iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60518

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Guardian Shield: Advance Phishing Detection Using Machine Learning

Prof. A. R. Ghongade[1], Miss. Ayeshwarya Tarone[2], Mr. Rushabh Urkude[3], Mr. Gaurav Sardar[4], Mr. Abhishek Wathore[5], Miss. Yaminee Chafale[6]
[1]*Professor,* [2, 3, 4, 5, 6]*Student, Computer Science And Engineering, Shri Shankarprasad Agnihotri College Of Engineering Ramnagar, Wardha, Maharashtra, India.*

Abstract: ***Criminals seeking sensitive information construct illegal clones of actual websites and e-mail accounts. The e-mail will be made up of real firm logos and slogans. When a user clicks on a link provided by these hackers, the hackers gain access to all of the user's private information, including bank account information, personal login passwords, and images. Random Forest and Decision Tree algorithms are heavily employed in present systems, and their accuracy has to be enhanced. The existing models have low latency. Existing systems do not have a specific user interface. In the current system, different algorithms are not compared. Consumers are led to a faked website that appears to be from the authentic company when the e-mails or the links provided are opened. The models are used to detect phishing Websites based on URL significance features, as well as to find and implement the optimal machine learning model. Logistic Regression, Multinomial Naive Bayes, and XG Boost are the machine learning methods that are compared. The Logistic Regression algorithm outperforms the other two.***
Keywords: Phishing Detection, Machine Learning, Malicious URL Detection.

I. INTRODUCTION

A. What is Machine Learning?

Machine Learning is a system of computer algorithms that can learn from example through self-improvement without being explicitly coded by a programmer. Machine learning is a part of artificial Intelligence which combines data with statistical tools to predict an output which can be used to make actionable insights.

The breakthrough comes with the idea that a machine can singularly learn from the data (i.e., example) to produce accurate results. Machine learning is closely related to data mining and Bayesian predictive modeling. The machine receives data as input and uses an algorithm to formulate answers.

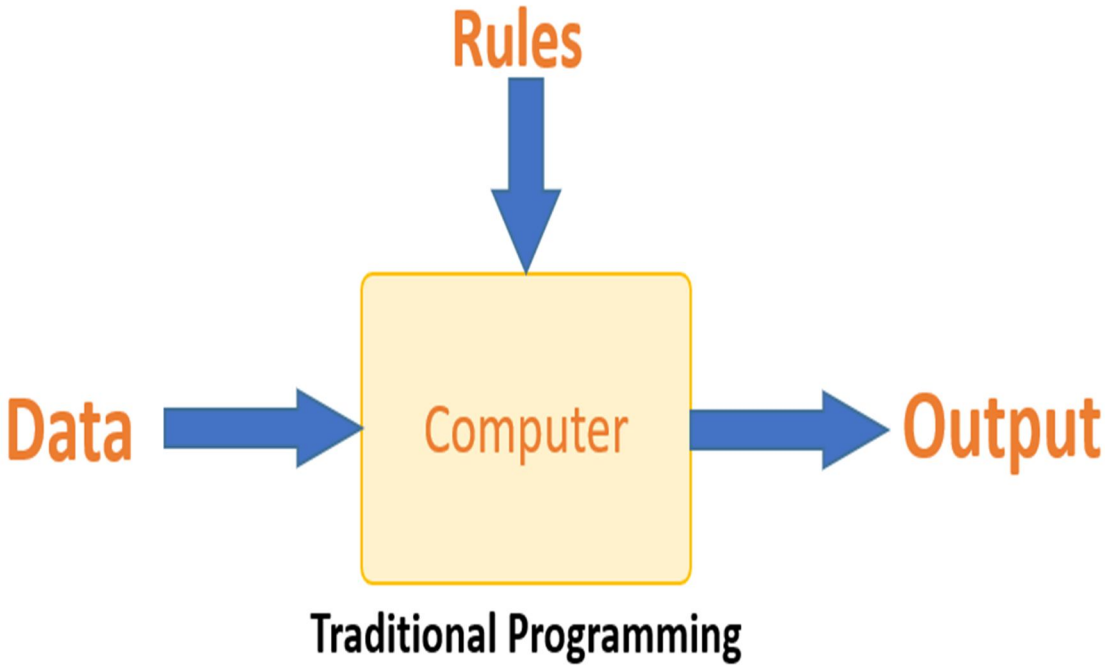
A typical machine learning tasks are to provide a recommendation. For those who have a Netflix account, all recommendations of movies or series are based on the user's historical data. Tech companies are using unsupervised learning to improve the user experience with personalizing recommendation.

