical or misspelling errors in emails, but attackers have become more sophisticated and have evolved to use human emotions, including fear, anger, and curiosity, to entice victims. There are different types of phishing attacks [11, 12]. These include classic email attacks, social media attacks, and attacks with multiple names such as smishing and vishing. Tab. 1 shows definitions of common harmful attack types.

Table 1 Harmful attack type

Type	Concept
Phishing	usually done by e-mail
Spear phishing	segmented e-mail
Whaling	highly targeted emails typically aimed at executives
Internal phishing	Phishing attacks that originate within an organization
Vishing	attack with phone calls
Smishing	done by text message
Social media phishing	attacks using Facebook or other social media posts
Parming	DNS cache corruption

There are several characteristics of phishing. Using email to pretend to be a trusted email address. Most of the phishing emails impersonate the sender. For example, if a scammer deceives into being Citibank, in this case, it is sent randomly by disguising as a normal e-mail address such as "info@citi.com". You will be asked to enter your credit card number or password. This is the ultimate goal of phishing scammers. Never enter such information. Not detected by antivirus software. This is because, in the case of a phishing scam, the URL can be hidden as an HTML mail without any attachments in the form of a simple mail without any features. HTML mail that attacks attachments or vulnerabilities is distinct from phishing. You don't need any special skills other than the skills to create a website. A phishing scam is a way to create websites and send emails. Anyone can make it because the technology is the only technology to create a website. Making it look like a large company site isn't too difficult, as you can pull the HTML source and photos from the actual website.

In the case of existing phishing detection technologies, blacklist-based detection is easy to implement and has a low false positive rate, but there is a limitation in that unknown phishing sites cannot be detected, such as problems that antivirus solutions face. In particular, in the case of Korea, it is difficult to detect phishing sites using blacklists because there is an insufficient system for collecting and sharing blacklists of phishing sites in Korea compared to overseas. In addition, the URL structure analysis technique has a limitation that the detection rate can be greatly reduced even if the attacker changes the URL pattern even slightly.

Various existing phishing-related detection algorithms and studies have been conducted. Phishing detection for mobile browsers, phishing detection using minimum classification error method, and phishing site blocking method using domain characteristics were studied. To detect phishing sites, blacklist-based, HTTP referrer detection, and heuristic-based methods have been studied to detect phishing sites. However, a phishing detection study was conducted using the data analysis and prediction technology in a situation where research was insufficient.

2.2 Machine Learning

Machine learning is one of many subsets of the currently trending technology, artificial intelligence. Instead of explicitly programming computers to learn and improve, the focus is on training computers to learn from data and improve through experience. Machine learning applications improve through application and become more accurate as the data available increases [13].

Machine learning helps businesses by driving growth, unlocking new revenue streams, and solving tough problems. Data is a key driving force behind business decisions, but in the past, businesses have used data from a variety of sources, such as customer feedback, employees, and finance. Machine learning research automates and optimizes this process. Companies can get results faster with software that analyzes very large amounts of data at high speed.

Machine learning and its components deep learning and neural networks are all a detailed subset of AI. AI processes data to make decisions and make predictions. AI not only processes data with machine learning algorithms, but also makes it intelligent as it learns the data without additional programming. Artificial intelligence is a superset that encompasses all machine learning-related subsets. The first subset is machine learning, which has deep learning within it and neural networks within deep learning.

Machine learning and its components deep learning and neural networks are all a detailed subset of AI. AI processes data to make decisions and make predictions. AI not only processes data with machine learning algorithms, but also makes it intelligent as it learns the data without additional

programming. Artificial intelligence is a superset that encompasses all machine learning-related subsets. The first subset is machine learning, which has deep learning within it and neural networks within deep learning [14, 15, 20, 21].

