International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

A Machine Learning Approach for AI-Based Phishing Detection and Classification of Malicious URLs

Dr. M. Subathra
M.C.A., M. Phil., Ph. D.,
Assistant Professor II - MCA
Dept. of Computer Applications,
Vellalar College for Women,
Erode, Tamil Nadu, India.

B. K. Sivavarsni,
Dept. of Computer Applications,
Vellalar College for Women,
Erode, Tamil Nadu, India

Phishing is considered to be one of the most common types of Cybersecurity threats. The attack tricks users into giving away sensitive information such as login credentials, financial data, and personal data. The traditional security systems fail to identify newly created phishing websites because attackers are always changing their methods. This project aims to solve this problem by developing an AI-Based Phishing Detection System. This system makes use of machine learning algorithms to identify phishing websites more effectively.

The proposed system makes use of various attributes such as characteristics of URLs, domain details, and web content to identify potential phishing attacks. The machine learning model is trained on a set of URLs, both legitimate and phishing websites. Once the model is trained, it can predict whether a particular website or link is safe or not.

The proposed system makes use of artificial intelligence to increase accuracy rates. This helps to avoid users being tricked by phishing attacks. The development of such a system can lead to a significant increase in online security. This is because it can provide warnings to users regarding potential phishing attacks. This helps to increase the accuracy rates of users while making browsing decisions.

Keywords - Phishing Detection, Machine Learning, Cybersecurity, URL Analysis, Artificial Intelligence, Website Classification.

INTRODUCTION

With the rise of internet usage, the number of cyber threats has also increased at a rapid pace. Among these cyber threats, phishing attacks have become one of the most common methods used by cybercriminals to steal sensitive information from internet users. In most cases, phishing attacks are carried out by sending fake emails, websites, or messages from organizations like banks, social media, or online shopping websites. When internet users unknowingly click on these phishing links, their personal information is misused by the attacker, leading to financial fraud, identity theft, and other illegal activities.

Blacklists are one of the most commonly used methods to detect phishing attacks. There are many limitations associated with the traditional method of detecting phishing attacks, like the generation of new phishing websites by cybercriminals with a changed URL, making it difficult for the traditional method to detect these phishing websites at a faster pace. Hence, these phishing websites are active for a period of time before being detected by the traditional method.

To avoid such shortcomings, artificial intelligence and machine learning can be used to effectively detect phishing attacks. Machine learning models can be used to analyze patterns and features from a large number of phishing and legitimate websites. Using such patterns and features, the system can be used to identify suspicious behavior and classify websites as either legitimate or phishing sites.

The objective of the project is to develop an AI-Based Phishing Detection System that can be used to automatically analyze the characteristics of a website and detect phishing sites. The system uses machine learning models to analyze features such as URL length, presence of special characters, domain age, and webpage structure. Using such features, the system can be used to classify a website as either legitimate or a phishing site.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

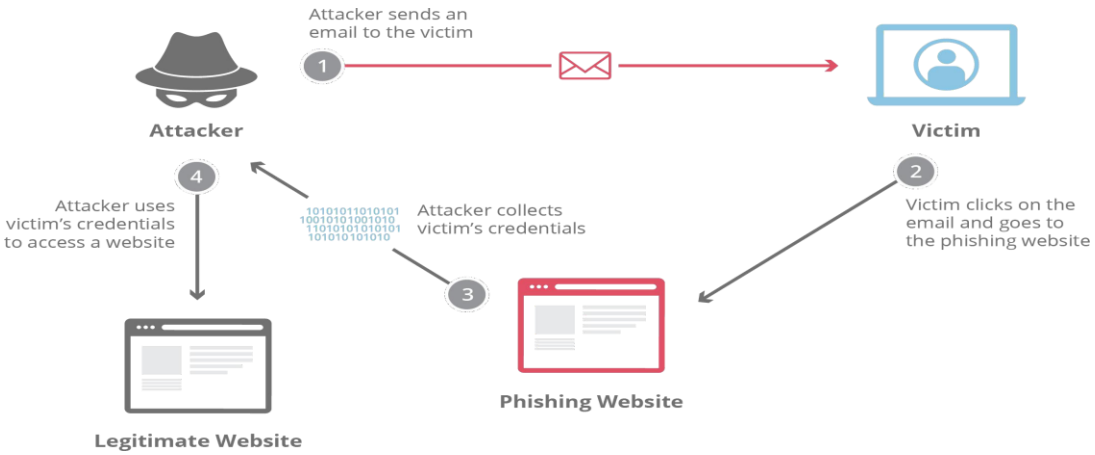

Fig.1.1

PROPOSED SYSTEM

The proposed AI-Based Phishing Detection System is intended to detect phishing websites using machine learning technology. Unlike other conventional systems that only employ a list of blacklisted phishing sites to detect phishing attacks, the proposed system employs intelligent algorithms to detect phishing websites.