Machine learning is also used for a variety of tasks like fraud detection, predictive maintenance, portfolio optimization, automatize task and so on.

B. Machine Learning vs. Traditional Programming

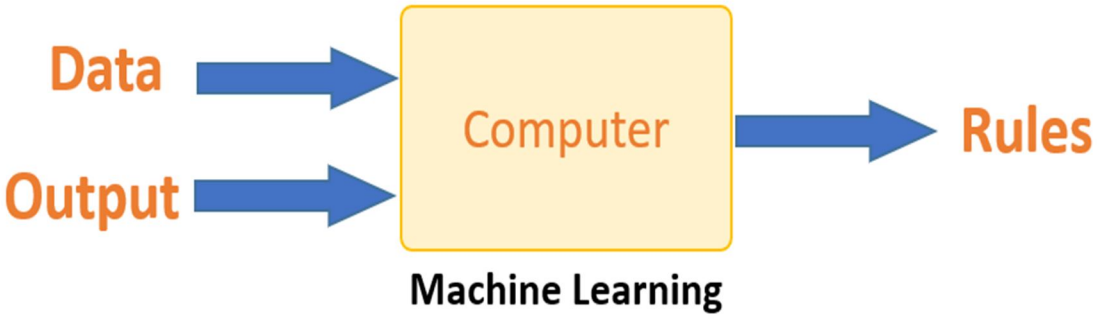
Traditional programming differs significantly from machine learning. In traditional programming, a programmer code all the rules in consultation with an expert in the industry for which software is being developed. Each rule is based on a logical foundation; the machine will execute an output following the logical statement. When the system grows complex, more rules need to be written. It can quickly become unsustainable to maintain.

Traditional programming differs significantly from machine learning. In traditional programming, a programmer code all the rules in consultation with an expert in the industry for which software is being developed. Each rule is based on a logical foundation; the machine will execute an output following the logical statement. When the system grows complex, more rules need to be written. It can quickly become unsustainable to maintain.



Traditional Programming

Machine learning is supposed to overcome this issue. The machine learns how the input and output data are correlated and it writes a rule. The programmers do not need to write new rules each time there is new data. The algorithms adapt in response to new data and experiences to improve efficacy over time.



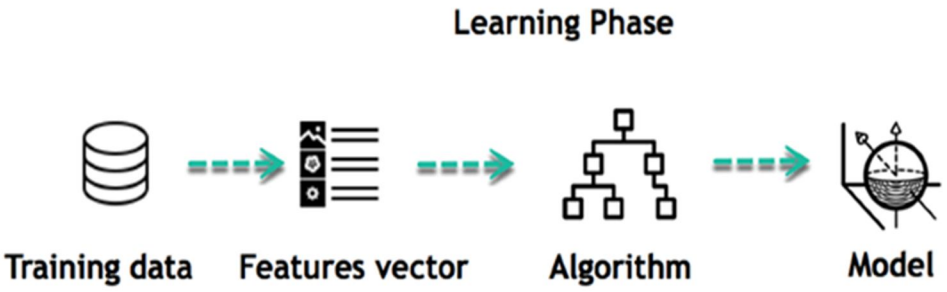
Machine Learning

C. How does Machine Learning Work?

Machine learning is the brain where all the learning takes place. The way the machine learns is similar to the human being. Humans learn from experience. The more we know, the more easily we can predict. By analogy, when we face an unknown situation, the likelihood of success is lower than the known situation. Machines are trained the same. To make an accurate prediction, the machine sees an example. When we give the machine a similar example, it can figure out the outcome. However, like a human, if its feed a previously unseen example, the machine has difficulties to predict.

