DETECTING PHISHING URL'S WEBSITES GRADIENT BOOSTING BASED ON MACHINE LEARNING

Ramdas Vankdothu[1] , L.K Suresh Kumar[2], P. Bhavani[1], U. Harish[1],

N. Teja Gopal Reddy[1], V. Rakshith[1]

[1]Department of Computer Science Engineering, Balaji Institute of Technology and Science, Warangal, Telangana.

[2]Department of Computer Science Engineering, University College of Engineering(A),Osmania University, Hyderabad

ABSTRACT: Phishing attack are one of the most prevalent cybersecurity threats phishing is most commonly used in social engineering in cyber-attack. Among the most common forms of cybersecurity threats, during phishing attack obtain based on passwords, financial details and other personal details from users by misleading them. Techniques to be identify phishing attack process on static blacklists or rule-based systems, the development of a machine learning techniques for detecting phishing URL's, be analysis of URLs and other relevant features. By leveraging diverse machine learning algorithms, used, like Random Forest, Support Vector Machines, Gradient Boosting. Users should have awareness of phishing Attack websites and have a blacklist of phishing attack websites which require knowledge of attack website being detected as phishing. Detect them in their early appearance, using machine learning algorithms with machine learning techniques users can easily identify the attack with this website. This website can be identifying real-time phishing websites by analysing the unseen URLs (https: //) security and safe and they predicting legitimacy based on the trained model.The proposed model was shown to be effective with an accuracy rate of97 percent. It's eliminating reliance on manually curated lists and static rules, making adaptable to new phishing techniques. so reduces phishing attacks by proactively, automated, and scalable detection. In this approach it can have an application by various users-individual, organizational, and platforms for cybersecurity benefiting users to enhance their online security and trust given to users.

Doi:10.48047/ijiee.2025.15.5.1

Keywords: Phishing detection, Gradient Boosting,URL analysis,Training data.

I. INTRODUCTION

Phishing attack websites are fraudulent online platforms designed to deceive users in to revealing sensitive information like usernames, password, & credit card details. Thismalicious site often legitimate attack websites.Phishing is the mostly used social engineering in cyber-attack.Through such attacks, the phisher targeting online users by tricking them in to revealing confidential information, with the purpose of using fraudulently.In order to avoid getting phished,users should have awareness of phishing Attack websites.They have a blacklist of phishing attack websites which requires the knowledge of attack websites being detected as phishing.To detect them in their early appearance, using machine learning and other algorithms.we are developing URL detection for phishing attack websites. It is very useful for everyone now-a-days to detect their websites and save sensitive information from attacker's.Detection of phishing sites using machine learning is essential to boost online security, users from identity theft, financial loss, and other forms of cybercrime[1-10].

Machine learning (ML) offers a promising approach to detecting phishing websites in real-time by analyzing various features that distinguish legitimate sites from malicious ones. Unlike traditional rule-based systems, which rely on predefined patterns, machine learning models can learn from large datasets of websites and identify subtle, often complex, patterns of phishing behavior. By training algorithms on features such as URL structure, HTML content, website traffic patterns, and domain reputation, ML-based systems can automatically classify websites as either legitimate or phishing with high accuracy[11-20].

Detection of phishing sites using machine learning is essential to boost online security, safeguard users from identity theft, financial loss, and other forms of cybercrime. As phishing techniques continue to evolve, using ML to remain ahead of attackers is a vital approach in the battle against cyber-attacks[21-34].

Doi:10.48047/ijiee.2025.15.5.1

Overall,phishing attacks this paper proposes an idea is toPhishingURL'S has become the most serious problem, harming individuals, corporations, andentirecountries. The availability of multiple services such as like online banking, entertainment, education,software downloading, and social networking has accelerated the Web's evolution in recent years.As a result, an immense amount of data is downloaded and also uploaded to the Internet continuously. The emails that claim to be from credible companies and agencies are employed as in socialengineering methods to lead consumers websites that trick users into providingfinancial data details, such as usernames and passwords. Technical approaches involve that use ofmalicious software on computers to hack and steal credentials directly,with systems frequently used tointercept users' online account usernames and passwords.

Types of Phishing Attacks

- **Email Phishing:**It is most prevalent condition, where attackers send deceptive emails pretending to be from legitimate organizations like banks or social media. These emails often contain malicious links or attachments designed to steal credentials or install malware.
- **Spear Phishing:**It is a more targeted attack aimed at specific individuals or groups. Attackers gather information about their targets to highly personalized emails, increasing the likelihood of success.
- **Whaling:** It is spearing phishing targeting notable figures like CEOs or executives. Hackers want to obtain confidential information or gain access to helpful company resources.
- **Smishing and Vishing:** These attacks use SMS messages smishingor phone calls to trick victims into revealing personal information or downloading malware.
- **Angler Phishing:** This involves attackers using social media to impersonate customer service accounts of reputable companies. They unsuspecting victims into sharing sensitive information or clicking malicious links.
- **URL Phishing:**URL Phishing is a type of phishing attack where malicious actors create fraudulent websites that closely mimic legitimate sites by using deceptive or

Doi:10.48047/ijiee.2025.15.5.1

misleading URLs. The goal is to trick users into thinking they are visiting a trusted site, prompting them to enter sensitive personal information, such as login credentials, financial details, or other confidential data. These URLs often appear very similar to those of legitimate websites but with slight alterations that are hard for the average user to detect.