The AI-Based Phishing Detection System works by analyzing various features associated with a particular website or URL. These features include the length of the URL, presence of special characters, number of subdomains, age of the domain, and characteristics of content associated with a particular website. Analyzing these features will help the system detect patterns that are usually associated with phishing attacks.

The system will employ a set of URLs associated with both phishing and legitimate websites to train a machine learning algorithm. During the training phase, the algorithm will be able to differentiate between legitimate and phishing websites using various features. Once the training phase is completed, the machine learning algorithm will be able to predict the nature of a particular website using its characteristics.

When a user types a website into the system, it processes the data and determines if it is a legitimate or phishing website. If the website is acting suspiciously, it warns the user and blocks them from accessing the site, which reduces the risk of users falling victim to a phishing attack.

The proposed system has several advantages, including increased accuracy, faster phishing site identification, and the ability to identify unknown phishing sites. The proposed system utilizes artificial intelligence to learn how to identify new types of phishing attacks created by attackers.

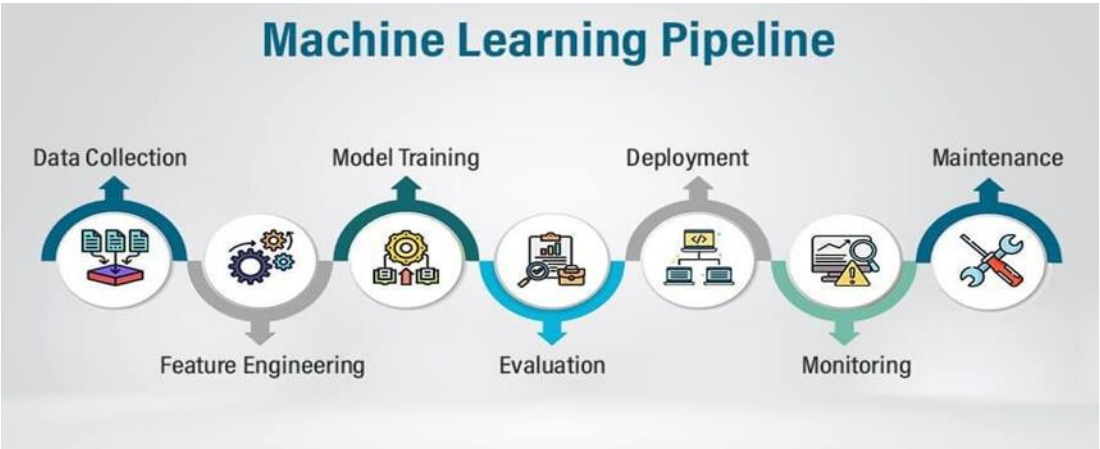

Fig:1.2

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

METHODOLOGY

The methodology used in the AI-Based Phishing Detection System is as follows:

The first stage in the methodology is to gather a dataset containing phishing and legitimate URLs from reliable sources. This dataset is used to train the machine learning model. Each URL in the dataset is marked as phishing or legitimate.

The second stage involves the extraction of significant features from URLs and websites. The features assist the model in recognizing the characteristics of phishing attacks. The features used can vary. The following are some of the common features used to identify phishing attacks:

- The length of the URLs
- The inclusion of special characters such as "@" or "-"
- The number of subdomains
- The use of HTTPS
- The registration age of the domain
- The content properties of websites

After feature extraction, the data is split into a training set and a testing set. The training set is used to train the machine learning algorithm. This allows the model to learn the patterns associated with phishing websites and legitimate websites. Various machine learning techniques, such as Decision Trees, Random Forest, or Logistic Regression, can be used.

After the model is trained, it is tested with the testing data set to measure its performance. The accuracy and reliability of the trained model are measured by various evaluation parameters such as accuracy, precision, recall, and F1 score.