The core objective of machine learning is the learning and inference. First of all, the machine learns through the discovery of patterns. This discovery is made thanks to the data. One crucial part of the data scientist is to choose carefully which data to provide to the machine. The list of attributes used to solve a problem is called a feature vector. You can think of a feature vector as a subset of data that is used to tackle a problem.

The machine uses some fancy algorithms to simplify the reality and transform this discovery into a model. Therefore, the learning stage is used to describe the data and summarize it into a model.



For instance, the machine is trying to understand the relationship between the wage of an individual and the likelihood to go to a fancy restaurant. It turns out the machine finds a positive relationship between wage and going to a high-end restaurant: This is the model

II. LITERATURE REVIEW

This article surveys the literature on the detection of phishing attacks. Phishing attacks target vulnerabilities that exist in systems due to the human factor. Many cyber attacks are spread via mechanisms that exploit weaknesses found in end-users, which makes users the weakest element in the security chain. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks. This paper aims at surveying many of the recently proposed phishing mitigation techniques. A high-level overview of various categories of phishing mitigation techniques is also presented, such as: detection, offensive defense, correction, and prevention, which we belief is critical to present where the phishing detection techniques fit in the overall mitigation process.

Q. Priming and warnings are not effective to prevent social engineering attacks

Humans tend to trust each other and to easily disclose personal information. This makes them vulnerable to social engineering attacks. The present study investigated the effectiveness of two interventions that aim to protect users against social engineering attacks, namely priming through cues to raise awareness about the dangers of social engineering cyber-attacks and warnings against the disclosure of personal information. A sample of visitors of the shopping district of a medium-sized town in the Netherlands was studied. Disclosure was measured by asking subjects for their email address, 9 digits from their 18 digit bank account number, and for those who previously shopped online, what they had purchased and in which web shop. Relatively high disclosure rates were found: 79.1% of the subjects filled in their email address, and 43.5% provided bank account information. Among the online shoppers, 89.8% of the subjects filled in the type of product(s) they purchased and 91.4% filled in the name of the online shop where they did these purchases. Multivariate analysis showed that neither priming questions, nor a warning influenced the degree of disclosure. Indications of an adverse effect of the warning were found. The implications of these findings are discussed.

III. AIM AND OBJECTIVE

A. *Aim*

The primary goal of a phishing detection website using machine learning is to identify and prevent phishing attacks. Phishing is a form of cyber attack where attackers try to trick individuals into providing sensitive information, such as login credentials or financial details, by posing as trustworthy entities. The aim of the project is to leverage machine learning techniques to detect and thwart such phishing attempts in real-time.

B. *Objectives:*

1) Detection Accuracy: Develop machine learning models capable of accurately identifying phishing websites. The objective is to achieve a high level of accuracy in distinguishing between legitimate and phishing websites to minimize false positives and false negatives.
2) *Real-time Detection:* Implement a system that can perform phishing detection in real-time. The objective is to provide timely alerts or preventive measures to users as they navigate websites, ensuring immediate protection against potential phishing threats

3) *Feature Extraction:* Identify and extract relevant features from website data that can be used as input for machine learning algorithms. This may include analyzing URLs, webpage content, SSL certificates, and other indicators of phishing behavior.
4) *Machine Learning Model Training:* Train machine learning models using labeled datasets that contain examples of both phishing and legitimate websites. The objective is to create models that can generalize well to new, unseen instances of phishing attacks.
5) *Integration with Web Browsers:* Integrate the phishing detection system with web browsers or as a browser extension. The objective is to provide a seamless user experience, with warnings or indicators directly within the browsing environment.
6) *User Education:* Include educational components to inform users about phishing threats and the importance of recognizing them. The objective is to empower users to make informed decisions and be vigilant against potential phishing attacks.
7) *Adaptability and Updates:* Develop the system to be adaptable and capable of evolving with new phishing tactics. Regularly update the machine learning models to ensure they remain effective against emerging threats.
8) *Scalability:* Design the system to handle a large number of users and website requests. The objective is to ensure scalability so that the phishing detection website can cater to a broad user base effectively.
9) *User Feedback:* Implement a feedback mechanism where users can report potential false positives or false negatives. The objective is to continuously improve the system based on user feedback and enhance its overall effectiveness.
10) *Compliance and Privacy:* Ensure compliance with privacy regulations and design the system to respect user privacy. The objective is to build a trustworthy and transparent solution that prioritizes user data security.

