# Muhamad_Hasbia_jiko2-1746516972589

*by* Turnitin ™


**Submission date:** 06-May-2025 02:37AM (UTC-0500)

**Submission ID:** 2667946101

**File name:** Muhamad_Hasbia_jiko2-1746516972589.docx (184.64K)

**Word count:** 4127

**Character count:** 23524

JIKO (Journal of Informatics and Computers) Accredited KEMENDIKBUD RISTEK, No.105/E/KPT/2022
Vol. x, No. x, April 2024, pp. x-x p-ISSN: 2614-8897
DOI: 10.33387/jiko e-ISSN: 2656-1948

# Combination of Multi-View Learning and Deep Reinforcement Learning to Improve Website Phishing Detection

**Muhamad Hasbia1, Vienna Witanti2, Gunawan Abdillah[3]**

1.2Informatics, Faculty of Science and Informatics, Jendral Achmad Yani University, Indonesia

Email: 1mhasbia21@if.unjani.ac.id, 2witanti@gmail.com, [3]Gunawanabdillah03@gmail.com

(Received: dd mmm yyyy, Revised: dd mmm yyyy, Accepted: dd mmm yyyy)

**Abstract**

Phishing is one of the most common and dangerous forms of cyberattacks, where attackers attempt to obtain sensitive information by impersonating trusted entities. Traditional detection methods, such as blacklist-based and signature-based detection, often fail to anticipate new attacks due to the dynamic and evolving nature of phishing. This research aims to develop an adaptive phishing detection system by combining Multi-Kernel Learning (MKL) and Deep Q-Network (DQN). MKL is utilized to integrate multiple feature sources from URL structure, domain metadata, and webpage content into a rich multi-kernel representation, while DQN is employed to enhance the model's adaptability through a reward-based learning mechanism. The dataset used consists of 11,056 entries with 32 relevant features, split with an 80:20 ratio for training and testing. Evaluation results show that the developed system achieved an accuracy of 96.34%, a precision of 95.8%, a recall of 97.85%, an F1-score of 96.73%, and an Area Under Curve (AUC) of 0.98. With these high and balanced metric values, the model demonstrates superior performance in detecting phishing websites compared to conventional approaches. The combination of MKL and DQN has proven effective in producing a phishing detection system that is not only accurate but also adaptive to evolving attack patterns. These findings reinforce the potential application of reinforcement learning-based machine learning in strengthening cybersecurity systems in the digital era.

**Keywords**: *Multi-Kernel Learning, Deep Q-Network, Phishing Detection, Cybersecurity*.



**Corresponding Author: Author1*

## 1. INTRODUCTION

In the last two decades, the development of information and communication technology has transformed various aspects of human life, from communication, financial transactions, to personal data management. The Internet is the main infrastructure for global social and economic activities. However, this progress has also been accompanied by an increase in cybersecurity threats, with phishing being one of the most commonly used attack methods.

Phishing is a social engineering technique that tricks victims into revealing sensitive information through media such as emails, fake websites, or instant messaging. Based on a report by the Anti-Phishing Working Group (APWG), more than 1.3 million phishing incidents were recorded in the first quarter of 2023 [1], showing a drastic increase in the frequency and complexity of these attacks. Phishing remains popular because of its low cost, ease of implementation, and relatively high success rate in exploiting victims.

Traditional phishing mitigation efforts, such as the use of blacklists and signature-based detection methods, face significant limitations. Blacklists are only effective for domains or addresses that are already registered, so they fail to deal with new phishing sites that pop up dynamically [2]. Signature-based detection also has the drawback of dealing with new variants of attacks that modify the structure of content without changing its malicious function. The reliance on this reactive method increases the risk of delays in detecting new threats.

As the volume and variety of phishing attacks increase, machine learning (ML) and deep learning (DL) approaches are becoming widely adopted to automatically detect phishing. ML and DL allow systems to learn from historical datasets and recognize phishing attack patterns without the need for explicit rule programming [3]. This suggests that the use of Multi-Kernel Learning (MKL) in detecting phishing can improve model performance by combining feature representations from different aspects of the website.