Finally, the trained model is integrated with the phishing detection system. When a user enters the website's URL, the system collects the necessary features and passes them to the trained model. The model then classifies the website as safe or malicious and displays the output to the user.

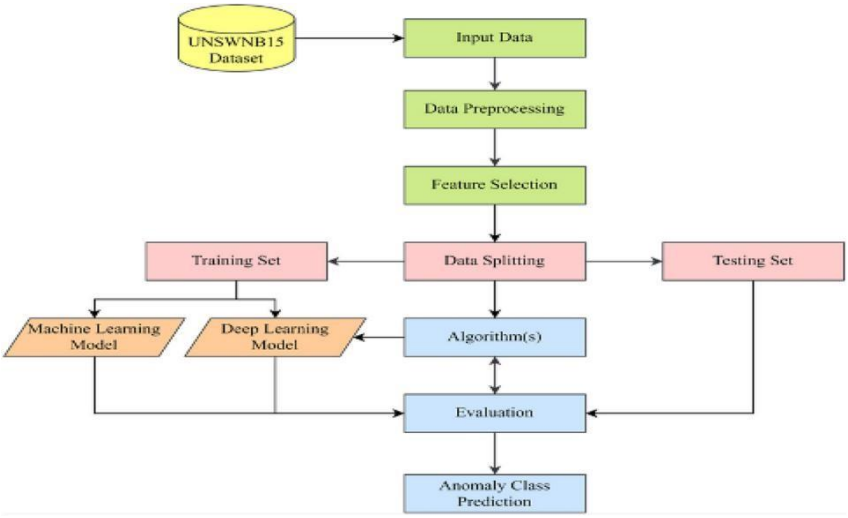

Fig 1.3

RESULTS

The usage of the AI-Based Phishing Detection System proves that it is possible to detect phishing websites with the usage of machine learning techniques. The system was trained with a set of phishing and legitimate website data, and it was

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

able to classify the websites with high accuracy.

The results show that the system is able to detect phishing attacks with common phishing patterns such as suspicious URLs, abnormal domain structures, and abnormal website characteristics. The performance of the machine learning model was good in terms of accuracy, precision, and recall values.

It is worth mentioning that the system offers real-time predictions to users when they input a URL. In case the system detects a phishing site, it will warn the user and prevent him from accessing the malicious site.

Based on the results, it is clear that the proposed system has the potential to enhance the detection of phishing sites compared to the traditional rule-based systems.

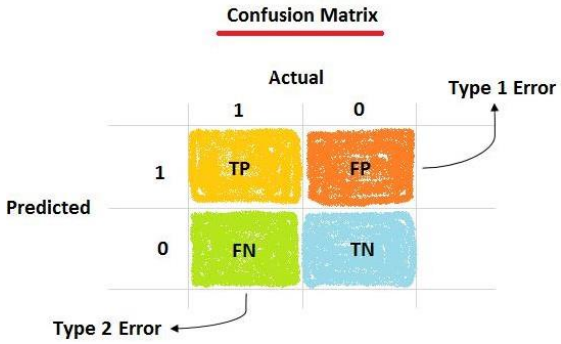

Fig.1.4

CONCLUSION

Phishing attacks are still a major threat to internet users, as attackers take advantage of human nature and trick people into accessing malicious websites that appear to be legitimate. Existing detection methods are not very reliable in identifying new phishing websites. In this context, the integration of artificial intelligence and machine learning is considered to be a more reliable solution to detect phishing attacks.

The AI-Based Phishing Detection System, which is designed and implemented in this project, relies on machine learning algorithms to analyze the features of a website and determine whether it is legitimate or a phishing site.

The results prove that machine learning can be used to improve the detection capabilities of phishing detection systems. In addition, the system can be enhanced in future using deep learning techniques to provide robust protection against phishing attacks.

REFERENCES

[1]. A. Jain and B. Gupta, “Phishing Detection: Analysis of Visual Similarity Based Approaches,” *Security and Communication Networks*, 2017.
[2]. Verma, R., & Hossain, N. “Semantic Feature Selection for Text with Application to Phishing Email Detection.”
[3]. Mohammad, R. M., Thabtah, F., & McCluskey, L. “Phishing Websites Detection Using Machine Learning.”
[4].Sahoo, D., Liu, C., & Hoi, S. C. H. “Malicious URL Detection using Machine Learning.”
[5]. IEEE Research Papers on Phishing Detection and Cybersecurity.