II. LITERATURE SURVEY:

Recent studies different author's have did many studies, and many researchers have done many research to detect and predict phishing attacks based on different approaches at different times.some of the researchers have come up with visual features,Sahingoz et al. in (2020) author used methods are logistic regression, SVM, Random Forest, Decision trees and analysis of machine learning to be classifier for email phishing website detection based on extracted website and focusing on accuracy and performance.Jain et al. in (2021) while developing author used methods are random forest, XGBoost, LightGBM, and SMS detection accuracy using methodology in advanced Machine learning algorithms.Le, A. T., Nguyen, T. N., & Nguyen, Q. H. in (2022) and CNN, deep learning and authors developed deep learning applications in phishing website detection, strengths and limitations.Aburrous, M., Hossain, M. A., Dahal, N., & Thabtah, developed in (2023) Feature selection methods as Information Gain, Chi-Square and machine learning classifiers and SVM, Naive Bayes Analyzing the effectiveness of different feature selection techniques in improving the accuracy and efficiency of phishing website detection models.A-Shorafa et al. in (2024) enchased used methods are like ensemble learning, Advanced Feature Engineering and development of an intelligent phishing websites detection system developed a robust system that strengths of multiple classifiers and feature sets to high detection.Zhang et al. in (2019) author used methods are lexical features and decision tree and accuracy dataset and developed phishing email detection based on Lexical Analysis.Marchal et al. in (2012) and used

Doi:10.48047/ijiee.2025.15.5.1

Feature Selection and Support Vector Machine to Predictive Blacklisting and developed as Automatic Detection of Malicious Websites.

Whittaker et al. developed in (2010) used methods like Machine Learning (SVM), Large-Scale developed Automatic Classification of Phishing Web Pages.

The article proposed an idea enhancing to usersthat Machine learning is to analysing the URL like (HTTPS) for the detection of phishing attempts. It utilizes algorithms that analyse large datasets of malicious URLs. Features such as URL length, specific characters, domain age, and the use of HTTPS are adequate for determining the probability of a phishing attack. Some of the common supervised methods are logistic regression and random forests, Gradient boosting where the models are trained on labelled datasets with phishing and safe URLs. These systems are able to analysis the phishing attempts by implementing real-time analysis and adapting to the changing nature of methods used by scammers. Such systems can check data encountered URLs in seconds against the known learned URLs for phishing patterns. Deep learning and neural networks are increasingly taking prominence over traditional methods of detecting phishing websites due to their efficiency in identifying advanced phishing attack websites. Being able to learn on the go helps these systems tackle the ever-growing threat posed by malicious individuals on the internet.

It introduces a website for detecting phishing attack is based on collected datasets. Development of the proposed detecting phishing attackSo, we are working on the phishing attack detection website using some really useful datasets. These datasets include both safe and harmful (malicious) URLs, which are training our machine learning models. When we use feature engineering, and the URLs, like their length, if they include IP addresses. We also check out host details, like how long a domain has been registered, along with content specifics, like any suspicious activities to be analysis. we are using the website like user-friendly. Users can see URLs for quick analysis, and then the system gives the URL is a phishing attempt. We're using a backend stays up-to-date by retraining its model regularly with new phishing URLs, so it can analysis new threats as they pop up.

Doi:10.48047/ijiee.2025.15.5.1

Somevisualization tools to help users see the features we've detected and provide educational resources to boost their understanding of phishing, helping them stay safe online.

III. PROBLEM STATEMENT

Phishing attack websites process a major cybersecurity risk, users into revealing sensitive information such as login credentials, financial information, and personal data. Conventional detection mechanisms are based on blacklists and heuristic-based detection, which do not always detect newly spawned phishing sites. This project will design a machine learning-based URL phishing websites detection system that can scan website URLS and classify them as phishing in real-time.

IV. EXISITING SYSTEM

Existing phishing detection systems use multiple techniques to identify the malicious activity and different platforms, such as email, SMS, and file downloads. These systems to be analyze email message headers, sender addresses for inconsistencies in sender information and evaluating the overall structure of the email. Machine learning used algorithms are to used detect phishing website.

More over phishing detection in SMS messages to be involves and identifying red flags such as unexpected requests for sensitive information like suspicious sender numbers to fraudulent websites and Emails and SMS, phishing detection projects may be also focus on analyzing downloaded files or monitoring application behavior on a user's device.

Doi:10.48047/ijiee.2025.15.5.1

Phishing techniques are used like sandboxing and file to be analysis to identify malicious software attack and bypass traditional detection methods. By integrating the various detection techniques, these systems provide a defense against phishing attacks, even when attackers data to be security and analyze.

V. FLOW CHART

The paper research approachPhishing detection system based on URL analysis and machine learning aims to identify malicious websites by analyzing various URLS. The system collects URLs from different sources and extracts attributes like domain age, URL length, and special characters like HTTPS, it is a highly security.