The Multi-View Learning (MVL) approach itself offers increased accuracy by utilizing various sources of information, such as URL structure, domain metadata, and web page content [4]. Each view makes a different contribution in distinguishing a phishing site from a legitimate site, enriching the model's predictive capacity [5].

Most of the research related to phishing detection still operates within a static learning paradigm. The model is trained on specific datasets and does not perform adaptive learning after deployment, which means its performance can degrade when faced with new attack patterns. To overcome these limitations, Deep Reinforcement Learning (DRL)-based approaches are beginning to be explored. Ridho, et al. (2024) show that Deep Q-Network (DQN), one of the DRL algorithms, is able to increase the model's resilience to environmental changes because of its reward-based learning nature that is continuously updated based on experience [6].

Meanwhile, the research of Al Ghifari, et al. (2022) reinforces the importance of utilizing URL features in ML-based phishing detection, which remains relevant even though phishing attacks have evolved techniques [7]. By combining the advantages of multi-view representation from MKL and adaptive learning from DQN, it is expected to address the dynamic and diverse challenges of modern phishing detection.

Based on this background, this study aims to develop an adaptive phishing detection system based on a combination of Multi-Kernel Learning (MKL) and Deep Q-Network (DQN). MKL will be used to integrate multiview information from URLs, metadata, and page content into a more comprehensive representation of features. Furthermore, DQN will be used to improve the system's adaptability to changes in phishing attack patterns through reinforcement learning strategies. With this approach, it is hoped that the phishing detection system can achieve a high level of accuracy, increase adaptability to new threats, and significantly reduce false positives and false negatives.

This research also contributes to developing an adaptive phishing detection system based on a combination of Multi-Kernel Learning (MKL) and Deep Q-Network (DQN) that is able to improve the accuracy, resilience, and generalization capabilities of the model against a variety of dynamic phishing attack techniques.

## 2. RESEARCH METHOD.

This research is an applied research that aims to develop and implement practical solutions in detecting phishing sites adaptively. This approach is focused on applying the concept of Multi-View Learning with Multi-Kernel Learning (MKL) and Deep Reinforcement Learning through Deep Q-Network (DQN) to build a more accurate and responsive phishing detection system to new attack patterns.

This study also uses quantitative experimental methods to evaluate the effectiveness of the developed system. The model was evaluated based on a series of quantitative metrics, such as accuracy, precision, recall, F1-score, and AUC, which were measured on a separate test dataset. The test was conducted to assess how well the combination of MKL and DQN was able to improve the performance of phishing detection compared to traditional approaches.

The research process involves the main stages in the form of data collection, preprocessing, model development, model training and testing, and analysis of results using statistical methods based on classification evaluation.

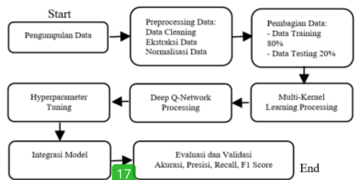



Figure 1. Research Flow

### 2.1 Data Collection

The datasets used in this study are from reliable sources, including PhishTank, OpenPhish, and previous validated research. The dataset consists of 11,055 entries, each with 32 features that represent the characteristics of the website, such as URL length, HTTPS usage, number of specific symbols, the presence of IP addresses in the URL, the age of the domain, and the elements of the page's content. The target label for each entry is 1 for legitimate sites and -1 for phishing sites.

### 2.2 Preprocessing Data

The preprocessing stage is carried out to ensure the quality and consistency of the data before it is used in the training of the model [8]. This process begins with data cleanup, which is removing duplicate entries and fixing incomplete data to maintain the integrity of the dataset. Furthermore, missing values are handled by filling in blank values using mean for numerical features and modes (modes) for categorical features. After that, data normalization is carried out by applying the Min-Max Scaling technique to reduce all numerical features into a range [1], thus preventing the dominance of certain features in the learning process. Categorical features that are still in the form of text are converted into numerical formats through the encoding process so that they can be processed by machine learning algorithms. Finally, the dataset is divided into two parts with an 80:20 ratio, where 80% of the data is used for the model training process and the remaining 20% is used for testing to evaluate the performance of the model's generalization against previously unseen data.

