Analysis on Phishing Detection Methods

Shisheng Zheng

Faculty of Science and Technology, Beijing Normal-Hong Kong Baptist University,Zhuhai, China

Abstract. With the popularization of the Internet, phishing has become one of the most threatening attacks in the field of network security, and the number of attacks continues to climb, the means are becoming increasingly complex, and it seriously threatens the privacy and property security of users. This paper aims to systematically analyze phishing detection methods to address this challenge and provide support for building a more secure network environment. The research focuses on four mainstream detection methods: list-based methods rely on black-and-white lists to quickly identify known threats, but are slow to react to new attacks; heuristic rule-based methods formulate rules through feature patterns, which have high interpretability but false positives may occur; machine learning based approach adapts to multiple phishing types through data learning, which is flexible but relies on feature engineering; Deep learning based approach uses neural networks to automatically extract complex features, with excellent generalization ability but insufficient interpretability. Future research needs to further promote the integration of technologies, enhance system transparency, develop lightweight models, and solve the problem of data scarcity.

1 Introduction

With the popularization of the Internet and the acceleration of digitization, phishing has become one of the most prevalent and destructive threats in the field of cybersecurity. Phishing lures users into divulging sensitive information, such as login credentials or financial data, by masquerading as a legitimate entity and utilizing email, social media, or fake websites. In the fourth quarter of 2024, the Anti-Phishing Working Group (APWG) observed 989,123 phishing attacks, significantly higher than the 877,536 phishing attacks in the second quarter and 932,923 phishing attacks in the third quarter. At the same time, phishing tactics are becoming increasingly sophisticated and diverse, with emerging attacks including but not limited to Quishing [1], AI-powered phishing [2].

As a result, the widespread and seriousness of phishing can no longer be ignored, and there is an urgent need for an in-depth study of its characteristics and response strategies to support the construction of a more secure network environment. For example, Adewole et al.[3] proposed a phishing URL detection method based on heuristic rules, which generates and optimizes the hybrid rule set through feature extraction, JRip and PART algorithms, and the method is especially outstanding on large-scale datasets; Liu et al.[4] proposed a PhishingIntention detection method, which makes use of the deep visual technology

s230026220@mail.uic.edu.cn

through Faster R-CNN, OCR-aided Siamese model and ResNetV2-50 classifier, combined with webpage screenshots and user interaction behaviors to extract brand intent and credential acquisition intent to accurately detect phishing websites.

This paper first sorts out the current situation and challenges of phishing, then systematically analyzes the advantages and disadvantages of the four types of detection methods, and finally evaluates their actual performance through application scenarios, which provides a reference for the selection of phishing defense technologies and future research.

2 Phishing detection methods

Phishing detection methods mainly include four types: list-based, heuristic rule-based, machine learning and deep learning.

List-based approaches, which utilize blacklists and whitelists to identify known phishing and secure websites, are simple and efficient, but are slow to react to emerging attacks and can bypass detection with simple URL changes, resulting in the need to update the list very frequently to stay current [5], as well as high false positives, which affects the user experience. List-based approaches provide basic protection, but their limitations have prompted research to turn to machine learning and deep learning to deal with increasingly sophisticated phishing techniques [6][7].

Heuristic rule-based detection methods identify phishing websites by dissecting the feature patterns associated with them, and based on known common characteristics of phishing websites, a series of heuristic rules are formulated for identification [8]. It has similar advantages and disadvantages as list-based detection methods.

Machine learning based method is capable of adapting to a wide range of phishing types by learning patterns from URLs, web content, and other features, showing high flexibility and high detection efficiency [9].

In contrast, deep learning based methods utilizes multi-layer neural networks such as convolutional neural networks (CNNs) and long short-term memory networks (LSTMs) to automatically extract complex data features, which is particularly suitable for handling unstructured data in modern phishing attacks, such as complex URL structures and HTML content, showing excellent performance with more superior generalization capabilities [10]. However, due to the complexity of the model, the interpretability is poor.

The purpose of this paper is to systematically analyze the implementation principles, characteristics, and application effects of phishing detection methods, so as to provide reference for technology selection and future research. The logic of this paper will be as follows: systematically discuss these four types of detection methods, sort out the realization principles and characteristics of each type of method, and focus on their advantages and limitations. Finally, through the analysis of application scenarios, the performance and applicability of these methods in actual phishing defense will be evaluated in depth.