Machine learning consists of several types of machine learning models that apply different algorithmic techniques [22]. Depending on the nature of the data and the desired outcome, one of four learning models can be applied: supervised, unsupervised, semi-supervised, or reinforcement. You can apply one or more algorithmic techniques within each model, depending on the data set being used and the desired results. Machine learning algorithms are primarily designed to classify things, discover patterns, predict outcomes, and make informed decisions [16, 17]. Algorithms can be used one by one, or multiple algorithms can be combined for maximum accuracy when complex and more unpredictable data is involved [18, 19]. Fig. 1 shows the process of how a machine learning process works.

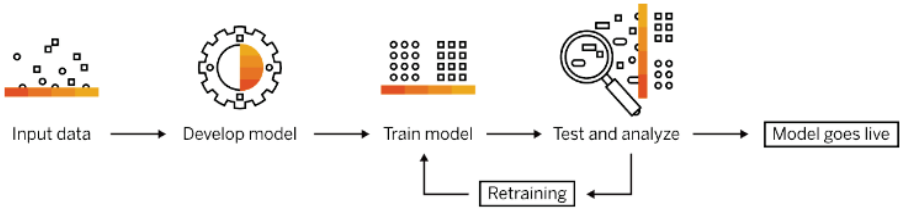

Figure 1 Machine learning process

In this paper, we analyzed the efficiency of phishing detection using deep learning framework and ensemble technique. That is, machine learning classification and regression machine learning models were compared, and through this, which model performed better was evaluated. In conclusion, this paper is a phishing detection study using machine learning that provides knowledge and predictions by learning patterns from data input to a computer. An analytical model is built using logistic regression of sklearn as a research method. A heatmap is used to visualize and indicate the phishing probability. Then, the results are visualized and displayed using graphs.

3 DATA COLLECTION AND TRANSFORMATION

In this paper, using the supply chain data set used by DataCo Global, the region, payment method, and customer where sales fraud was detected were derived. Unlike previous studies, we implemented a methodology to compare machine learning classification and regression machine learning models. In particular, deep learning frameworks Tensorflow and keras were used, and ensemble techniques XGBoost and LightGBM were used. Through this methodology, we analyzed which model performed better and predicted fraud detection and sales.

For data collection and transformation, import pandas, a library that can handle table types often used in data analysis. It also imports numpy, a library that makes mathematical operations easy. Import the matplot library to draw graphs. Finally, we import the seaborn library to visualize the data. Loading data uses the pandas read_csv method to load csv data. The datasets were provided by Kaggle and used.

To improve data utilization, the data were transformed and applied to the study. Converts float64 and int64 data to float32 and int32, respectively, to save memory usage. The final data has 10,000 rows and 50 columns including labels. Fig. 2 shows the final data set after data conversion.

```
float_cols = data.select_dtypes('float64').columns
for c in float_cols:
    data[c] = data[c].astype('float32')

int_cols = data.select_dtypes('int64').columns
for c in int_cols:
    data[c] = data[c].astype('int32')

data.info()
```