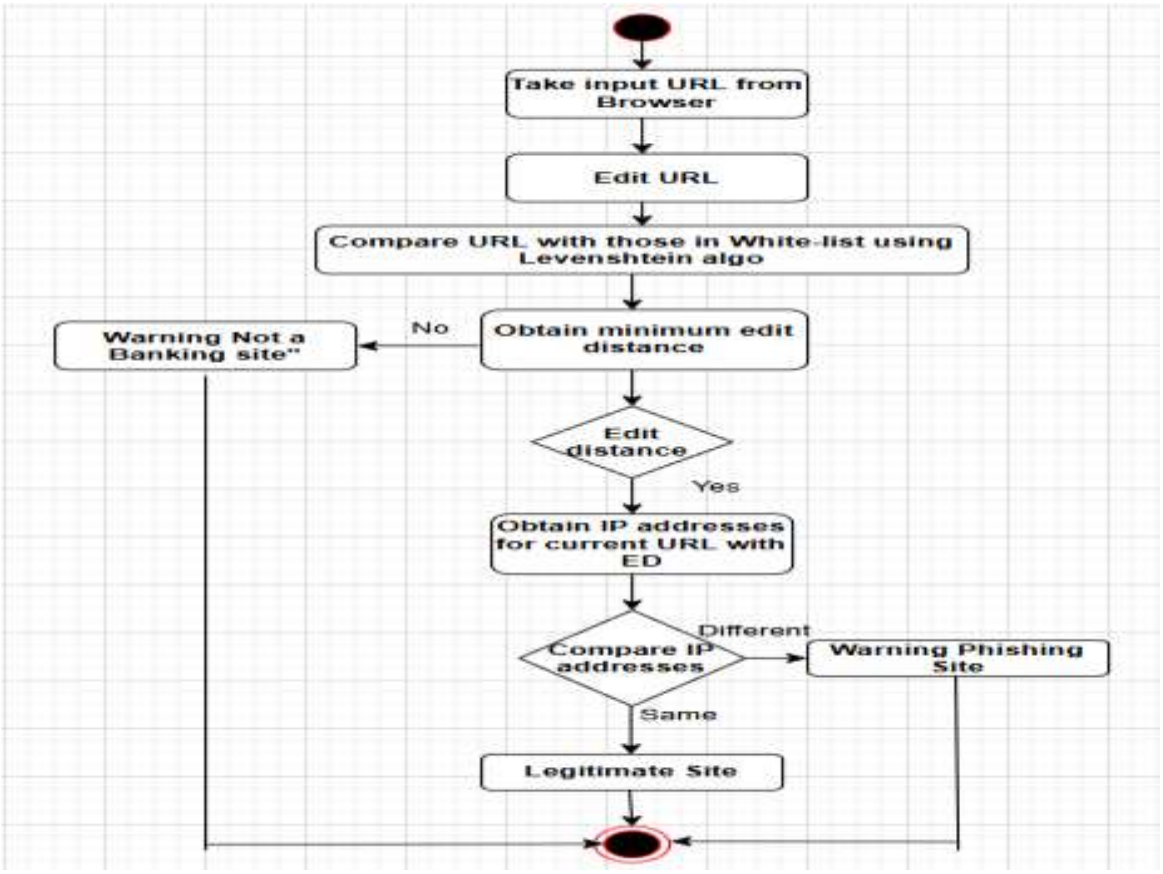

Fig: 4.1 Flow Chart

VI. PROPOSED SYSTEM

Phishing detection system based on URL analysis and machine learning aims to identify malicious websites by analyzing various URLS. The system collects URLs from different

Doi:10.48047/ijiee.2025.15.5.1

sources and extracts attributes such as domain age, URL length, Use of HTTPS, it is a highly security. A machine learning model, can be trained on a dataset and phishing URLs, classifies incoming URLs as safe or malicious activities. The model can be using algorithms like Random Forest, Support Vector Machines (SVM), or deep learning techniques to improve accuracy. Additionally, we using real-time feature extraction and analysis enable the system to detect zero-day phishing attacks. A web-based interface or browser extension can be integrated as allowing users to check URLs before using them. The system continuously updates its database with new threats using automated web and threat intelligence feeds. By machine learning and real-time detection, this approach enhances cybersecurity by providing a proactive defense against phishing attacks.