IV. METHODOLOGY

The model is preprocessed in the proposed system, the words are tokenized, and stemming is performed. Data Processing is the process of converting or encoding data for easy machine transfer. In other words, the algorithm can now easily define data features. We must vectorize our URLs now that we have the data. Because some words in URLs are more essential than others, such as "virus," ".exe," and so on, the model employs Count Vectorizer and tokenizer to aggregate words. Let's make a vector representation of the URLs. A tokenizer that separates a string using a regular expression that matches either the tokens or the separators between tokens is known as a regular expression tokenizer. A regex pattern is a particular language for representing general text, numbers, or symbols in order to extract texts that match the pattern. 's+' is a simple example.. The method will sync at least one or more gaps if you add a '+' at the end.. In the world, stemming is crucial. Queries and Internet search engines both use stemming. The Fast Api framework is used for deployment.

Fast API is a web framework for constructing APIs with Python 3.6+ and standard Python type hints that is current and fast (high-performance). The following are the main characteristics: Fast: Extremely fast, comparable to NodeJS and Go (thanks to Starlette and Pydantic). One of the quickest Python frameworks on the market. The UI is provided using FastAPI by loading the machine learning model into it. The architectural flow is shown in fig.1..

A. *Advantages Of Proposed System*

1) User Interface is provided
2) Model is trained using many features
3) High level of accuracy

B. *Logistic Regression*

A statistical strategy for predicting binary classes is logistic regression. The outcome or target variable is a binary variable. The term dichotomous refers to the fact that there are only two potential classes. It can, for example, be utilized to solve cancer detection issues. It calculates the likelihood of an event occurring.

C. *XG Boost*

Extreme Gradient Boosting is abbreviated as XG Boost. The word XG Boost, on the other hand, refers to the engineering goal of pushing the computational resources for boosted tree algorithms to their limits. XG Boost is a software library that may be downloaded and installed on a computer and then accessed through a variety of interfaces.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

D. Multinomial NB (MNB)

The Multinomial NB (MNB) in Natural Language Processing, an algorithmic is a possible learning method (NLP). Using the Bayes theorem, the software estimates a text's tag, such as an email or a news report.

E. Testing

System testing is based on the logical assumption that, if all components of the system are correct, system testing will be useful as a user-oriented vehicle prior to deployment. System testing finds faults, provides a recommendation to the administrator and alters the alteration, as well as checks the output's reliability. Before going live, the system is checked to see if the necessary software and hardware are in place to complete the project. To guarantee that this project is correct, it has passed the following testing methods.

