STM JOURNALS

Journal of
Telecommunication, Switching Systems and Networks

ISSN: 2454-6372
Volume 11, Issue 2, 2024
May–August
DOI (Journal): 10.37591/JoTSSN

https://journals.stmjournals.com/jotssn

Review JoTSSN

Advancements in Phishing Detection: Automated Systems in Real-World Scenarios

S. Umamaheswari[1], S. Saranya[2,*]

Abstract

The goal of the study is to offer an automated method that uses login URLs to identify real-world scenarios. Phishing is a type of cyberattack that involves social engineering, when malefactors trick victims into providing their login credentials via a login form that sends the information to a hostile site. In this research, we offer a system that uses URL analysis to detect phishing websites by comparing machine learning and deep learning methodologies. The legitimate class in the majority of modern state-of-the-art phishing detection technologies consists of homepages without login fields. Instead, we utilize the login page URL in both classes, since we believe it to be a lot more realistic case scenario, and we show that testing with legitimate login page URLs yields a significant false-positive rate for existing methodologies. Additionally, we train a base model with old datasets and test it with new URLs, using datasets from different years to illustrate how models lose accuracy with time. Additionally, we run a frequency analysis across active phishing domains to find various tactics used by phishers in their campaigns. In order to validate these claims, we have developed a new dataset called Phishing Index Login URL (PILU-90K), which consists of 30K phishing URLs and 60K authentic URLs, such as index and login webpages.

Keywords: Phishing index, frequency, traffic, PyCharm, python libraries, Naïve Bayes

INTRODUCTION

In the digital era, phishing assaults continue to be one of the most prevalent and harmful cyberthreats, and perpetrators are always improving their methods of tricking gullible targets. These attacks frequently entail the illicit capture of private data, including passwords, usernames, and financial information, by impersonating reliable parties in online contacts. Due to the increasing sophistication of phishing attempts, sophisticated detection measures that can recognize and neutralize these threats in advance are required. Consequently, it has become evident that utilizing artificial intelligence (AI) is a feasible approach to enhance the efficacy of phishing detection systems. Artificial intelligence (AI) in phishing detection makes use of deep learning (DL) and machine learning (ML) algorithms' ability to find patterns and abnormalities in large datasets. Unlike traditional rule-based systems that rely on predefined heuristics, artificial intelligence (AI)-based approaches have the ability to learn from data, adapt to new hazards, and improve over time. This flexibility is essential in the ever-changing world of cyber threats, where attackers often alter their strategies in order to avoid discovery. Real-time threat response and mitigation are made possible by the use of AI into phishing detection, which not only increases the accuracy of recognizing malicious activity but also decreases the need for human

***Author for Correspondence**
S. Saranya
E-mail: seesaran08@gmail.com

[1,2]Professor, Department of Information Technology, C. Abdul Hakeem College of Engineering and Technology/Anna University, Tamil Nadu, India

Received Date: July 06, 2024
Accepted Date: July 10, 2024
Published Date: July 23, 2024

Citation: S. Umamaheswari, S. Saranya. Advancements in Phishing Detection: Automated Systems in Real-World Scenarios. Journal of Telecommunication, Switching Systems and Networks. 2024; 11(2): 12–17p.

interaction. Prior studies have proven AI's capacity to identify phishing attempts, regardless of their level of effectiveness. Sahingoz *et al*., for example, investigated the application of natural language processing (NLP) techniques in phishing detection and found that these methods significantly improved accuracy in comparison to more conventional approaches [1]. Comparably, Rao and Pais looked into the use of DL models to identify phishing websites and provide improved performance metrics [2]. But these studies frequently concentrate on particular facets of phishing detection or use small datasets, which could not adequately represent the variety of phishing tactics used by attackers [3]. Cybercriminals who have depended on the illicit use of digital assets, especially personal information, to harm people are growing and changing at a rapid pace, much like the digital world. Identity theft, which is defined as impersonating a person to steal and use their personal information (such as bank account details, social security numbers, credit card numbers, etc.) by an attacker for the individuals' own gain, not just for stealing money but also for committing other crimes, is one of the most dangerous crimes that affect all internet users [4]. Although cybercriminals have also improved their techniques, their preferred method of information theft is still social engineering-based attacks. Phishing attacks are a type of social engineering crime where the attacker uses deception to steal someone's identity. Since phishing targets a large number of internet users, it has become one of the main problems. This is a social engineering attack in which a hacker uses an automated pattern to deceive users into divulging their sensitive information by falsely posing as a reputable or well-known organization. The goal is to gain the victim's trust by tricking them into sending the attacker their sensitive information [5].

Phishers utilize social engineering techniques to send people to malicious websites when they click on an embedded link in an email they receive [6]. As an alternative, hackers might use other platforms including Instant Messaging (IM), Short Message Service (SMS), and Voice over IP (VoIP) to carry out their assaults [6]. Additionally, phishers have shifted from sending bulk emails that target random targets to more targeted emails that are sent to specific victims, a tactic known as “spear-phishing”. Along with technological flaws, cybercriminals typically take advantage of individuals who lack digital or cyber ethics or who are ill-trained in order to accomplish their objectives. Individuals differ in their susceptibility to phishing depending on their characteristics and degree of awareness. For this reason, most assaults involve phishers taking use of human nature for hacking rather than using advanced technologies. There is a dearth of knowledge on which ring in the information security chain is first compromised, despite the fact that people are more to blame for the chain's fragility than technology. Research suggests that certain personality traits may increase a person's likelihood of committing crimes. For instance, people who typically follow the law more closely than others are more likely to become victims of Business Email Compromise (BEC) attacks, in which a fraudulent email purporting to be from a financial institution is forwarded to victims, requesting urgent action. Another human vulnerability that an attacker could exploit is greed. For instance, an attacker could send emails advertising fantastic discounts, free gift cards, or other incentives. The attacker uses a variety of methods to trick the victim into falling for a scam or to subtly deliver a payload in order to obtain private and sensitive information from them. Phishing assaults, however, have already resulted in significant losses and have the potential to harm a victim not only financially but also in other ways, such as reputational damage or jeopardizing national security. Cybersecurity Ventures projects that global cybercrime costs will grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. According to official statistics from the cybersecurity breaches study 2020 in the United Kingdom, phishing attacks are the most prevalent kind of cybersecurity breaches. While both individuals and businesses are impacted by these attacks, organizations suffer substantial losses as a result of them. These losses include recovering costs, reputational damage, fines from information laws and regulations, and decreased productivity. Phishing is an area of research that combines political science, technical systems, social psychology, and security issues. According to a recent survey, targeted phishing attacks affected almost 90% of firms in 2019. This indicates that phishing assaults are becoming increasingly common. 88% of them dealt with spear-phishing assaults, 83% with voice phishing (also known as Vishing), 86% with social media attacks,

84% with SMS/text phishing (also known as SMishing), and 81% with malicious USB drops. According to the 2018 Proofpoint 1 annual report, the frequency of all types of phishing assaults increased from 76% in 2017 to 83% in 2018 [7].

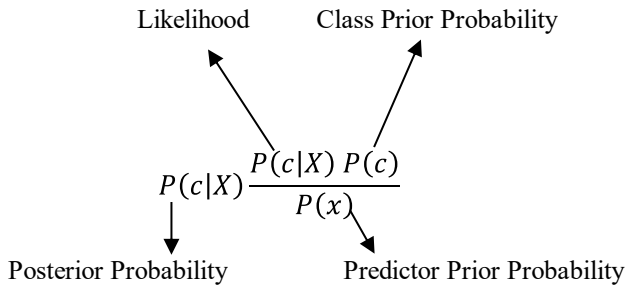
NAIVE BAYES ALGORITHM

This Bayesian-based classification technique is predicated on the assumption of predictor independence. In other words, a Naive Bayes classifier operates under the premise that the existence of one feature in a class does not depend on the existence of any other feature. For example, a fruit that is crimson, spherical, and around 3 in in diameter could be considered an apple. "Naive" describes how each of these traits, even if they rely on the existence of other traits or one another, independently raises the probability that this fruit is an apple [7, 8].

.

The Naive Bayes model is easy to build and particularly useful for very large data sets. In addition to being straightforward, Naive Bayes is known to outperform even rather complicated classification systems.

The Bayes theorem can be used to obtain the posterior probability P(c|x) from P(c), P(x), and P(x|c). Look at the equation shown in Figure 1 that follows:



$$P(c|X) = P(x_1|c) \times P(x_2|c) \times \cdots \times P(x_n|c) \times P(c)$$

Figure 1. Bayes Probability.

where

- Pc|x) is the posterior probability of class (c, target) given predictor (x, attributes);
- P(c) is the prior probability of class in Figure 1;
- P(x|c) is the likelihood which is the probability of predictor given class; and
- P(x) is the prior probability of predictor.

NAIVE BAYES ALGORITHM WORKS

Training data set of weather along with the objective variable "Play" (which indicates the likelihood of playing) is included below. We must now categorize the players' participation in relation to the weather. Let us carry it out by following the procedures below:

Step 1: Compile likelihood as shown in Table 1–3 using the probabilities you have determined, such as the overcast probability of 0.29 and the playing probability of 0.64.

Step 2: Next, determine the posterior probability for each class shown in Figure 2 using the Naive Bayesian equation.

Problem: If it is sunny outside, players will play. Is this assertion accurate? We can use the posterior probability method that was previously mentioned to solve it.

P(Sunny out side | Yes)/P(Yes) = P(Sunny out side | Yes) * P(Yes)

Table 1. Chances of being outside vs weather condition.

Weather	Play
Sunny	No
Overcast	Yes
Rainy	Yes
Sunny	Yes
Sunny	Yes
Overcast	Yes
Rainy	No
Rainy	No
Sunny	Yes
Rainy	Yes
Sunny	No
Overcast	Yes
Overcast	Yes
Rainy	No

Table 2. Frequencies as per weather conditions.

Weather	No	Yes
Overcast		4
Rainy	3	2
Sunny	2	3
Grand Total	5	9

Table 3. Likelihood of being outside vs weather condition (in decimals also).

Weather	No	Yes		
Overcast		4	=4/14	0.29
Rainy	3	2	=5/14	0.36
Sunny	2	3	=5/14	0.36
All	5	9		
		=5/14	=9/14	
		0.36	0.64	

A similar technique is used by Naive Bayes to forecast the likelihood of a distinct class depending on a variety of criteria.

FOUR OF NAIVE BAYES ALGORITHM

- *Real time Prediction:* Naive Bayes is a quick and eager learning classifier. Thus, it could be used for making predictions in real time [9].
- *Multi class Prediction:* The multi-class prediction feature of this algorithm is another well-known feature.
- *Text classification/Spam Filtering/Sentiment Analysis:* In comparison to other algorithms, naive Bayes classifiers, which are primarily utilized in text classification, have a greater success rate because to their superior performance in multi-class situations and independence rule [10].
- *Recommendation System:* Naive Bayes Classifier and Collaborative Filtering together build a Recommendation System that uses machine learning and data mining techniques to filter unseen information and predict whether a user would like a given resource or not [11, 12].

HOW DOES IT WORK?

The procedure mentioned earlier of using a hyper-plane to divide the two classes became familiar to us. Let us comprehend: Choose the appropriate hyper-plane (Scenario-1): Three hyper-planes (A, B, and C) are shown here in Figure 2. Select the appropriate hyper-plane now to categorize the star and circle.

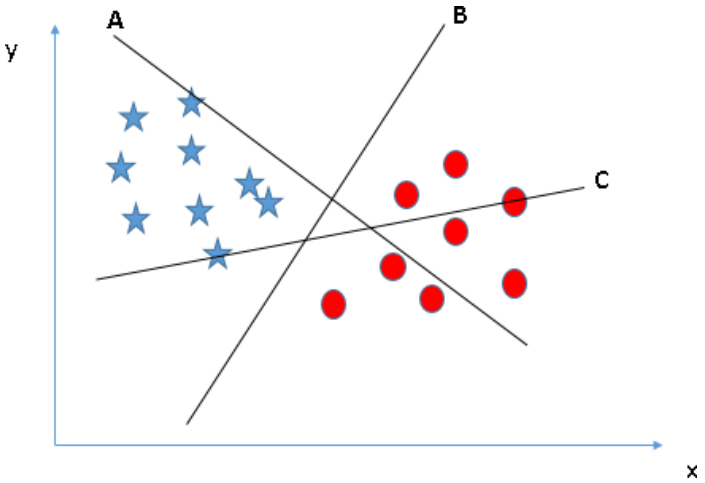


Figure 2. Hyperplanes.

To choose the appropriate hyper-plane, keep in mind the following general guideline: "Select the hyper-plane which segregates the two classes better" (Figure 3). Hyper-plane "B" has done a fantastic job in this case.

Architecture Diagram: Architectural Diagram of process is shown in Figure 3.

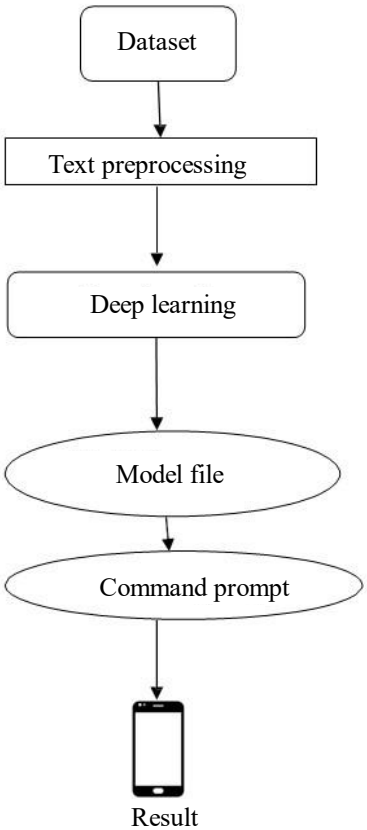


Figure 3. Process Architecture Diagram.

CONCLUSION

In conclusion, we have shown that the performance of machine learning models using handcrafted URL attributes is boosted. Consequently, machine learning techniques should be trained with recent URLs to avoid significant aging from the date of release.

Future Work

In the future, we will include more details about the samples in the analysis, like the website's content and a screenshot of it, which can help improve the performance of the phishing detection system. In order to boost efficiency, we will also add more data to our dataset and use a few additional algorithms. Lastly, we want to investigate other URL codifications to enhance detection performance, having seen that automatic feature extraction and deep learning algorithms produced encouraging results compared to traditional feature extraction.

REFERENCES

1. Sahingoz OK, Buber E, Demir O, Diri B. Machine learning based phishing detection from URLs. Expert Syst Appl. 2019 Mar 1; 117: 345–57.
2. Rao RS, Pais AR. Jail-Phish: An improved search engine based phishing detection system. Comput Secur. 2019 Jun 1; 83: 246–67.
3. Maddireddy BR, Maddireddy BR. AI-Based Phishing Detection Techniques: A Comparative Analysis of Model Performance. Unique Endeavor in Business & Social Sciences (UEBSS). 2022 Jun 30; 1(2): 63–77.
4. Ramanathan V, Wechsler H. phishGILLNET—phishing detection methodology using probabilistic latent semantic analysis, AdaBoost, and co-training. EURASIP J Info Security. 2012 Dec; 2012: 1–22.
5. Jakobsson M, Myers S, editors. Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons New York, United States; 2006 Dec 5.
6. Zhang W, Gupta S, Lian X, Liu J. Staleness-aware async-sgd for distributed deep learning. arXiv preprint arXiv:1511.05950. 2015 Nov 18.
7. Alkhalil Z, Hewage C, Nawaf L, Khan I. Phishing attacks: A recent comprehensive study and a new anatomy. Front Comput Sci. 2021 Mar 9; 3: 563060.
8. Pandey N, Pal A. Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. Int J Inf Manag. 2020 Dec 1; 55: 102171.
9. Alzahrani A. Coronavirus social engineering attacks: Issues and recommendations. Int J Adv Comput Sci Appl. 2020; 11(5): 154–161.
10. Patel P, Sarno DM, Lewis JE, Shoss M, Neider MB, Bohil CJ. Perceptual representation of spam and phishing emails. Appl Cogn Psychol. 2019 Nov; 33(6): 1296–304.
11. Chaudhry JA, Chaudhry SA, Rittenhouse RG. Phishing attacks and defenses. Int J Secur its Appl. 2016 Jan 1; 10(1): 247–56.
12. Hijji M, Alam G. A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. IEEE Access. 2021 Jan 1; 9: 7152–69.