3 Application analysis of phishing detection method

3.1 List-based detection methods

List-based detection methods rely on maintaining databases of known phishing sites (blacklists) or known safe sites (whitelists). When a user tries to access a URL, the system checks to see if the URL is on the blacklist or not on the whitelist to determine if it is a phishing site. Blacklists are typically collected through user reports, automated crawlers, or

security organizations such as APWG. Whitelists, on the other hand, are used to protect known safe websites. This method is commonly used to deal with email, and SMS scams.

In fact, this approach is suitable for resource-constrained scenarios, as it does not require specialized technical support or large upfront investment, and its simplicity and ease of use lowers the threshold of use for individual users and small businesses. It is especially friendly to organizations or individuals with limited budgets, performs well in resource-constrained environments, does not rely on high-performance hardware or large amounts of computing resources, and has low deployment and maintenance costs [11]. In addition to this, this approach has a fast response time and short duration of action, thus significantly reducing the time and risk of user exposure to phishing websites, and this immediate response capability is especially important in scenarios that require fast decision making, especially when users browse web pages or click on links. In a study with Google Safe Browsing, PhishTank, and OpenPhish as the main subjects [12], this strategy showed superiority in terms of response time.

Yet, it also reveals a certain degree of sacrifice in accuracy, where automated detection may incorrectly blacklist some non-phishing websites. Such false positives may not only affect the accessibility of legitimate websites and increase the chances of false positives but may also reduce users' trust in blacklists during actual use. In addition to this, the list-based approach requires frequent updates to maintain timeliness; phishing websites may generate a large number of new URLs in a short period of time, and the update speed of the blacklist cannot keep up with it, leading to a decrease in the detection effectiveness. In addition, the update process requires continuous data collection, validation, and distribution, which increases maintenance costs. However, even when combining URL and web content profiling [13], the coverage is still limited and the maintenance workload is high, especially when the number of phishing sites surges [5]. Finally, when confronted with ZERO-DAY ASSAULTS, the detection is unsatisfactory and often unrecognizable.

3.2 Heuristic rule-based detection methods

Heuristic rules refer to a set of simplified judgment criteria or patterns based on experience, statistical laws or expert knowledge, which are used to make decisions or solve problems quickly in complex problems without relying on complex calculations or comprehensive data analysis. In the field of network security, especially in phishing detection, heuristic rules are usually a set of conditional judgment rules developed by analyzing the common features of known phishing websites or emails. These rules are based on common features of phishing websites, such as URL patterns or web content anomalies, to help users quickly identify possible risks.

In 2009, two heuristic rule-based systems were proposed in an early study, where traditional blacklists achieved only 20% recognition accuracy when confronted with brand new phishing sites, but both heuristic rule-based detection rates achieved at least twice the performance compared to blacklists (41% and 70%) [14]. Higher interpretability is another outstanding advantage of this method, as the rules are built based on the experience or experts or authorities, so the decision-making model and judgment basis of the whole system are relatively transparent. Moreover, similar to list-based detection methods, this set of methods is highly advantageous in terms of response speed.

However, precisely because of the principle and mechanism of operation of heuristic rules, and the fact that legitimate websites may also fulfill some of the conditions defined by the rules, it is also possible to some extent that the false positive rate of this method is usually higher than that of the list-based approach. This is the main drawback of this approach.

3.3 Machine Learning based detection methods

Machine Learning in Phishing Detection Identifying threats by learning underlying patterns from data has become an important tool for dealing with sophisticated cyber attacks. The core concept is to utilize algorithms trained on datasets containing features of phishing and legitimate websites, which in turn classify unseen websites [9]. These features usually include URL length, domain age, keyword occurrence frequency, SSL certificate status, and webpage content structure, etc. The process generally includes data collection, feature engineering, modeling, and evaluating the performance [9] In addition, machine learning methods can further enhance the detection of dynamic attacks by analyzing traffic characteristics or user behavior patterns, e.g., combining URL and webpage content feature analysis can effectively identify targeted attacks such as Spear Phishing [15].

The advantages of machine learning methods are significant, starting with their adaptability and ability to learn from new data to cope with evolving phishing techniques, and especially showing high accuracy against unknown attacks. Compared to list-based approaches, machine learning does not rely on known databases but learns generic patterns from training data, thus providing an advantage when facing newly generated phishing sites. Second, since this method detects based on multiple features, it can comprehensively analyze multi-dimensional information such as URLs, web page contents, traffic data, etc., thus improving the recognition ability of complex attacks. For example, the machine learning method can also further improve the performance and reduce the false alarm rate by Adaboost, so that it can perform well in dynamic environments [16].