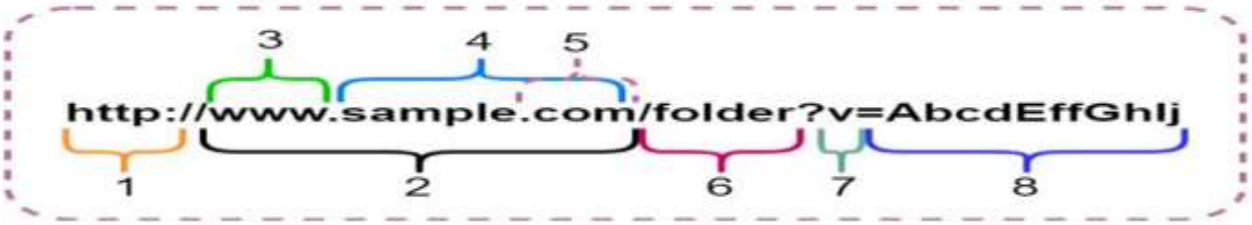

Fig: 6.1 URL is HTTP Unsafe Protocol

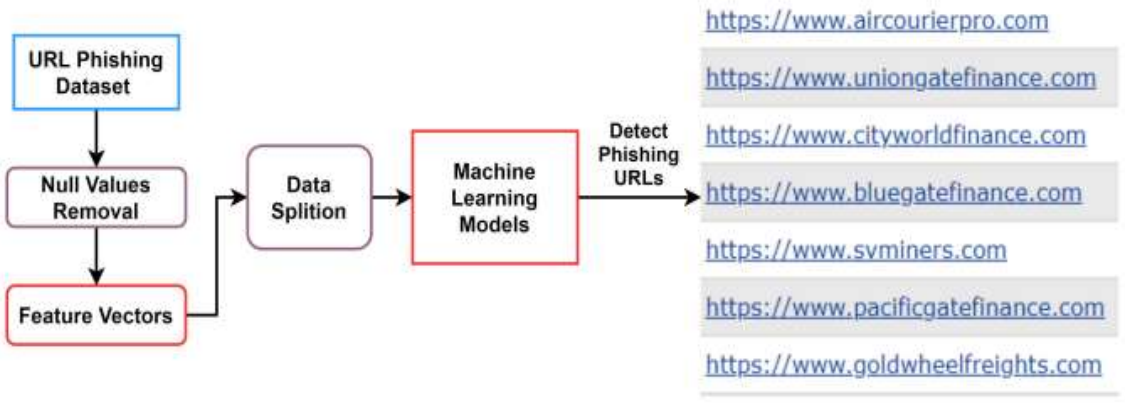

Fig: 6.2 Detection of phishing URLs and structure of proposed system.

ALGORITHMS:

Doi:10.48047/ijiee.2025.15.5.1

Random Forest:

Random Forest is an ensemble learning method that constructs multiple decision trees and combines their predictions. Each tree is built on a random subset of the data and features, increasing robustness and reducing overfitting. For URL detection, each tree analyses features like URL length, domain age, and presence of suspicious keywords, and outputs a classification. The final prediction is determined by a majority vote of all trees.

The Random Forest algorithm is an effective means of detecting phishing URLs, which is mainly because it can process complex and high-dimensional data. Fundamentally, it works by training a huge number of decision trees. Each tree is learned using a random subset of the training dataset, and also uses a random subset of available features. The addition model is important because it avoids the model overfitting to the training set, a usually issue with individual decision trees.When a new URL is for classification, the Random Forest algorithm sends it through the individual decision trees in the random forest. Each tree generates URLs for phishing or valid. Algorithm these predictions, often through a majority vote, to determine a final classification.

- Phishing detection system based on URL analysis and machine learning aims to identify malicious websites by analyzing various URLS. The system collects URLs from different sources and extracts attributes such as domain age, URL length, and special characters, use of HTTPS, it is a highly security.
- A machine learning model, can be trained on a dataset and phishing URLs, classifies incoming URLs as safe or malicious activities. The model can be using algorithms like Random Forest, Support Vector Machines (SVM) .

This ensemble technique greatly improves the accuracy and reliability of the model since it utilizes the strength of multiple trees in making the predictions, mitigating the influence of any one tree's error.

Doi:10.48047/ijiee.2025.15.5.1

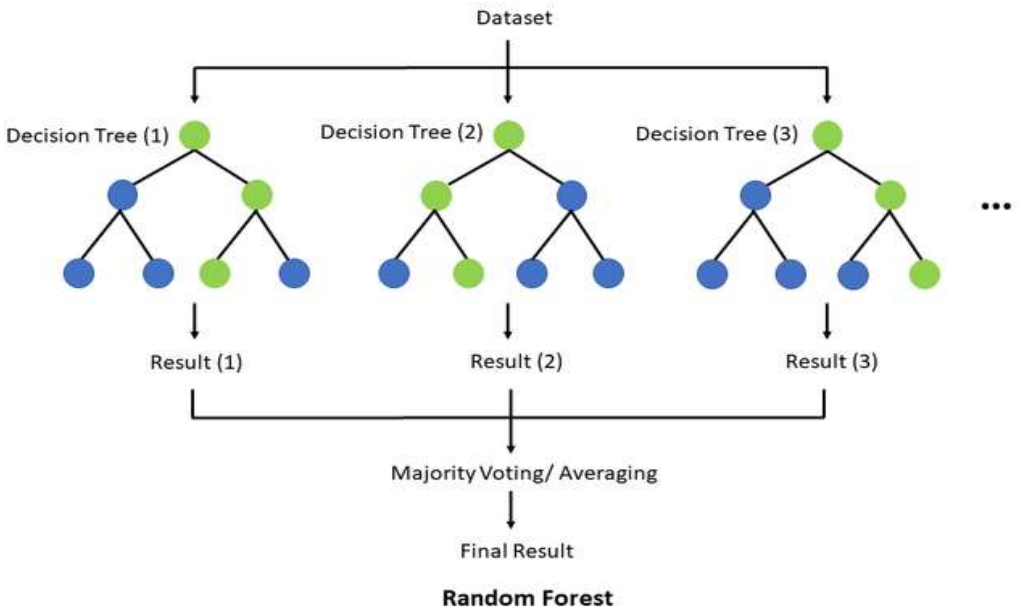

Fig: 6.3 Random Forest Working

Support Vector Machines (SVM):