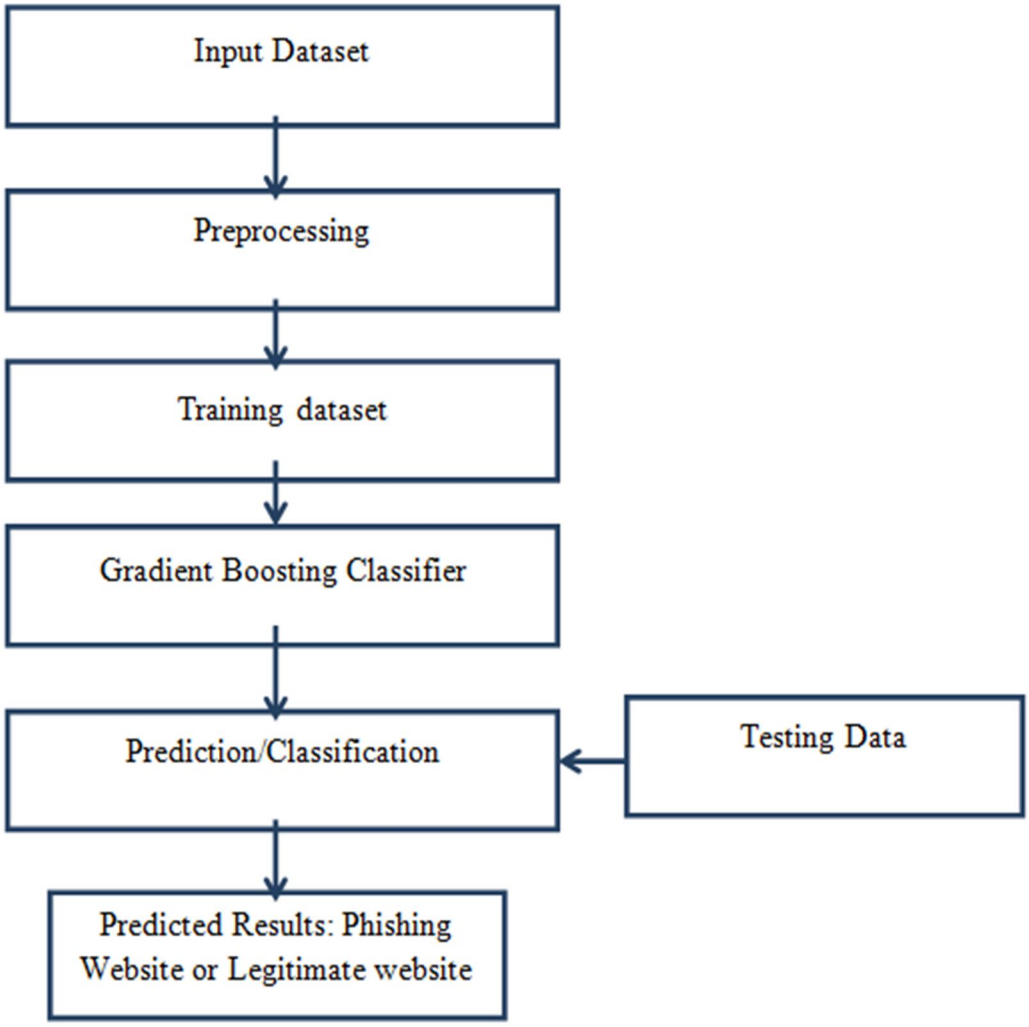


Figure 1. Graphical workflow of proposed models for detection of phishing websites

V. RESULT AND DISCUSSION

Phishing attacks are categorized according to Phisher's mechanism for trapping alleged users. Several forms of these attacks are keyloggers, DNS toxicity, Etc., . The initiation processes in social engineering include online blogs, short message services (SMS), social media platforms that use web 2.0 services, such as Facebook and Twitter, file-sharing services for peers, Voice over IP (VoIP) systems where the attackers use caller spoofing IDs . Each form of phishing has a little difference in how the process is carried out in order to defraud the unsuspecting consumer. E-mail phishing attacks occur when an attacker sends an e-mail with a link to potential users to direct them to phishing websites.

Classification of phishing attack techniques

Phishing websites are challenging to an organization and individual due to its similarities with the legitimate websites . presents the multiple forms of phishing attacks. Technical subterfuge refers to the attacks include Keylogging, DNS poisoning, and Malwares. In these attacks, attacker intends to gain the access through a tool / technique. On the one hand, users believe the network and on the other hand, the network is compromised by the attackers. Social engineering attacks include Spear phishing, Whaling, SMS, Vishing, and mobile applications. In these attacks, attackers focus on the group of people or an organization and trick them to use the phishing URL . Apart from these attacks, many new attacks are emerging exponentially as the technology evolves constantly.