However, machine learning methods have some limitations. First, feature engineering is its main bottleneck, requiring manual design and selection of features, which is not only time-consuming but also highly dependent on expert knowledge. If the features are not selected properly, it may lead to degradation of model performance. It is susceptible to attacks generated through GANs, leading to perturbations in the order of feature engineering, which ultimately affects the performance accuracy [17]. Second, the high dependence of machine learning on large amounts of labeled data is a significant problem. Training a high-performance model requires a dataset containing sufficient samples of phishing and legitimate websites, and with insufficient or inaccurately labeled data, the model may be over- or under-fitted, affecting detection results. For example, studies using the UCI dataset (more than 11,000 URLs and 30 characteristics.) have found that model performance fluctuates more when the data size is small [18]. In addition, the training and running of machine learning models require more computational resources, especially in dealing with large-scale datasets or real-time detection scenarios, which require higher performance hardware support, which increases the deployment cost [19].

3.4 Deep Learning based detection methods

Deep learning is a machine learning approach based on multi-layer neural networks, which differs from traditional machine learning in that its core feature lies in end-to-end learning via multi-layer neural networks (e.g., convolutional neural networks and long- and short-term memory networks), which automatically extracts hierarchical feature representations directly from the raw data (e.g., URLs, web content, emails, or audio data), and then proceeds to the unseen website or content classification without the manual feature engineering required by traditional machine learning [20]. The advantages of deep learning methods are significant, starting with their automatic feature extraction capability, which can learn hierarchical feature representations from raw data, reducing manual intervention and making them suitable for processing unstructured data. Compared with traditional machine learning methods, deep learning does not need to manually design features, but

automatically captures complex patterns through multi-layer neural networks, and is therefore more advantageous in facing dynamically generated phishing websites. Second, deep learning is able to handle complex patterns and model non-linear relationships in data, which is suitable for the diversity of modern phishing attacks. In addition, deep learning has good scalability, can handle large-scale data, and the performance continues to improve with the increase of data volume, which is suitable for dynamically changing phishing attack scenarios [20]. It is worth mentioning that voice phishing (vishing) has been regarded as a more difficult problem to deal with due to the unstructured nature of its data, which increases the difficulty of feature extraction. However, with the introduction of deep learning methods, which take advantage of capturing the temporal structure and high-dimensional features of speech signals and omitting feature engineering, it has a better performance in the field of voice phishing.

However deep learning methods still have problems. For example, poor interpretability: on the one hand, due to the black-box nature of the model itself, decision-making information and operations are opaque, and the problem of superimposing high-dimensional parameters and thus increasing the difficulty of feature extraction leads to questionable model trust. Second, similar to machine learning, training deep learning models involves a large amount of computational resources and a long iteration cycle, thus limiting deployment on mobile devices and increasing hardware requirements in real-world applications.

4 Application Scenario

In practice, there is often a deep fusion of various detection methods.

Since list-based detection methods are mainly fused with other detection methods for detection. Therefore Azeez et al. [11] proposed a detection system that fuses traditional whitelist detection methods and visual similarity of pages, aiming at efficiently detecting phishing websites and reducing manual maintenance costs. The model architecture of the system is modular: first, the URL and DNS matching module maintains a whitelist of domain names and IP addresses of legitimate websites, after the user inputs a URL, the system checks whether it matches or not, if it matches, it is determined to be a legitimate website, otherwise it is passed on to the next module; the module is used for phishing detection algorithms by analyzing the characteristics of the web page's hyperlinks: first, it extracts all the <a& gt; tags (i.e., href attribute) in the HTML of the web page to obtain a collection of hyperlinks; secondly, if the web page has no hyperlinks (the number of 0), it is directly determined as a phishing website, because legitimate websites usually contain functional links; thirdly, it is to detect the null-pointer hyperlinks (e.g., <a href="#">), and if it exists, it will be labeled as a suspicious one, because the attackers often use this as a way of disguising the functional links; fourthly, it is to calculate the proportion of hyperlinks in external domains. Proportion of hyperlinks to external domains If the percentage of hyperlinks to external domains exceeds the threshold, it is recognized as a phishing website, because legitimate websites mostly point to their own domains while phishing websites often point to external domains. The algorithm realizes efficient detection through simple features. The algorithm determines whether a URL is a phishing website, and enters the update process if it is a legitimate website, and issues a warning if it is a phishing website; finally, the whitelist update module automatically adds the newly recognized legitimate websites to the whitelist to ensure system adaptability. This modularized design realizes the complete process from rapid initial screening to in-depth detection to dynamic updating, which is highly practical. The experimental validation is based on PhishTank (phishing websites) and Alexa (legitimate websites) datasets, with an initial test of 200 websites (140 phishing, 60 legitimate), which is expanded to 800 websites

to evaluate scalability. The results show an average accuracy of 95.17% and a TPR of 95.0%. It shows that the method can effectively recognize phishing websites with low false positive rate. It demonstrates its superiority.