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 10000 entries, 0 to 9999
Data columns (total 50 columns):
 #   Column                Non-Null Count  Dtype
---  ------                --------------  -----
 0   id                    10000 non-null  int32
 1   NumDots               10000 non-null  int32
 2   SubdomainLevel        10000 non-null  int32
 3   PathLevel             10000 non-null  int32
 4   UrlLength             10000 non-null  int32
 5   NumDash               10000 non-null  int32
 6   NumDashInHostname     10000 non-null  int32
 7   AtSymbol              10000 non-null  int32
 8   TildeSymbol           10000 non-null  int32
 9   NumUnderscore         10000 non-null  int32
 10  NumPercent            10000 non-null  int32
 11  NumQueryComponents    10000 non-null  int32
 12  NumAmpersand          10000 non-null  int32
 13  NumHash               10000 non-null  int32
 14  NumNumericChars       10000 non-null  int32
 15  NoHttps               10000 non-null  int32
```

Figure 2 Part of the final data set after data transformation

4 ANALYSIS AND PREDICTION

4.1 Data Analysis

In this paper, we designed a phishing detection model using machine learning that provides knowledge and prediction by learning patterns from data input to a computer. For this, an analysis model was built using sklearn logistic regression, and the phishing probability was visualized using a heatmap. In addition, a graph was used to visually indicate the result, and a function for attribute information of a phishing website was provided.

To analyze the data using the final data set, correlations were calculated. For correlation, def.corr() was applied. By analyzing the Spearman correlation, a function with a linear correlation was derived in terms of predicting the phishing classification of a website. Also, the derived results were visualized with a heatmap. Fig. 3 visualizes the results of correlation analysis with corr_heatmap(data, 0, 10).

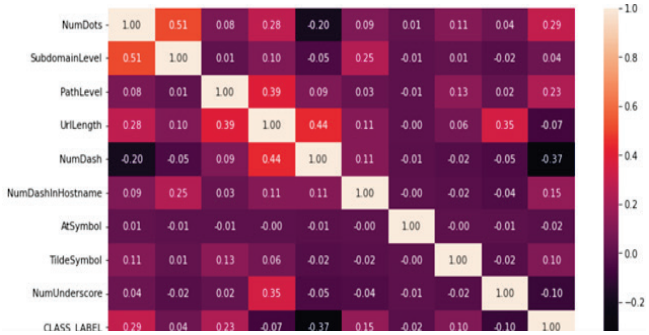

Figure 3 Result of analysis with 'corr_heatmap(data,0,10)' setting

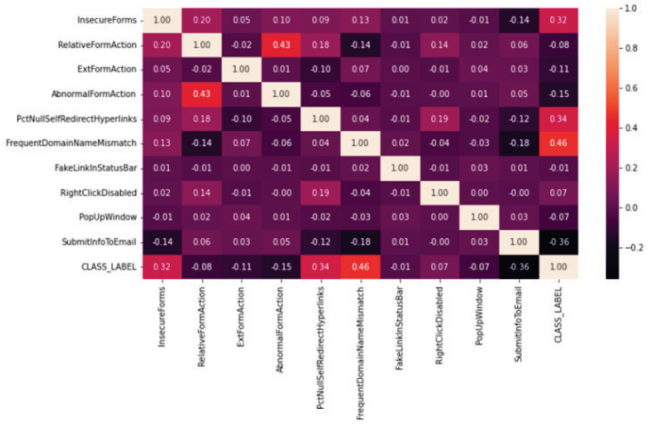

Figure 4 Correlation analysis result according to 'corr_heatmap(data,30,40)' setting

As can be seen from the results, looking at the first 10 columns, we can see that there are no features that have a strong correlation with the label. On the other hand, NumDash has a negative effect on labels, so it can be seen that the lower the number of Dash, the more likely it is a phishing site. In the same way, even under the corr_heatmap (data, 10, 20) and corr_heatmap (data, 20, 30) setting conditions, a strong correlation function was not derived for the label. However, in the analysis set with corr_heatmap(data, 30, 40), it was found that the correlation function of intensity was derived from the label. Fig. 4 is a visualization of the correlation analysis results according to the corr_heatmap (data, 30, 40) setting.

Figure 5 Correlation analysis result according to 'corr_heatmap(data,40,50)' setting

The higher the value of 'InsecureForms', the more likely it is to be a phishing site. 'PctNullSelfRedirectHyperlinks' shows the same positive correlation as 'InsecureForms'. 'SubmitInfoToEmail' is a site that asks users to expose detailed information in their emails, indicating a higher chance of phishing.

In addition, in the result of setting corr_heatmap(data, 40, 50), the phishing probability increases when a 'null self-redirect' hyperlink occurs because it negatively affects the label in the left column 'PctExtNullSelfRedirectHyperlinksRT'. Fig. 5 is a visualization of the correlation analysis results according to the corr_heatmap(data, 40, 50) setting.