VI. INPUT DESIGN AND OUTPUT DESIGN

A. *Input Design*

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

1) What data should be given as input?
2) How the data should be arranged or coded?
3) The dialog to guide the operating personnel in providing input.
4) Methods for preparing input validations and steps to follow when error occur.

B. *Objectives*

1) Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2) It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3) When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

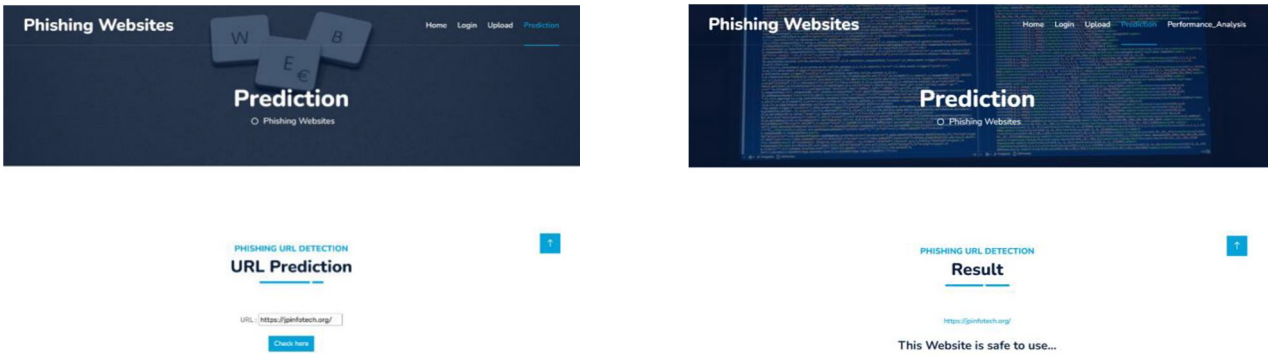
C. *Output Design*

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1) Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2) Select methods for presenting information.
3) Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

• Convey information about past activities, current status or projections of the
• Future.
• Signal important events, opportunities, problems, or warnings.
• Trigger an action.
• Confirm an action