Support Vector Machines to identifying phishing URLs by seeking an optimal hyperplane that discriminates best between genuine URLs and phishing URLs in a high-dimensional feature space. In the detection of phishing, SVM inspects different URL features, including length, existence of suspicious characters, and domain info, and transforms them into such a space. The algorithm is non-linear and using kernel functions so that it can be classify URLs correctly even when the difference between phishing and legitimate is complex. Most importantly, SVM tries to maximize the margin between the two classes, which improves the model's ability to generalize and minimizes the possibility of misclassification, making it a strong weapon against changing phishing strategies.

$$\left[\frac{1}{n}\sum_{i=1}^{n}\max\left(0, 1 - y_i(w \cdot x_i - b)\right)\right] + ||w||^2$$

where: w = weight vector, x = input vector, b = bias

Gradient Boosting Classifiers:

Doi:10.48047/ijiee.2025.15.5.1

Gradient Boosting Classifiers are the strong ensemble learning method that constructs a robust predictive model by ensembling the predictions of many weak models, most often decision trees. In the case of phishing URL detection, GBCs utilize major concept of training decision trees, where each tree is trying to rectify the mistakes of the previous tree. This sequential learning procedure targets the misclassified instances by previous trees, in essence, placing higher emphasis on the hard-to-classify URLs. This iterative optimization enables the model to continuously enhance its accuracy and identify intricate patterns in the data. In particular, when used for phishing URL detection, GBCs evaluate different features derived from URLs, including URL length, domain details, and HTTPS. The algorithm begins with a basic first model and then computes the errors committed by this model. The next decision trees are then trained to forecast these residuals, essentially learning to correct the errors of the previous trees. All the trees' predictions are then aggregated, typically through a weighted sum, to generate the final prediction. This enhancement process continues until a specified number of trees are constructed or a given level of performance has been attained**.**

K-Nearest Neighbours (KNN):

KNN is a straightforward but powerful algorithm that uses the training dataset's neighbouring URLs to classify URLs. KNN uses a distance metric such as the Euclidean distanceto determine the 'k' closest URLs neighbours when a new URL is presented. The majority class of the new URL's "k" neighbours is then used to classify it. KNN characteristics taken from URLs, including length, and domain information, in order to detect phishing attempts. The new URL is categorised as phishing if the vast majority of its closest neighbours have been flagged as such. A large 'k' can smooth out decision boundaries, while a small 'k' can result in noisy classifications.

Logistic Regression:

The logistic regression is also known as a statistical model that a URL is authentic or phishing. The linear combination of URL features is mapped to a probability value between 0 and 1 using a logistic function. The URL is labelled as phishing if the probability is higher than a predetermined threshold like 0.5. Logistic Regression is used

Doi:10.48047/ijiee.2025.15.5.1

in phishing detection to determine the correlation between URL characteristics and the probability of phishing. Each feature is given a weight that indicates how important it is for predicting phishing activity. Higher weights are given to features that have a strong correlation with phishing URLs.

The logistic regression calculated using:

$$p = \frac{1}{1 + e^{-(+b_1x_1 + b_2x_2 + \cdots + b_px_p)}}$$

where p = logistic model predicted probability, x = feature or attribute, b_i = changes in values of x.

VII. ADVANTAGES

- Automation of Feature Engineering
- Adaptability and Learning
- Real-time Detection Potential
- Handling Large Datasets
- Scalability
- Cost-Effective

VIII. RESULT

Detecting Phishing URL's Attack Website

Our machine learning project aimed to detect phishing URL's attacks identifying the malicious websites by analyzing various URLS. The system collects URLs from different sources and extracts attributes such as domain age, URL length, and special characters,

Doi:10.48047/ijiee.2025.15.5.1

use of HTTPS, it is a highly security. A machine learning model, can be trained on a dataset and phishing URLs, classifies incoming URLs as safe or malicious activities. The model can be using algorithms like Random Forest, Support Vector Machines (SVM), or deep learning techniques to improve accuracy. Additionally, we using real-time feature extraction and analysis enable the system to detect zero-day phishing attacks. A web-based interface or browser extension can be integrated as allowing users to check URLs before using them. The system continuously updates its database with new threats using automated web and threat intelligence feeds. By machine learning and real-time detection, this approach enhances cybersecurity by providing a proactive defense against phishing attacks.

A web-based interface or browser extension can be integrated as allowing users to check URLs before using them. The system continuously updates its database with new threats using automated web and threat intelligence feeds. By machine learning and real-time detection, this approach enhances cybersecurity by providing a proactive defense against phishing attacks.

Specifically, we observed that the model was particularly effectives and trained machine learning models.

Doi:10.48047/ijiee.2025.15.5.1

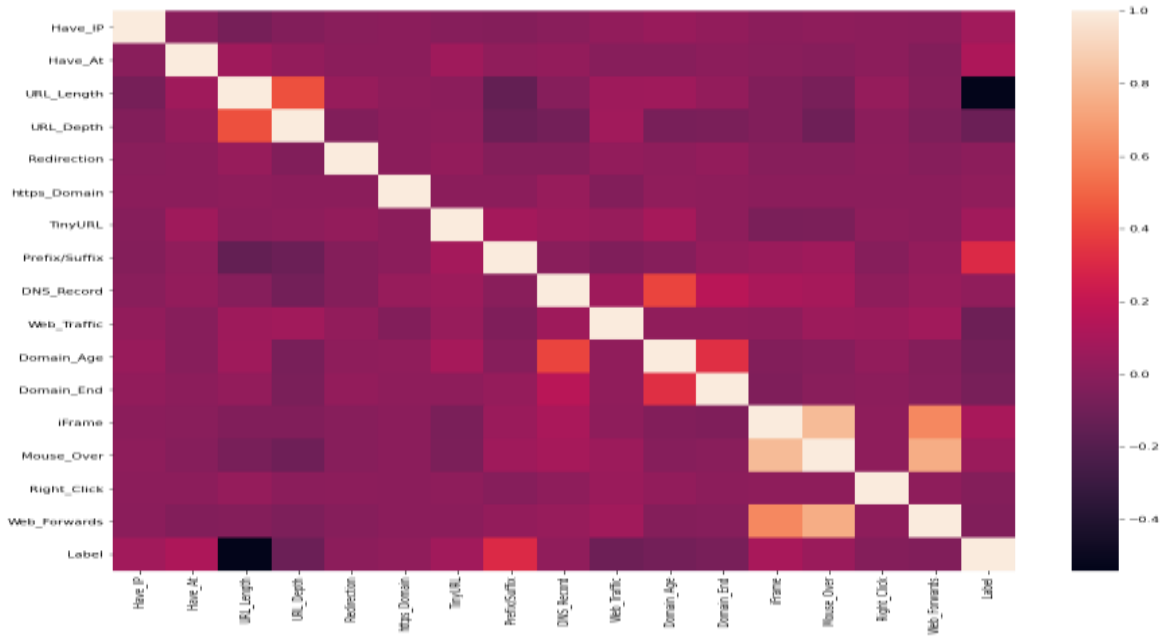

Fig: 8.1 Data visualization

The correlation matrix of a dataset that is website attributes, probably employed for phishing or malicious URL detection. The heatmap employs a color gradient to display correlation values, where lighter colors represent stronger positive correlations and darker colors represent stronger negative correlations. The diagonal, from top-left to bottom-right, is light white, representing perfectThere are a few important observations to note: "URL Length" has a high positive correlation with "Label," which could indicate that longer URLs tend to be more likely to be associated with the target category and thus possibly point to malicious websites. URL and also have moderate positive correlations with "Label," which means that URL shortening services can possibly be used to infer some characteristics of websites. On the other hand, "HTTPs Domain" has a negative correlation with "Label," which means that websites with HTTPS secure and safe. "Web Traffic" and "Domain Age" also have some correlation with "Label," implying that website traffic and domain age could be contributing factors.Other significant correlations are seen between "URL

Doi:10.48047/ijiee.2025.15.5.1

Length" and "URL Depth," which means longer URLs tend to have higher depth. "Domain Age" and "Domain End" also have a significant correlation, as it is reasonable since the age.