Adewole et al. [3] proposed a heuristic rule-based phishing URL detection method, which demonstrates its application value in the field of network security by designing a hybrid rule model that combines feature extraction, rule generation, rule optimization and detection modules. The method firstly selects 30 key features based on domain knowledge and heuristic intuition through the feature extraction module, which are designed for the abnormal behavioral patterns of phishing URLs to ensure that the subsequent rule generation is targeted, and these features will also be used as the basis for the generation of subsequent rules. Next, the rule generation module utilizes the JRip (Repeated Incremental Pruning to Produce Error Reduction) and PART (Projective Adaptive Resonance Theory) algorithms to automatically generalize IF-THEN rules from the training data. For example, JRip generates concise rules that capture typical patterns of phishing URLs. While PART generates more detailed rules to improve the accuracy and interpretability of the rules. Subsequently, the hybrid model module fuses the rule sets of both and optimizes the rule sets through heuristic strategies such as de-weighting to improve the detection efficiency and generalization ability. Finally, the detection module for the new input URL, the system first extracts its features, and then applies the optimized hybrid rule set to match it to quickly determine whether it is a phishing link or not to achieve real-time detection. Experimental results show that the method shows higher accuracy than JRip and PART alone on both datasets. The method ensures rule relevance through feature selection and utilizes a data-driven rule generation and optimization strategy, which excels in both accuracy and generalization ability, with obvious advantages especially on large-scale datasets.

Research on machine learning detection often involves taking the CLASSIFIER as the object of study, the CLASSIFIER as a key pre-step in the subsequent development of machine learning, the selection of the CLASSIFIER in the model, often directly affects the accuracy of the subsequent measurements and the performance of the actual processing problem. While feature selection reduces noise and redundant features and enhances the generalization ability.Alazaidah et al.[21] explored the performance of multiple classifiers and feature selection methods. The paper evaluated a total of 24 different classifiers in six categories and compared four feature selection methods. Two fishing-related datasets (binary classification dataset and multiclass dataset) with different characteristics are used to analyze the performance of the classifiers and feature selection methods in different scenarios to enhance the generalizability of the methods, and then eight evaluation metrics are used to comprehensively measure the model performance. The final results show that FilteredClassifier and J48 perform well for large data volume and binary feature dataset, which is suitable for training simpler scenarios. For small data volume, multi-class labeled datasets (e.g., Dataset2), RandomForest is more suitable for handling complex datasets. The classification performance after feature selection is significantly improved, where InfoGainAttributeEval is recommended as the preferred method for phishing website detection.

Liu et al. [4] proposed a detection method called PhishingIntention, where the system architecture is based on deep vision techniques to extract the Brand Intention and Credential-Taking Intention of web pages, aiming at combining the static appearance (screenshots) and the dynamic behavior (user interactions) of web pages to infer its phishing intention and realize accurate detection by combining the static appearance (screenshots) and dynamic behavior (user interaction) of the webpage. The method can be divided into the following four main steps: First, using Faster R-CNN, important UI components are extracted from webpage screenshots, and each component is compressed

into a vector containing location information and type to form an Abstract Webpage Layout (AWL). II: Next, to recognize the brand intent represented by the webpage through the logo, we propose an OCR-aided Siamese model, combining the appearance features and text shape features, and generating the logo embedding vector through a fully connected network by splicing the extracted features, and using cosine similarity to compare the similarity between the logo to be detected and the reference brand logo. III: Designing a vision-based CRP classifier with a mixture of webpage screenshots and AWL as input. The AWL is encoded into multiple channels (one channel for each UI type), stacked with the RGB image channels and fed into the ResNetV2-50 model for classification. Score-CAM technique is used to generate a heat map that interprets the region of credential acquisition intent and determines whether the web page requires the user to enter credentials. IV: If judged not to be a CRP, the credential acquisition intent is confirmed by detecting buttons or links that may be linked to the CRP through a hybrid approach of HTML heuristic rules and visual detection. Ultimately, if the web page is recognized as a CRP and its domain name does not match the legitimate domain name of the matching brand, it is judged to be a phishing website. If the webpage is not a CRP, it is analyzed dynamically to find potential CRPs, and if it is found and the domain name does not match, it is determined to be a phishing website. The robustness of the method is significant, with a false alarm rate of only 5.10%, which is much lower than the baseline (45.5%-60.1%). The recall of the method reaches 0.9, which is significantly better than the baseline method.

5 Discussion

The concept of phishing attacks has not yet been popularized among most Internet users, resulting in many users not being sufficiently alert to phishing attacks [22], and lacking the awareness to combat or defuse the attacks. At the level of data acquisition, outside the English-speaking world, phishing detection may be limited by the spread of the language and the number of users, resulting in a lack of sufficient data to build, optimize, or iterate the detection model (e.g., machine learning model), e.g., Lee et al. mentioned that due to the lack of Korean data on voice phishing, the model's performance in cross-language scenarios is degraded [23]. In addition, many data are sensitive (e.g., the contents of internal emails of employees in an organization), and the protection of data varies from region to region, with some regions having a high degree of protection of private data. In short, for various reasons, some data are difficult to obtain, leading to a lack of corresponding data, which makes the problem of obtaining data for specific scenarios even more problematic.

It is difficult for a single detection method to cope with rapidly evolving phishing attacks. In the future, a hybrid model needs to be formed through technology fusion, combining the advantages of each method to enhance the overall protection capability. For example, list-based detection can be used as the first line of defense to quickly filter known threats; heuristic rules can be used as an early warning to identify zero-day attacks; machine learning and deep learning enhance the adaptability to new attacks through dynamic feature extraction and real-time learning.Safi et al.[4] proposed a hybrid approach that combines heuristic rules with machine learning by first filtering the apparent phishing sites using rules, and then entering the remaining URLs into the model. phishing websites, and then input the remaining URLs into the model, and finally excel the performance of baseline approaches. Recently with the rise of the concept of transfer learning [24], the problem of data volume has been alleviated to a certain extent by migrating from high-resource language models to low-resource language, The future direction of phishing detection enhancement is to improve the detection of phishing attacks, and to improve the performance of phishing attacks. The future direction of phishing detection enhancement is

to improve the transparency of the detection system, to help users understand the risk, and ultimately to improve the user's ability to recognize. Develop lightweight models to reduce computational requirements and adapt to resource-constrained scenarios. For example, Wei et al. [25] proposed a light-weight detection method that can not only run in resource-constrained scenarios but also shorten the runtime by 30%

6 Conclusion

This paper systematically analyzes four major methods for phishing detection - list-based, heuristic rule-based, machine learning and deep learning - and thoroughly discusses the implementation principles and characteristics of each type of method and its performance in practical applications. It is shown that each method has unique advantages in dealing with phishing threats, but also has certain limitations. This paper further evaluates the performance of these methods in practical phishing defense. List and heuristic rule-based methods are suitable as initial screening means to quickly filter known threats, while machine learning and deep learning are more suitable for dynamic environments and can adapt to emerging attack patterns through continuous learning. In practice, it is difficult for a single method to comprehensively cope with the rapidly evolving phishing attacks, and technology convergence has become an important direction to improve the detection effect. Phishing detection research needs to continue to deepen in the following directions: first, to promote technology convergence, build hybrid models to integrate the advantages of various methods to form a multi-level defense system; second, to improve the transparency and interpretability of the detection system, to help users understand the risks and enhance security awareness; third, to develop lightweight models to reduce computational requirements. And ultimately provide strong support for building a more secure network environment.

References

1. Blancaflor, E., Calida, M. B., Chan, M., et al.: 'Impact Analysis and Attack Simulation on Quishing (a QC Code Phishing) using QRLJacker', Proc. 2024 Int. Conf. Electrical, Computer and Energy Technologies (ICECET), July 2024, pp. 1–5, (IEEE)
2. Lamina, O. A., Ayuba, W. A., Adebiyi, O. E., et al.: 'AI-Powered Phishing Detection and Prevention', Path of Science, 2024, 10, (12), pp. 4001–4010
3. Adewole, K. S., Akintola, A. G., Salihu, S. A., et al.: 'Hybrid Rule-Based Model for Phishing URLs Detection', in Emerging Technologies in Computing: Second International Conference, iCETiC 2019, London, UK, August 2019, pp. 119–135, (Springer International Publishing)
4. Liu, R., Lin, Y., Yang, X., et al.: 'Inferring Phishing Intention via Webpage Appearance and Dynamics: A Deep Vision Based Approach', Proc. 31st USENIX Security Symposium (USENIX Security 22), August 2022, pp. 1633–1650
5. Yang, L., Zhang, J., Wang, X., et al.: 'An Improved ELM-Based and Data Preprocessing Integrated Approach for Phishing Detection Considering Comprehensive Features', Expert Systems with Applications, 2021, 165, pp. 113863
6. Safi, A., Singh, S.: 'A Systematic Literature Review on Phishing Website Detection Techniques', Journal of King Saud University-Computer and Information Sciences, 2023, 35, (2), pp. 590–611
7. Barraclough, P. A., Fehringer, G., Woodward, J.: 'Intelligent Cyber-Phishing Detection for Online', Computers & Security, 2021, 104, pp. 102123