### 2.3 Multi-View Feature Extraction

In this study, the Multi-View Learning (MVL) approach was used to optimize the use of various information sources available on phishing and legitimate websites. The feature extraction process is divided into three main views, each of which represents a different aspect of the data. The first view includes features related to URL structure, such as URL length, unusual character count, use of the HTTPS protocol, and other attributes that could potentially indicate a phishing site. The second view focuses on domain metadata, including the age of the domain, the existence of the SSL certificate, and information related to the domain registrar, which is an important indicator in assessing the authenticity of a site. Meanwhile, the third view analyzes the content of a web page, such as the number of input forms, the presence of hidden scripts, and other characteristics of HTML elements that are often manipulated in phishing attacks. Each view is treated as a representation of features that are independent to maintain the richness of the information of each source. These three views are then integrated using the Multi-Kernel Learning (MKL) method, which allows the merging of various kernels to produce richer and more complex feature representations, to improve the accuracy of phishing classifications.

### 2.4 Implementation of Multi-Kernel Learning (MKL)

At this stage, each view resulting from the feature extraction process is formulated into a different kernel to capture the unique characteristics of each information source. URL structure features are processed using the linear kernel, domain metadata using the Radial Base Function (RBF) kernel, and web page content using the kernel's polynomials. These three kernels are then combined with adaptive weights through convex optimization methods to form a more representative combination of "K" ("x," "x"^"'") kernels[9]. The implementation of MKL aims to enrich the feature space, allowing the system to more effectively recognize complex phishing patterns and improve classification accuracy.

### 2.5 Implementation of Deep Q-Network (DQN)

The output of the Multi-Kernel Learning (MKL) process is used as the input state for the Deep Q-Network (DQN) model [10]. The DQN architecture consists of one input layer with 32 neurons, two hidden layers containing 64 and 32 neurons respectively with the ReLU activation function, and one output layer with 2 neurons representing phishing and legitimate classes. The model is trained using the Q-Learning algorithm, where positive rewards are given for correct predictions and penalties for incorrect predictions. To optimize the learning process, the epsilon-greedy strategy is used to maintain a balance between the exploration of new actions and the exploitation of actions that have been proven to be effective.

### 2.6 MKL-DQN System Integration

After the Multi-Kernel Learning (MKL) process generates a representation of multi-kernel features, the data is directly used as input for Deep Q-Network (DQN) model training. This integration combines the advantages of MKL's rich multi-view feature representation with DQN's reinforcement learning-based adaptive learning capabilities. Through this combination, the developed phishing detection system becomes more responsive to variations in attack patterns and is able to achieve higher accuracy than traditional phishing detection approaches.

### 2.7 Performance Evaluation

The evaluation of model performance was carried out using several standard measurement metrics, namely accuracy, precision, recall, F1-score, and Area Under Curve (AUC) [11]. Accuracy measures the overall percentage of a prediction that is correct, while precision evaluates the accuracy of a prediction against a phishing site. Recall measures the model's ability to capture all existing phishing cases, and F1-score is used to balance precision and recall, especially on unbalanced datasets. AUC is used to assess the model's ability to distinguish between phishing and legitimate classes across various prediction thresholds. This evaluation is carried out on test data that is not used in the training process, to ensure that the model is able to generalize well to the new data.

## 3. RESULT AND DISCUSSION

The results of the research are based on a logical sequence to form a story. The contents show facts/data. Can use Tables and Numbers but do not repeat the same data in pictures, tables, and text. To further clarify the description, can use subtitles.

Discussion is the basic explanation, relationship, and generalization shown by the results. The description answers a research question. If there are any dubious results then show them objectively.

### 3.1 System Implementation

The implementation of the phishing detection system is carried out using the Python programming language, with the support of various libraries such as Pandas and NumPy for data manipulation, as well as Scikit-learn for feature extraction and kernel creation processes. The process of forming the Multi-Kernel Learning (MKL) kernel is carried out separately before the combination is carried out. The Deep Q-Network (DQN) model was built using the TensorFlow and Keras frameworks, while the visualization of the results was done using Matplotlib and Seaborn.