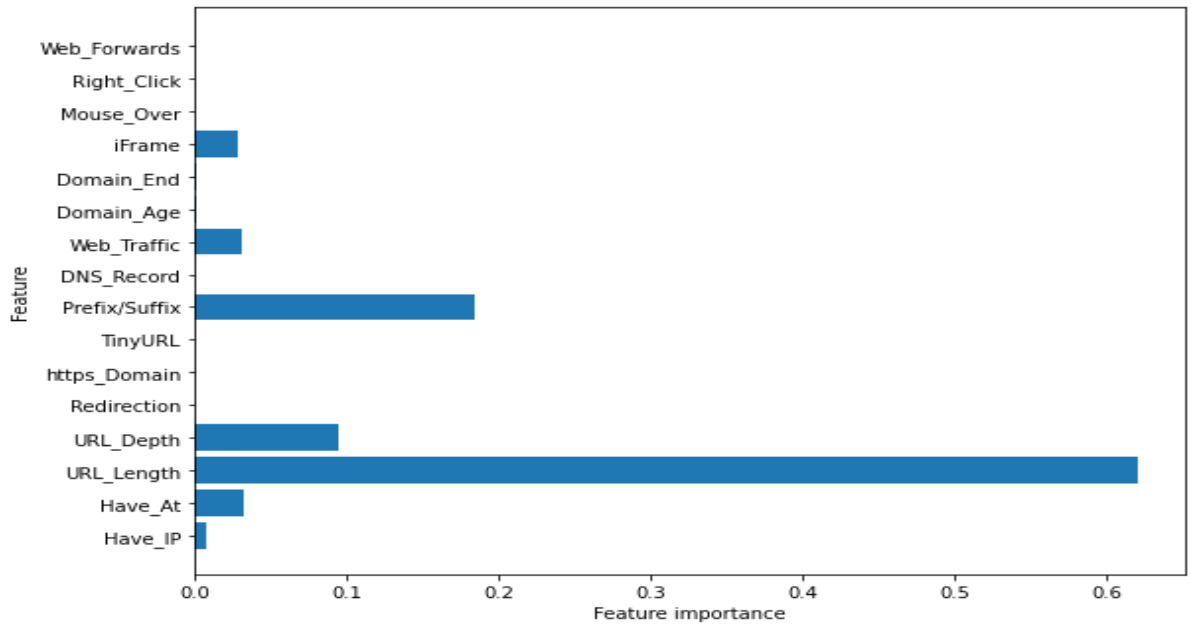

Fig: 8.2 Decision Tree Classifier

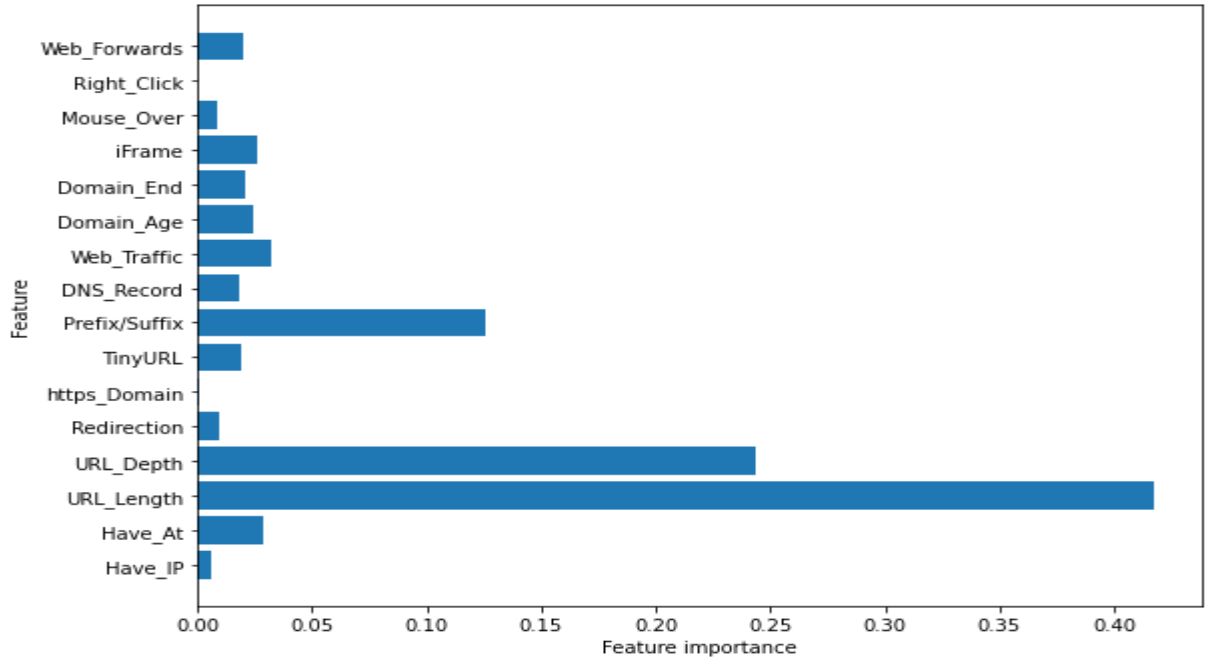

Fig: 8.3 Random Forest Classifier

Doi:10.48047/ijiee.2025.15.5.1

IX. CONCLUSION

Conclusion,project aims to “Detecting Phishing URL’s Attack Websites based on Machine Learning” we examined and analysis large dataset based on current situation we facing during problems in society now-a-days cyber-attacks are happening for that we are providing in our portal we are providing for people they can easily analysis URL’s. Bar graph visualization of the algorithm accuracy scores indicates the performance of various machine learning models in this context. Algorithms such as Random Forest, Support Vector Machines, Gradient Boosting, and were seen to perform consistently well in terms of accuracy rates, indicating that they can learn complex relationships and make correct predictions. The algorithms and fine-tuning their parameters for the best results.The proposed model was shown to be effective with an accuracy rate of 97 percentBycombining feature analysis, algorithm selection, and continuous improvement, we can strengthen our defences against this ever-evolving threat and create a safer online environment. The research should focus on developing more machine learning models, exploring real-time detection methods, and enhancing collaboration between cybersecurity experts and machine learning practitioners to stay ahead of malicious actors.

REFERENCE

1. Abuzuraiq A, Alkasassbeh M, Almseidin M (2020) Intelligent methods for accurately detecting phishing websites a research papers on the practice of big data analysis in cyber-attacks.
2. Gupta BB, Yadav K, Razzak I, Psannis K, Castiglione A, Chang X (2021) A novel approach for phishing E-mail detection using machine learning in a real-time environment a research Attack’s.
3. Aljofey, A., Jiang, Q., Rasool, A., Chen, H., Liu, W., Qu, Q., and Wang, Y. (2022). An effective detection approach for phishing websites using SMS based approach.
4. ResearchGate- discovered research papers by Sahingoz, R., Topaloglu, E., & Buber, N. (2015). Phishing website detection using hybrid features. This paper is foundational because it explored combining different types of features as SMS, E- mail based with machine learning.