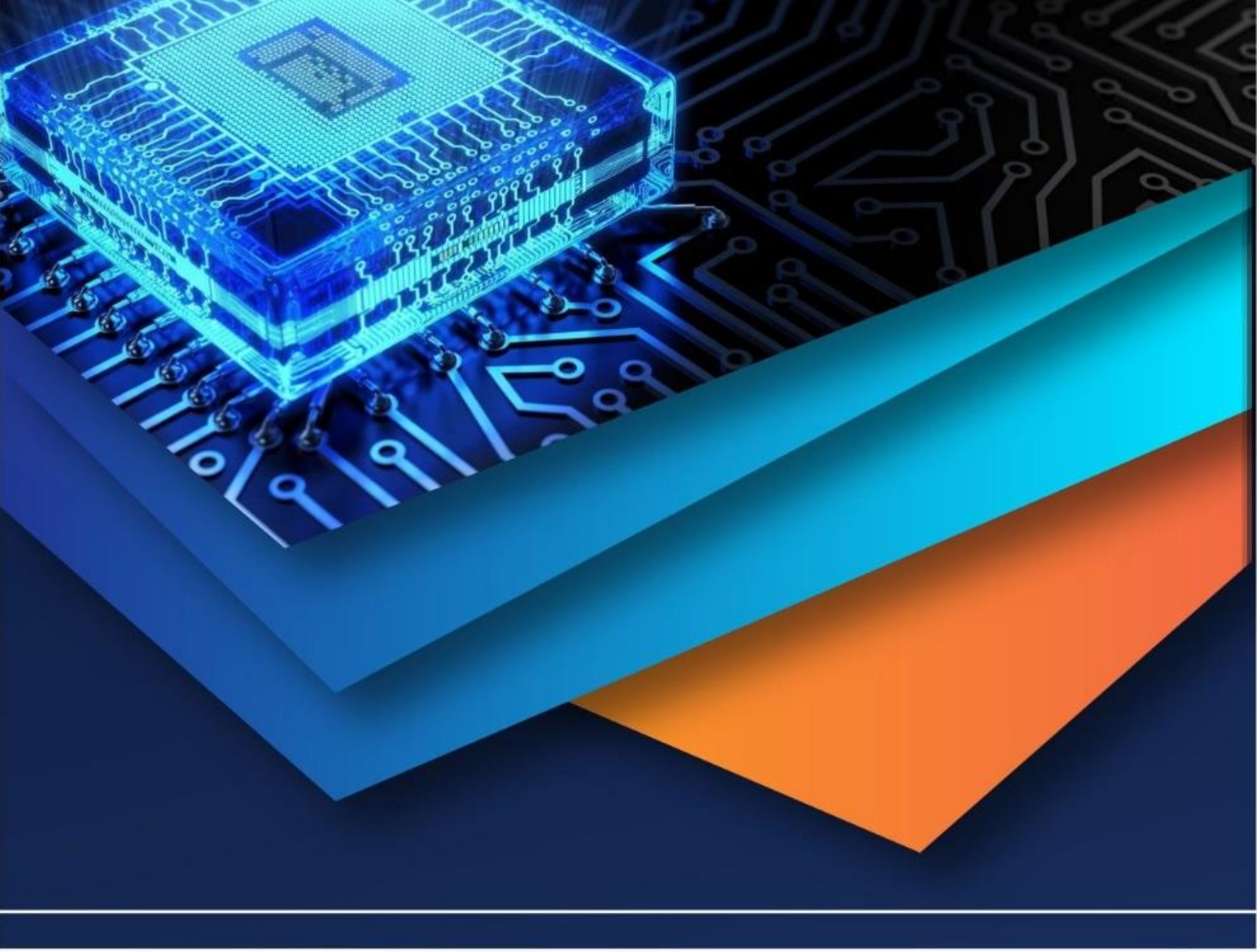
Output image

VII. CONCLUSION

It is remarkable that a good anti-phishing system should be able to predict phishing attacks in a reasonable amount of time. Accepting that having a good anti-phishing gadget available at a reasonable time is also necessary for expanding the scope of phishing site detection. The current system merely detects phishing websites using Gradient Boosting Classifier. We achieved 97% detection accuracy using Gradient Boosting Classifier with lowest false positive rate.

REFERENCES

[1] Introduction to Phishing Attack, https://en.wikipedia.org/wiki/Phishing.
[2] Andrew Jones, Mahmoud Khonji, Youssef Iraqi, Senior Member A Literature Review on Phishing Detection 2091-2121 in IEEE Communications Surveys and Tutorials, vol. 15, no. 4, 2013. 2013.
[3] Introduction to Machine Learning (Define, how it works, properties, etc) - https://en.wikipedia.org/wiki/Machine_learning
[4] M. El-Alfy, El-Sayed M. Probabilistic Neural Networks and K-Medoids Clustering are used to detect phishing websites. The Computer Journal, 60(12), pp.1745-1759, published in 2017.
[5] Ilango Krishnamurthi, R. Gowtham A system for detecting phishing websites that is both thorough and effective. pp. 23-37 in Computers & Security, Vol. 40, 2014.
[6] "Discoveringphishing target based on semantic link network," by Wenyin Liu et al. Future Generation Computer Systems, vol. 26.3, no. 3, pp. 381-388, 2010.
[7] Wenyin Liu et al., "Discovering phishing target via semantic link networks," Future Generation Computer Systems, vol. 26.3, no. 3, pp. 381- 388, 2010.
[8] How to identify Phishing Sites,-https://www.kaspersky.com/phishing-url-data-feed?reseller=gl_oem-ppc_leg_enterprise_sem_gen__b2b_google_ppc-ad_&utm_source=google&utm_medium=cpc&utm_campaign=oemppc&utm_content={ad_id}&utm_term=phishing%20attack&gad_source=1&gclid=CjwKCAiA1MCrBhAoEiwAC2d64WpDxakfGxnqkkJKOh-08Mv3Y0rZ49mVqnxZsPnRYrUjlzapNNZvvBoCTiQQAvD_BwE



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY