Jurnal Elektronik Ilmu Komputer Udayana
Volume 9 No. 4. May 2021

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Implementation of the Support Vector Machine (SVM) Algorithm in Classifying Website Phishing

Putu Agus Prawira Dharma Yuda[a1], I Putu Gede Hendra Suputra[a2]

[a]Informatics Department, Faculty of Math and Science, Udayana University
South Kuta, Badung, Bali, Indonesia
[1]agusprawira28@gmail.com
[2]hendra.suputra@gmail.com

Abstract

The development of the internet is so significant, if we look at the growth of the internet in the world, it has reached more than 4 billion and in Indonesia, there are more than 171 million users out of a total population of more than 273 million people. This is due to the very fast development of information technology and various kinds of media and functions. However, of the advances in internet technology, it did not escape the existing internet attacks. One of them is phishing. Phishing is a form of activity that threatens or traps someone with the concept of luring that person. Namely by tricking someone so that the person indirectly provides all the information the trapper needs. Phishing is included in cybercrime, where crime is rampant through computer networks. Along with the times, crime is also increasingly widespread throughout the world. So that the threats that are happening today are also via computers. With such cases, this study aims to predict phishing sites with a classification algorithm. One of them is by using the SVM (Support Vector Machine) Algorithm. This research was conducted by classifying the phishing website data set and then calculating the accuracy for each kernel. From the study, the results are SVM with Gaussian RBF has the best performance with 88.92% accuracy, and SVM with Sigmoid kernel has the worst performance with 79.33% accuracy.

Keywords: *Internet, Cyber Attack, Phishing, Classification, Support Vector Machine (SVM).*

1. Introduction

The development of the internet is so significant, if we look at the growth of the internet in the world, it has reached more than 4 billion and in Indonesia, there are more than 171 million users out of a total population of more than 273 million people [1]. This is due to the very fast development of information technology and various kinds of media and functions, one of which is in terms of financial transactions and e-commerce. This makes it easier for customers without having to bother and without having to leave the house. However, in the ease of transactions, one of the biggest problems appears, namely transaction security. This is a frightening specter for online users, especially since it has penetrated online users. One thing is security from ignorance in terms of users which as a result falls into the world of Cybercrime. Also, many online users cannot distinguish between genuine sites and fake or phishing sites, therefore this research aims to be able to predict which sites are indicated by Phishing.

Phishing is a form of activity that threatens or traps someone with the concept of luring that person. Namely by tricking someone so that the person indirectly provides all the information the trapper needs. Phishing is included in cybercrime, where crime is rampant through computer networks. Along with the times, crime is also increasingly widespread throughout the world. So that the threats that are happening today are also via computers. For hackers, this method is the easiest way to make an attack. Even though it is considered easy and trivial, there are still users who fall into the hacker's trap [2].

With such cases, this study aims to predict phishing sites with a classification algorithm. One of them is by using the SVM (Support Vector Machine) Algorithm. SVM is a technique for finding hyperplane which can separate two sets of data from two different classes. SVM has advantages including determining the distance using support vectors so that the computation process becomes fast [3]. Research on SVM has been carried out by Rachman and Purnami (2012) conducted a study on the classification of cancer malignancies using logistic regression and SVM methods, which in the end showed that the accuracy rate using SVM was higher, namely 98.11% [4]. Based on previous research, it is hoped this study can classify website phishing using a Support Vector Machine algorithm based on the existed dataset and determine which kernel is best for classifying phishing websites.

2. Literature Reviews

2.1. Cyber Attack

Cyber-attack is the result of the development of information and communication technology, so that the weapons used in cyber-attacks have several different characteristics compared to the characteristics of conventional weapons. The real goal of cyber-attack perpetrators is not merely to destroy a cyber system. The real purpose of cyber-attack is broader, including the destruction of integrity, availability, confidentiality, and physical destruction, which have an impact on the victim's activity in real space [7]. There are many types of cyber-attack including virus, worm, trojan horse, spam, DDoS attack, rootkit, phishing [9].

2.2. Phishing

According to George W. Reynolds, phishing is “the act of fraudulently using email to try to get the recipient to reveal personal data.” [9]. Phishing is carried out by sending links that appear to be genuine from related organizations to internet users via email and websites. When a user clicks on the link, the attacker gets information from the user and uses it for personal gain, for example to take money from a user's account or use the account for online payments [2].

2.3. Support Vector Machine (SVM) Algorithm

Support Vector Machine was first introduced by Vapnik in 1992 as a harmonious series of leading concepts in the field of pattern recognition. SVM is a machine learning algorithm that works on the principle of Structural Risk Minimization (SRM) with the aim of finding the best hyperplane that separates two classes in the input space [8].

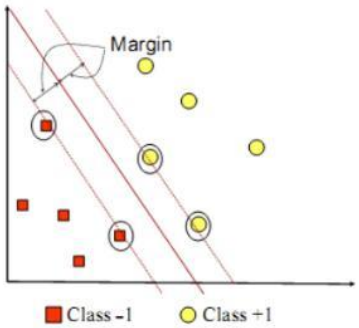

Figure 1. SVM Hyperplane

The learning process on SVM in finding support vector points only depends on the dot product from data that has been transformed into a new higher dimensional space, namely.

$$\phi(xi).\phi(xj) \quad (1)$$

Because generally this F transformation is unknown, and very difficult to understand easily, the calculation of the dot product according to Mercer's theory can be replaced by a kernel function

p-ISSN: 2301-5373
e-ISSN: 2654-5101

that implicitly defines the F transformation. This is known as the Kernel Trick, which is formulated:

$$K(xi, xj) = \phi(xi).\phi(xj) \quad (2)$$

The following are the types of kernels used on support vector machines algorithm.

a. Polynomial
$$K(xi, xj) = (xi, xj + 1)^p \quad (3)$$
b. Linear
$$K(xi, xj) = xi^t\ xj \quad (4)$$
c. Gaussian Radial Basis Function
$$K(xi, xj) = exp\left(-\frac{\|xi-xj\|^2}{2\sigma^2}\right) \quad (5)$$
d. Sigmoid
$$K(xi, xj) = \tanh(axi, axj + \beta) \quad (6)$$

Furthermore, the classification results from the data are obtained from the following equation.

$$f(\phi(x)) = \sum_{i=1.x,\in SV}^{n} a_i y_i\ K(x, x_i) + b \quad (7)$$

3. Research Methods

The methodology of this research is simulation-based research. Figure.1 shows the stages of the research in this paper.

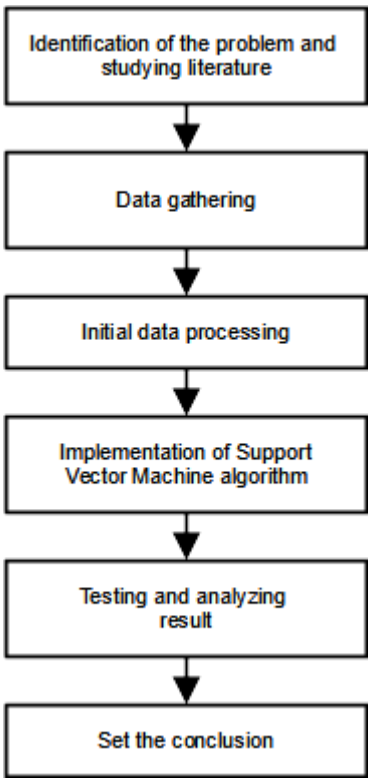

Figure 2. Flowchart Research Stages

3.1. Identification of the Problem and Study of Literature

In this research, problem identification aims to classify the type of website. The results to be achieved from this study are to classify a website whether the site is valid, suspicious, or

phishing and measure the level of accuracy. The literature study was conducted by studying previous research on phishing and SVM.

3.2. Data Collection

The sample in this study is secondary data obtained from digital computations at the UCI Neda Abdelhamid Auckland Institute of Studies. The data obtained consisted of Legitimate (-1), Suspicious (0), and Phishy (1) variables. There are 9 parameters, namely SFH, popUpWindow, SSLfinal_State, Request_URL, URL_of_Anchor, web_traffic, URL_Length, age_of_domain, and having_IP_Address. Overall there are 1353 data then divided into 2 parts which are used as training data and testing data, then there will be 1082 training data and 271 testing data [5].

Table 1. Website Phishing Data

No	Parameters	Value
1	SFH	(-1, 0, 1)
2	popUpWindow	(-1, 0, 1)
3	SSLfinal_State	(-1, 0, 1)
4	Request_URL	(-1, 0, 1)
5	URL_of_Anchor	(-1, 0, 1)
6	web_traffic	(-1, 0, 1)
7	URL_Length	(-1, 0, 1)
8	age_of_domain	(-1, 1)
9	having_IP_Address	(0, 1)
10	Result	(-1, 0, 1)

3.3. Initial Data Processing

At this stage, the data obtained from the UCI Data Sets will be processed using the SVM algorithm. The data can be converted into an integer data format so that data can be processed in the program. The program is used in the processing of this data using JetBrains PyCharm with sklearn python library to analyze the classification result.

3.4. Implementation of Support Vector Machine (SVM) Algorithm

SVM is a linear classification method. SVM's main role in classifying is to define a separator in the search space that can separate different classes. This separator is commonly referred to as a hyperplane. One of the advantages of this SVM method is that it is quite good at classifying high-dimensional data because the method tries to determine the optimal direction of discrimination in the feature space by examining the right feature combination [6]. Figure.2 shows the flowchart of the Support Vector Machine in this research.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

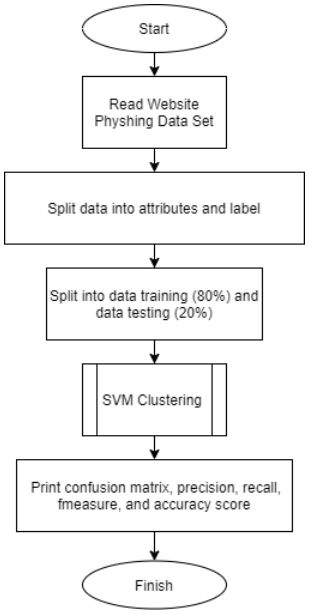

Figure 3. Support Vector Machine's Flowchart

The following are the steps for classifying phishing website data with the SVM algorithm.

a. Import the website phishing dataset.
b. Divide the data into attributes and label
c. Divide the data set into two parts, data training (80%) and data testing (20%).
d. After doing the data preprocessing, data will be classified with Support Vector Machine (SVM) algorithm. In this study will use linear, gaussian radial basis function (RBF), and sigmoid kernel type.
e. Print confusion matrix, precision, recall, f1 score, and accuracy score from data testing for each kernel type.

4. Result and Discussion

After classification, a confusion matrix is formed. In Table 2, Table 3, and Table 4 shows the result of the confusion matrix each kernel.

Table 2. Confusion Matrix on SVM Gaussian Radial Basis Function

		Real		
		-1	0	1
Prediction	-1	147	1	7
	0	4	5	5
	1	11	2	89

Table 3. Confusion Matrix on SVM Linear

		Real		
		-1	0	1
Prediction	-1	133	2	14
	0	6	2	11
	1	4	1	98

Table 4. Confusion Matrix on SVM Sigmoid

		Real		
		-1	0	1
Prediction	-1	123	1	17
	0	10	0	13
	1	15	0	92

From the table above, it is found that SVM with a gaussian kernel has more true values than linear and sigmoid kernels. After obtaining a confusion matrix, the value of precision, recall, f1 score for each class can be found with the following formula.

$$Precision = \frac{TP}{TP+FP} \quad (8)$$

$$Recall = \frac{TP}{TP+FN} \quad (9)$$

$$F1\ score = 2\ \times \frac{(Recall \times Precision)}{(Recall+Precision)} \quad (10)$$

Description:
TP = True Positive
FP = False Positive
FN = False Negative

The following is the result of calculating the precision, recall, and f1 score for each SVM kernels.

	precision	recall	f1-score	support
-1	0.91	0.95	0.93	155
0	0.62	0.36	0.45	14
1	0.88	0.87	0.88	102

Figure 4. The Result of Precision, Recall, and F1 Score from SVM Gaussian Radial Basis Function

	precision	recall	f1-score	support
-1	0.93	0.89	0.91	149
0	0.40	0.11	0.17	19
1	0.80	0.95	0.87	103

Figure 5. The Result of Precision, Recall, and F1 Score from SVM Linear

p-ISSN: 2301-5373
e-ISSN: 2654-5101

	precision	recall	f1-score	support
-1	0.83	0.87	0.85	141
0	0.00	0.00	0.00	23
1	0.75	0.86	0.80	107

Figure 6. The Result of Precision, Recall, and F1 Score from SVM Sigmoid

To calculate the accuracy value, it can use the following formula.

$$Precision = \sum \frac{total\ data\ classified\ correctly}{total\ data} \quad (11)$$

From this formula, calculations are made, and here are the following results for each SVM kernel.

```
accuracy:  0.8892988929889298
```

Figure 7. Accuracy Test Result for SVM Gaussian Radial Basis Function

```
accuracy:  0.8597785977859779
```

Figure 8. Accuracy Test Result for SVM Linear

```
accuracy:  0.7933579335793358
```

Figure 9. Accuracy Test Result for SVM Sigmoid

From the results above, it can be concluded that SVM with a gaussian radial basis function kernel has better performance in classifying website phishing compared to linear and sigmoid kernels. This can be seen from the resulting precision, recall, f1 score, and accuracy values as shown in Figures 5 and 8 while the sigmoid kernel has the lowest performance in classifying phishing websites. This can be seen from the resulting precision, recall, f1 score, and accuracy values as shown in Figures 7 and 10.

5. Conclusion

Based on the research that has been done, it is concluded that the SVM is good at classifying website phishing with Gaussian RBF kernel has the best performance on classifying phishing websites. This can be seen from the resulting level of accuracy of 88.92% in data testing using the Gaussian RBF kernel. Meanwhile, SVM with Sigmoid kernel has the worst performance on classifying phishing websites. Where the level of accuracy on SVM using the sigmoid kernel is 79.33%.

References

[1] Internet World Stats, “Asia Internet Stats by Country and 2020 Population Statistics,” 2020. https://internetworldstats.com/asia.htm#id (accessed Sep. 24, 2020).

[2] M. H. W. dan N. Fatimah, “Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime,” *JOEICT(jurnal Educ. Inf. Commun. Technol.*, vol. 1, pp. 1–5, 2017, doi: 10.29100/.V1I1.69.

[3] V. Cherkassky and F. Muller, “Guest editorial vapnik-chervonenkis (vc) learning theory and its applications,” *IEEE Trans. Neural Networks*, vol. 10, no. 5, pp. 985–987, Sep. 1999, doi: 10.1109/TNN.1999.788639.

[4] F. Rachman and S. W. Purnama, “Perbandingan Klasifikasi Tingkat Keganasan Breast

Cancer Dengan Menggunakan Regresi Logistik Ordinal Dan Support Vector Machine (SVM)," *J. Sains Dan Seni Its*, vol. 1, no. 1, pp. 130–135, 2012.

[5] N. Abdelhamid, "UCI Machine Learning Repository: Website Phishing Data Set," *UCI Machine Learning Repository*, 2016. https://archive.ics.uci.edu/ml/datasets/Website+Phishing (accessed Sep. 24, 2020).

[6] C. C. Aggarwal and C. C. Aggarwal, "Mining Text Data," in *Data Mining*, Springer International Publishing, 2015, pp. 429–455.

[7] K. E. A. Tampubolon, "Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare," *Jurist-Diction*, vol. 2, no. 2, pp. 539–554, 2019.

[8] F. Rahutomo, P. Y. Saputra, and M. A. Fidyawan, "Implementasi Twitter Sentiment Analysis Untuk Review Film Menggunakan Algoritma Support Vector Machine," *J. Inform. Polinema*, vol. 4, no. 2, p. 93, 2018, doi: 10.33795/jip.v4i2.152.

[9] G. W. Reynolds, "Ethics in Information Technology," *J. Inf. Sci.*, vol. 1, no. 5, pp. 277–283, 2014, doi: 10.1177/016555157900100505.