```
mi_scores = mutual_info_classif(X, y, discrete_features=discrete_features)
mi_scores = pd.Series(mi_scores, name='MI Scores', index=X.columns)
mi_scores = mi_scores.sort_values(ascending=False)
mi_scores
```

PctExtHyperlinks	4.710189e-01
PctExtResourceUrls	2.902114e-01
PctNullSelfRedirectHyperlinks	2.367851e-01
PctExtNullSelfRedirectHyperlinksRT	2.123850e-01
NumNumericChars	1.326711e-01
FrequentDomainNameMismatch	1.254908e-01
ExtMetaScriptLinkRT	1.175434e-01
NumDash	1.140136e-01
SubmitInfoToEmail	7.802617e-02
NumDots	6.553700e-02
PathLength	6.413269e-02
QueryLength	5.818557e-02
PathLevel	5.543887e-02
InsecureForms	5.508096e-02
UrlLength	5.263855e-02
NumSensitiveWords	4.180522e-02
NumQueryComponents	3.361768e-02
PctExtResourceUrlsRT	2.831059e-02
IframeOrFrame	2.805496e-02
HostnameLength	2.564249e-02

Figure 6 Interdependency measurement results using Mutual Information

In addition, to analyze the information dependence between each other, Mutual Information was applied. Mutual information refers to a method of measuring how interdependent random variables. Find linear and non-linear correlations between labels. Fig. 6 shows the results of measuring interdependence using Mutual Information.

4.2 Data Prediction

In this paper, a phishing detection technique using machine learning that provides knowledge and prediction by learning patterns from data input to a computer by itself was studied. To this end, an analysis model was built using logistic regression of sklearn, and a random forest method was finally applied for data prediction.

First, a line plot graph was used to visualize logistic regression analysis. To do this, import the module that provides evaluation metric calculations from the sklean.metrics package. In addition, a line chart was used to visualize and group data trends. As evaluation indicators, the number of features was visualized as a graph with accuracy, precision, recall, f1_score, and performance evaluation indicators were output. Fig. 7 visualizes logistic regression analysis using a line plot.

Next, a visualization of the performance was performed using a random forest to improve the logistic regression baseline. Random forest is an ensemble method for learning

multiple decision trees. Random forests are being solved for various problems such as detection, classification, and regression. In the final random forest model, 32, the number of features of the model that performed best in all evaluation metrics, were applied. In addition, a final random forest model was trained based on the optimal n features, and used sort values, a method for sorting labels based on values.

```
sns.lineplot(x='num_of_features', y='precision', data=df, label='Precision Score')
sns.lineplot(x='num_of_features', y='recall', data=df, label='Recall Score')
sns.lineplot(x='num_of_features', y='f1_score', data=df, label='F1 Score')
sns.lineplot(x='num_of_features', y='accuracy', data=df, label='Acc Score')
```

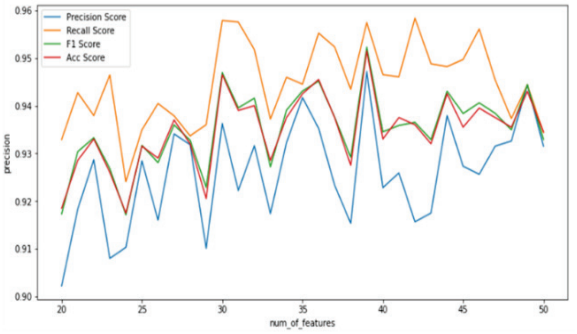

Figure 7 Line plot graph for logistic regression visualization

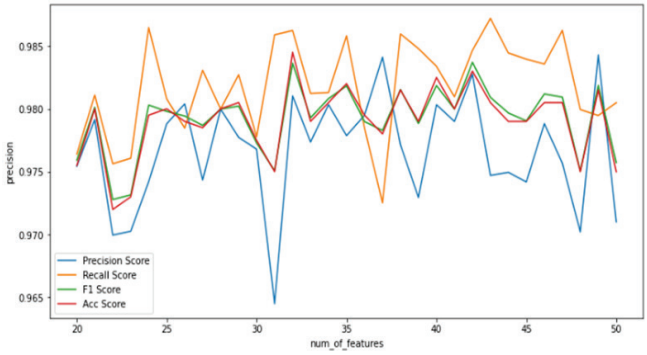

Figure 8 Visualization of performance using random forest

As a final prediction result, accuracy = 0.947162, precision = 0.957468, recall = 0.952287, and f1_score = 0.9515 were derived. Fig. 8 shows the final output of performance visualization using random forest.

5 CONCLUSIONS

Recently, there have been cases of phishing attempts to steal personal information through fake sites disguised as major sites. Although phishing attacks continue and increase, countermeasures remain in the form of defense after identifying the attack. Typically, an attacker composes and sends an attack email or message that induces the user to connect to a spoofed server. If the page displayed by the spoofed server is mistaken for the real server and personal information is entered, the information is delivered to the attacker who manages the spoofed server. Actual phishing attack methods and routes vary by phone call and text message.

Accordingly, a method for effectively preventing phishing is to predict and prevent in advance. To this end, a typical technique used is to design and build a predictive model using machine learning. Machine learning is an effective analysis method suitable for a rapidly changing big data environment with a lot of data related to the problem to be solved.

The phishing detection project using machine learning techniques performed regression analysis using sklearn, a machine learning library. Therefore, in this paper, we constructed a phishing detection model using machine learning that provides knowledge and prediction by learning patterns from data input to a computer. Finally, in the prediction model results, the accuracy was 0.947162, the precision was 0.957468, the recall was 0.952287, and the f1_score was 0.9515, respectively.

Through this study, it can contribute to information protection by efficiently detecting phishing, a type of social engineering. In addition, it does not waste a lot of manpower and time by using machine learning as a security solution to prevent phishing attacks. Sites suspected of being phishing can be detected through the judgment stage and significant damage can be prevented.

6 REFERENCES

[1] Mao, J. Tian, W. Li, P. Wei, T., & Liang, Z. (2017). Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity. *IEEE Access*, 5, 17020-17030. https://doi.org/10.1109/ACCESS.2017.2743528

[2] Agarwal, N., Renfro, S., & Bejar, A. (2007). Phishing Forbidden: Current anti-phishing technologies prevent users from taking the bait. *Queue, 5*(5), 28-32. https://doi.org/10.1145/1281881.1281890

[3] Park, S. H. (2021). A Study on Review of legislation for Voice Phishing public interest Whistleblowers. *Korean Corruption Studies Review, 26*(1), 101-115. https://doi.org/10.52663/kcsr.2021.26.1.101

[4] Purkait, S. (2015). Examining the effectiveness of phishing filters against DNS based phishing attacks. *Information andamp; Computer Security, 23*(3), 333-346. https://doi.org/10.1108/ics-02-2013-0009

[5] Al-Zahrani, A. & Al-Hebbi, M. (2022). Big Data Major Security Issues: Challenges and Defense Strategies. *Technical Journal, 16*(2), 197-204. https://doi.org/10.31803/tg-20220124135330

[6] Jeong E. S. & Lim J. I. (2019). Study on intelligence (AI) detection model about telecommunication finance fraud accident. *Journal of the Korea Institute of Information Security & Cryptology, 29*(1), 149-164. https://doi.org/10.13089/JKIISC.2019.29.1.149