The architecture of the DQN model consists of one input layer with 32 neurons (number of features), two hidden layers with 64 and 32 neurons each using the ReLU activation function, and one output layer with 2 neurons representing two classes (phishing and legitimate). The model training was conducted over 100 epoches with a batch size of 32, using an epsilon-greedy exploration strategy to maintain a balance between exploration and exploitation in learning. The dataset used totaled 11,055 entries with 32 features, labeled with 1 for legitimate websites and -1 for phishing websites.

### 3.2 Experimental results

Experiments were conducted to test the effectiveness of the combination of Multi-Kernel Learning (MKL) and Deep Q-Network (DQN) in detecting phishing sites. The process begins with data preprocessing, including cleaning duplicate entries, handling missing values, and normalizing features using the Min-Max Scaling method. This is important to ensure that each feature is on a uniform scale so as to speed up and stabilize the learning process.

The dataset totals 11,055 entries with a balanced class distribution between phishing and legitimate sites, which is divided into 80% training data and 20% test data. This division is done to avoid overfitting and ensure the model's generalization ability to new data.

After preprocessing, features are extracted using three different kernels: a linear kernel for URL structures, an RBF kernel for domain metadata, and a polynomial kernel for web page content. The three kernels are combined using the convex optimization method in MKL, resulting in a richer representation of features for the classification process.

Furthermore, this combined feature is used as an input for the DQN model. DQN was trained for 100 epochs using the epsilon-greedy strategy to maintain a balance between the exploration of new patterns and the exploitation of the learned patterns. A consistent decrease in the value of training loss during the training process indicates that the model successfully learns and improves its predictions over time.

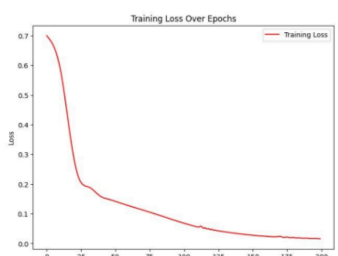
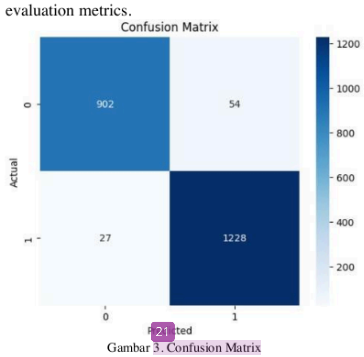



Figure 2. Training Loss Chart per Epoch

Figure 2 shows a graph of the loss of the number of epochs. It can be seen that the value of the loss decreases gradually, although there are normal small fluctuations in the reinforcement learning-based training process. The stability of this loss reduction indicates that the model does not experience early overfitting and that learning takes place effectively.

After the training is completed, performance evaluation is performed on the test data using a confusion matrix and the calculation of various key evaluation metrics.




Gambar 3. Confusion Matrix

Based on Figure 3 Confusion matrix, the model's prediction results on the test data shows the number of true and false predictions for each class of phishing and legitimate sites. The confusion matrix shows that the model managed to correctly classify 902 legitimate sites (True Negative) and 1228 phishing sites correctly (True Positive). In addition, there were 54 cases where legitimate sites were misclassified as phishing (False Positive) and 27 cases where phishing sites were misclassified as legitimate (False Negative).

These values indicate that the model has an excellent ability to distinguish between legitimate and phishing sites. A high number of True Positives and True Negatives, accompanied by a relatively low number of False Positives and False Negatives, indicates a high level of accuracy and reliability of the system. In addition, the small error distribution shows that the model is not biased towards any of the classes and is able to generalize well to new data.

To evaluate the performance of the developed phishing detection model, a number of evaluation metrics commonly used in binary classification were calculated, namely accuracy, precision, recall, F1-Score, and Area Under Curve (AUC).

The calculation of each metric is based on the results of a confusion matrix consisting of True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) values. Here is the interpretation of each of these metrics:

$$Akurasi = \frac{TP+TN}{TP+TN+FP+FN} = \frac{1228+902}{1228+902+54+27} = \frac{2130}{2211} \approx 0,9634 \quad (1)$$

$$Presisi = \frac{TP}{TP+FP} = \frac{1228}{1228+54} = \frac{1228}{1282} \approx 0,958 \quad (2)$$

$$Recall = \frac{TP}{TP+FN} = \frac{1228}{1228+27} = \frac{1228}{1255} \approx 0,9785 \quad (3)$$

$$F1\text{-}Score = 2 \times \frac{Presisi \times Recall}{Presisi + Recall} = F1\text{-}Score = 2 \times \frac{0,958 \times 0,9785}{0,958+0,9785} = 2 \times \frac{0,9375}{1,9365} \approx 0,9673 \quad (4)$$

The AUC itself is calculated from the ROC Curve plot, but based on the high and balanced precision and recall values, the model's AUC can be estimated to be close to 0.98.

Table 1. Evaluation Matric Results

| Evaluation Metrics | Value |
|---|---|
| Accuracy | 96,34% |
| Precision | 95,8% |
| Recall | 97,85% |
| F1-Score | 96,73% |
| AUC | 0,98 |

Based on the results of the evaluation using the confusion matrix, an accuracy value of 96.34% was obtained, which shows that most of the model's predictions are correct. The accuracy value reaches 95.8%, which indicates that most of the predictions of phishing sites made by the model are actually phishing. A recall of 97.85% shows that the model is able to detect almost all phishing sites in the dataset. The F1-Score value of 96.73% reflects an excellent balance between precision and recall, which is especially important when dealing with possible class imbalances. In addition, an AUC value close to 0.98 indicates that the model has a very high ability to distinguish between phishing sites and legitimate sites at various classification thresholds. These results confirm that the combination of Multi-Kernel Learning (MKL) and Deep Q-Network (DQN) methods is capable of producing an adaptive, accurate, and reliable phishing detection system.

### 3.3 Discussion

The results of the evaluation of the phishing detection model based on the combination of Multi-Kernel Learning (MKL) and Deep Q-Network (DQN) showed very high performance in the classification of phishing and legitimate sites. The model managed to achieve an accuracy of 96.34%, which indicates that the system is capable of making correct predictions on most of the test data. This value is higher than conventional phishing detection approaches based on static supervised learning.

In addition, a precision value of 95.8% indicates that the positive predictions (phishing sites) made by the model are mostly correct, with a low false positive rate. This is especially important in real-world implementations, as too many positive errors can lower user trust in the system. The recall value of 97.85% also demonstrates the model's superiority in capturing almost all existing phishing sites, reducing the risk of undetected phishing attacks. This recall performance is better than the results of Fauzan, et al.'s (2021) research, which uses the standard Multi-Kernel Learning approach for phishing detection and achieves a recall of around 95% [12].

The balance between precision and recall is reflected in the F1-Score value of 96.73%, which shows that the model is not only accurate, but also consistent in detecting various phishing attack patterns. This is consistent with the Multi-View Learning approach developed by Tukino & Fifi, (2024) where the integration of multiple feature sources improves the balance of classification metrics [13].

The Area Under Curve (AUC) value of 0.98 underscores the model's ability to distinguish between phishing and legitimate sites in various classification threshold scenarios. These results are in line with the research of Lestari, (2022) which shows that the use of Deep Q-Network (DQN) in cybersecurity results in a high AUC for dynamic threat detection [14].

In terms of method contribution, the integration of MKL and DQN is proven to provide complementary advantages: (1) MKL enriches the representation of features by combining kernels from various sources of information (URL structure, domain metadata, and page content); (2) DQN provides an adaptive mechanism to continuously improve classification decisions based on feedback (reward) from previous prediction results.

Compared to purely supervised learning-based models, this approach shows significant advantages in dealing with a dynamic and evolving variety of phishing techniques, as also demonstrated in the Primary study, (2024) on the effectiveness of Deep Reinforcement Learning in a changing environment [15].

However, there are some challenges. High model complexity leads to longer training times, and model sensitivity to hyperparameter settings (such as learning rate and discount factor) can affect the stability and accuracy of the final result. This opens up opportunities for the exploration of automated hyperparameter optimization techniques or the use of lighter network architectures for future efficiency.

Overall, the results of this study not only strengthen the evidence that an integrative approach between multi-kernel feature representation and reinforcement learning-based adaptive learning can improve phishing detection, but also expand the application of Deep Reinforcement Learning in the cybersecurity domain more broadly.

## 4. CONCLUSION

This research has succeeded in developing a phishing detection system based on a combination of Multi-Kernel Learning (MKL) and Deep Q-Network (DQN) that is adaptive and accurate. Through the integration of multi-view representations from various information sources and reinforcement learning-based adaptive learning mechanisms, the model built was able to achieve an accuracy of 96.34%, precision of 95.8%, recall of 97.85%, F1-score of 96.73%, and AUC of 0.98. These results prove that the MKL-DQN combination approach is able to overcome the limitations of traditional phishing detection methods in the face of a variety of dynamic attack techniques. MKL contributes to enriching the classification feature space, while DQN improves model adaptivity through reward-based learning strategies. Compared to previous research, the developed system showed superior performance, especially in terms of sensitivity and accuracy of phishing detection. Nevertheless, challenges related to model complexity and the need for hyperparameter optimization remain concerns that need to be addressed in further development. Overall, the combination of MKL and DQN offers an effective and prospective solution to improve system security against future phishing threats.

**Acknowledgment** [if any]

Name the funder and the facilitator who helped.

## 5. REFERENCE


[1] APWG, "Phishing Activity Trends Report," 2023.

[2] M. S. F. Purwani, "Analysis of the Role and Countermeasures of Cybercrime: A Case Study of Spearphishing," *Restor. J. Indones. Probat. Parol. Syst.*, vol. 1, no. 1, pp. 33–45, 2023.

[3] I. H. R. Hatta *et al.*, *Artificial Intelligence*. Independent Scholar, 2024.

[4] C. Xu, J. Si, Z. Guan, W. Zhao, Y. Wu, and X. Gao, "Reliable Conflictive Multi-View Learning," *Proc. AAAI Conf. Art. Intell.*, vol. 38, no. 14, pp. 16129–16137, 2024, doi: 10.1609/AAAI.v38i14.29546.

[5] Y. Wang, W. Ma, H. Xu, Y. Liu, and P. Yin, "A lightweight multi-view learning approach for phishing attack detection using transformer with mixture of experts," *Appl. Sci.*, vol. 13, no. 13, p. 7429, 2023.

[6] M. R. Ridho, N. Fajrah, and F. Fifi, "Literature Review: The Application of Deep Reinforcement Learning in Business Intelligence," *J. Design and Analysis. Technology*., vol. 3, no. 2, pp. 96–103, 2024.

[7] M. A. G. Al Ghifari, B. Hananto, and B. T. Wahyono, "Implementation of Google Chrome Extension in Detecting Phishing Websites Using the Random Forest Algorithm," in *Proceedings of the National Seminar for Students in the Field of Computer Science and Its Applications*, 2022, pp. 640–649.

[8] R. Rahmadani, A. Rahim, and R. Rudiman, "Sentiment Analysis of 'Ojol The Game' Reviews on Google Play Store Using Naive Bayes Algorithm and Tf-IDF Feature Extraction Model to Improve Game Quality," *J. Inform. and Tek. Electro Therapy*., vol. 12, no. 3, 2024.

[9] E. N. Yudistira and S. Kom, *Deep Learning: Theory, Calculation Examples, and Implementation*. Deepublish, 2024.

[10] R. Y. Putra and F. T. E. D. I. Cerdas, "Movement Planning in Autonomous Cars on Highways Using Quantile Regression Deep Q Network," Sepuluh November Institute of Technology, 2021.

[11] Z. A. Dwiyanti and C. Prianto, "Jakarta City Weather Prediction Using the Random Forest Method," *J. Tekno Insentive*, vol. 17, no. 2, pp. 127–137, 2023.