8. Rao, R. S., Ali, S. T.: 'Phishshield: A Desktop Application to Detect Phishing Webpages through Heuristic Approach', Procedia Computer Science, 2015, 54, pp. 147–156
9. Basit, A., Zafar, M., Liu, X., et al.: 'A Comprehensive Survey of AI-Enabled Phishing Attacks Detection Techniques', Telecommunication Systems, 2021, 76, pp. 139–154
10. Tang, L., Mahmoud, Q. H.: 'A Survey of Machine Learning-Based Solutions for Phishing Website Detection', Machine Learning and Knowledge Extraction, 2021, 3, (3), pp. 672–694
11. Azeez, N. A., Misra, S., Margaret, I. A., et al.: 'Adopting Automated Whitelist Approach for Detecting Phishing Attacks', Computers & Security, 2021, 108, pp. 102328
12. Bell, S., Komisarczuk, P.: 'An Analysis of Phishing Blacklists: Google Safe Browsing, Openphish, and Phishtank', Proc. Australasian Computer Science Week Multiconference, February 2020, pp. 1–11
13. Aljofey, A., Jiang, Q., Rasool, A., et al.: 'An Effective Detection Approach for Phishing Websites using URL and HTML Features', Scientific Reports, 2022, 12, (1), pp. 8842
14. Sheng, S., Wardman, B., Warner, G., et al.: 'An Empirical Analysis of Phishing Blacklists', 2009
15. Samad, D., Gani, G. A.: 'Analyzing and Predicting Spear-Phishing using Machine Learning Methods', Multidiszciplináris Tudományok, 2020, 10, (4), pp. 262–273
16. Ramanathan, V., Wechsler, H.: 'phishGILLNET—Phishing Detection Methodology using Probabilistic Latent Semantic Analysis, AdaBoost, and Co-Training', EURASIP Journal on Information Security, 2012, 2012, pp. 1–22
17. Valentim, R., Drago, I., Trevisan, M., et al.: 'Augmenting Phishing Squatting Detection with GANs', Proc. CoNEXT Student Workshop, Virtual Event, December 2021, pp. 3–4
18. Alnemari, S., Alshammari, M.: 'Detecting Phishing Domains using Machine Learning', Applied Sciences, 2023, 13, (8), pp. 4649
19. Varshney, G., Misra, M., Atrey, P. K.: 'A Survey and Classification of Web Phishing Detection Schemes', Security and Communication Networks, 2016, 9, (18), pp. 6266–6284
20. Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., et al.: 'A Deep Learning-Based Phishing Detection System using CNN, LSTM, and LSTM-CNN', Electronics, 2023, 12, (1), pp. 232
21. Alazaidah, R., Al-Shaikh, A., Al-Mousa, M. R., et al.: 'Website Phishing Detection using Machine Learning Techniques', Journal of Statistics Applications & Probability, 2024, 13, (1)
22. Singh, K., Aggarwal, P., Rajivan, P., et al.: 'Cognitive Elements of Learning and Discriminability in Anti-Phishing Training', Computers & Security, 2023, 127, pp. 103105
23. Lee, M., Park, E.: 'Real-Time Korean Voice Phishing Detection Based on Machine Learning Approaches', Journal of Ambient Intelligence and Humanized Computing, 2023, 14, (7), pp. 8173–8184
24. Torrey, L., Shavlik, J.: 'Transfer Learning', in Handbook of Research on Machine Learning Applications and Trends: Algorithms, Methods, and Techniques, 2010, pp. 242–264, (IGI Global)

25. Wei, B., Hamad, R. A., Yang, L., et al.: 'A Deep-Learning-Driven Light-Weight Phishing Detection Sensor', Sensors, 2019, 19, (19), pp. 4258