[7] Chen, R., Gaia, J., & Rao, H. Raghav. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision support systems*, 133. https://doi.org/10.1016/j.dss.2020.113287

[8] Saravanan, P. & Subramanian, S. (2020). A Framework for Detecting Phishing Websites using GA based Feature Selection and ARTMAP based Website Classification. *Procedia computer science*, 171, 1083-1092. https://doi.org/10.1016/j.procs.2020.04.116

[9] Tran, M.-H., Yang, H.-G., Dang, T.-B., & Choo, H.-S. (2019). iCaMs: An Intelligent System for Anti Call Phishing and Message Scams. *Proceedings of the Korea Information Processing Society Conference*, 156-159. https://doi.org/10.3745/PKIPS.Y2019M10A.156

[10] Gupta, B. B. & Kumar, J. A. (2020). Phishing Attack Detection using a Search Engine and Heuristics-based Technique.

Journal of Information Technology Research, 13(2), 94-109. https://doi.org/10.4018/jitr.2020040106
[11] Kim, I. S. & Choi, J. M. (2018). Password-Based Mutual Authentication Protocol against Phishing Attacks. *KIPS Transactions on Computer and Communication Systems*, 7(2), 41-48. https://doi.org/10.3745/KTCCS.2018.7.2.41
[12] Kartal, G. (2022). The Effects of Positive and Negative Shocks in Energy Security on Economic Growth: Evidence from Asymmetric Causality Analysis for Turkey. *Economic Computation and Economic Cybernetics Studies and Research, 56*(1), 223-240. https://doi.org/10.24818/18423264/56.1.22.14
[13] Zhao, L. & Zhu, J. (2019). Learning from correlation with extreme learning machine. *International Journal of Machine Learning and Cybernetics, 10*(12), 3635-3645. https://doi.org/10.1007/s13042-019-00949-y
[14] Baik J. W. (2022). Machine learning in survival analysis. *Industry Promotion Research, 7*(1), 1-8. https://doi.org/10.21186/IPR.2022.7.1.001
[15] Kim B. H. (2022). A Study on the Prediction of KRW/USD Exchange Rate against the Number of COVID-19 Confirmed Cases Using LSTM Model. *Journal of Next-generation Convergence Technology Association, 6*(4), 593-598. https://doi.org/10.33097/JNCTA.2022.06.04.593
[16] Zheng, W., Liu, H., Wang, B., & Sun, F. (2020). Cross-modal learning for material perception using deep extreme learning machine. *International Journal of Machine Learning and Cybernetics, 11*(4), 813-823. https://doi.org/10.1007/s13042-019-00962-1
[17] Shellman, M. H. & Shellman, Y. G. (2020). Human against Machine? Machine Learning Identifies MicroRNA Ratios as Biomarkers for Melanoma. *Journal of Investigative Dermatology, 140*(1), 18-20. https://doi.org/10.1016/j.jid.2019.07.688
[18] Özgur, C. & Sarikovanlik, V. (2022). Forecasting BIST100 and NASDAQ Indices with Single and Hybrid Machine Learning Algorithms. *Economic Computation and Economic Cybernetics Studies and Research, 56*(3), 235-250. https://doi.org/10.24818/18423264/56.3.22.15
[19] Trușcă, M. M., Aldea, A., Grădinaru, S. E., & Albu, C. (2021). Post-Processing and Dimensionality Reduction for Extreme Learning Machine in Text Classification. *Economic Computation and Economic Cybernetics Studies and Research, 55*(4), 37-50. https://doi.org/10.24818/18423264/55.4.21.03
[20] Al-Akashi, F. (2021). Learning-to-Rank: A New Web Ranking Algorithm using Artificial Neural Network. *International Journal of Hybrid Information Technologies, 1*(1), 15-32. https://doi.org/10.21742/IJHIT.2021.1.1.02
[21] Al-Akashi, F. (2021). Improving Learning Performance in Neural Networks. *International Journal of Hybrid Innovation Technologies, 1*(2), 27-42. https://doi.org/10.21742/IJHIT.2021.1.2.02
[22] Sharma, S. & Kalra, S. (2016). A Comparative Analysis of Phishing Detection and Prevention Techniques. *International Journal of Grid and Distributed Computing, NADIA, 9*(8), 371-384. https://doi.org/10.14257/ijgdc.2016.9.8.32

Authors' contacts:

Bong-Hyun Kim
School of Software, Major of Computer Engineering,
Seowon University,
377-3 Musimseo-ro, Seowon-gu, Cheongju-si,
Chungcheongbuk-do, 28674, Republic of Korea
bhkim@seowon.ac.kr