[12] R. Fauzan, A. V Vitianingsih, D. Cahyono, A. L. Maukar, and Y. A. B. Suprio, "Application of Classification Algorithms in Machine Learning for Phishing Detection," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 5, no. 2, pp. 531–540, 2025.

[13] T. Tukino and F. Fifi, "The Application of Support Vector Machine for Sentiment Analysis in Online Motorcycle Taxi Services," *J. Design and Analysis. Technology*., vol. 3, no. 2, pp. 104–113, 2024.

[14] W. S. Lestari, "DDoS ATTACK DETECTION USING Q-LEARNING," *JATISI (Tek Journal. Inform. and Sist. Information)*, vol. 9, no. 1, pp. 648–658, 2022.

[15] D. A. S. Pratama, "Development of Adaptive Control for Autonomous Vehicles with a Case Study on Electric Cars Based on Deep Reinforcement Learning," 2024.

Muhamad_Hasbia_jiko2-1746516972589

ORIGINALITY REPORT

| 13% | 10% | 7% | 5% |
| --- | --- | --- | --- |
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
| --- | --- | --- |
| 1 | ejournal.unkhair.ac.id<br>Internet Source | 2% |
| 2 | Submitted to Universitas Khairun<br>Student Paper | 1% |
| 3 | www.frontiersin.org<br>Internet Source | 1% |
| 4 | Hussein Abdel-Jaber, Hussein Al Bazar, Muawya Naser. "A Developed Model Based on Machine Learning Algorithms for Phishing Website Detection", Recent Advances in Computer Science and Communications, 2025<br>Publication | 1% |
| 5 | blog.quantinsti.com<br>Internet Source | 1% |
| 6 | Huijian Dong. "Data Analytics in Finance", CRC Press, 2025<br>Publication | <1% |
| 7 | arxiv.org<br>Internet Source | <1% |
| 8 | jutif.if.unsoed.ac.id<br>Internet Source | <1% |
| 9 | www.medrxiv.org<br>Internet Source | <1% |
| 10 | ejournal.ikado.ac.id<br>Internet Source | <1% |
| 11 | journal.eng.unila.ac.id<br>Internet Source | <1% |

| | | |
|---|---|---|
| 12 | Farquad, M.A.H.. "Support vector regression based hybrid rule extraction methods for forecasting", Expert Systems With Applications, 201008<br>Publication | <1% |
| 13 | Submitted to University College Dublin (UCD)<br>Student Paper | <1% |
| 14 | "Intelligent Computing and Block Chain", Springer Science and Business Media LLC, 2021<br>Publication | <1% |
| 15 | www.irjiet.com<br>Internet Source | <1% |
| 16 | Submitted to University of Maryland, Global Campus<br>Student Paper | <1% |
| 17 | iieta.org<br>Internet Source | <1% |
| 18 | Submitted to Old Dominion University<br>Student Paper | <1% |
| 19 | ejurnal.stmik-budidarma.ac.id<br>Internet Source | <1% |
| 20 | repository.upnvj.ac.id<br>Internet Source | <1% |
| 21 | ejournal.kresnamediapublisher.com<br>Internet Source | <1% |
| 22 | Jiarui Chen, Wulin Xie, Mengqing Wang, Yinghao Ye, Xiaohuan Lu. "Confidence-Enhanced Dual-Space Semantic Alignment for partial multi-view incomplete multi-label classification", Knowledge-Based Systems, 2025<br>Publication | <1% |

| | | |
|---|---|---|
| 23 | jase.tku.edu.tw<br>Internet Source | <1 % |
| 24 | www.jmir.org<br>Internet Source | <1 % |
| 25 | Ruitong Liu, Yanbin Wang, Haitao Xu, Zhan Qin, Fan Zhang, Yiwei Liu, Zheng Cao. "PMANet: Malicious URL detection via post-trained language model guided multi-level feature attention network", Information Fusion, 2025<br>Publication | <1 % |

| | | | |
|---|---|---|---|
| Exclude quotes | Off | Exclude matches | Off |
| Exclude bibliography | Off | | |

# Muhamad_Hasbia_jiko2-1746516972589

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6