Doi:10.48047/ijiee.2025.15.5.1

5. IEEE Journal- Toolan, M., & Caruana, M. (2016). Phishing Detection Using Machine Learning Techniques. This research is important because it directly compares many machine learning algorithms against one another for phishing detection.
6. Ali W (2017) Phishing website detection based on supervised machine learning with wrapper features selection. Int J Adv Comput Sci Appl 8(9):72–78 Breiman L (2001) Random forests. Mach Learn 45(1):5–32
7. Kumar A, Gupta JBB (2018) A machine learning based approach for phishing detection using hyperlinks information Number of Unique Phishing Sites Detected. J Ambient Compute.
8. Leng K et al (2019) A new hybrid ensemble feature selection framework for machine learning-based phishing detection system.
9. Alazab, M., Awad, A., & Mesleh, M. (2018). Phishing website detection using hybrid features and machine learning. Reinforces the trend of hybrid feature sets and explores more advanced machine learning classifiers.
10. Alzahrani, A., Alghamdi, A., & Alshehri, A. (2019). Phishing detection using ensemble learning techniques. Ensemble methods combine multiple models for better accuracy, research.
11. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" A Brain Tumor Identification and Classification Using Deep Learning based on CNN-LSTM Method" Computers and Electrical Engineering , 101 (2022) 107960
12. Ramdas Vankdothu,.Mohd Abdul Hameed "Adaptive features selection and EDNN based brain image recognition on the internet of medical things", Computers and Electrical Engineering , 103 (2022) 108338.
13. Ramdas Vankdothu,.Mohd Abdul Hameed,Ayesha Ameen,Raheem,Unnisa " Brain image identification and classification on Internet of Medical Things in healthcare system using support value based deep neural network" Computers and Electrical Engineering,102(2022) 108196.
14. Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor segmentation of MR images using SVM and fuzzy classifier in machine learning" Measurement: Sensors Journal,Volume 24, 2022, 100440 .
15. Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor MRI images identification and classification based on the recurrent convolutional neural network" Measurement: Sensors Journal,Volume 24, 2022, 100412 .
16. Bhukya Madhu, M.Venu Gopala Chari, Ramdas Vankdothu,.Arun Kumar Silivery,Veerender Aerranagula " Intrusion detection models for IOT networks via deep learning approaches "

Doi:10.48047/ijiee.2025.15.5.1

Measurement: Sensors Journal,Volume 25, 2022, 100641

17. Mohd Thousif Ahemad ,Mohd Abdul Hameed, Ramdas Vankdothu" COVID-19 detection and classification for machine learning methods using human genomic data" Measurement: Sensors Journal,Volume 24, 2022, 100537
18. S. Rakesh [a], NagaratnaP. Hegde [b], M. VenuGopalachari [c], D. Jayaram [c], Bhukya Madhu [d], Mo hdAbdul Hameed [a], Ramdas Vankdothu [e], L.K. Suresh Kumar "Moving object detection using modified GMM based background subtraction" Measurement: Sensors ,Journal,Volume 30, 2023, 100898
19. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Efficient Detection of Brain Tumor Using Unsupervised Modified Deep Belief Network in Big Data" Journal of Adv Research in Dynamical & Control Systems, Vol. 12, 2020.
20. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Internet of Medical Things of Brain Image Recognition Algorithm and High Performance Computing by Convolutional Neural Network" International Journal of Advanced Science and Technology, Vol. 29, No. 6, (2020), pp. 2875 – 2881
21. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Convolutional Neural Network-Based Brain Image Recognition Algorithm And High-Performance Computing", Journal Of Critical Reviews,Vol 7, Issue 08, 2020(Scopus Indexed)
22. Ramdas Vankdothu, Dr.Mohd Abdul Hameed "A Security Applicable with Deep Learning Algorithm for Big Data Analysis",Test Engineering & Management Journal,January-February 2020
23. Ramdas Vankdothu, G. Shyama Chandra Prasad " A Study on Privacy Applicable Deep Learning Schemes for Big Data" Complexity International Journal, Volume 23, Issue 2, July-August 2019
24. Ramdas Vankdothu, Dr.Mohd Abdul Hameed, Husnah Fatima " Brain Image Recognition using Internet of Medical Things based Support Value based Adaptive Deep Neural Network" The International journal of analytical and experimental modal analysis, Volume XII, Issue IV, April/2020
25. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" Adaptive Features Selection and EDNN based Brain Image Recognition In Internet Of Medical Things " Journal of Engineering Sciences, Vol 11,Issue 4 , April/ 2020(UGC Care Journal)
26. Ramdas Vankdothu, Dr.Mohd Abdul Hameed " Implementation of a Privacy based Deep Learning Algorithm for Big Data Analytics", Complexity International Journal , Volume

Doi:10.48047/ijiee.2025.15.5.1

24, Issue 01, Jan 2020

27. Ramdas Vankdothu, G. Shyama Chandra Prasad" A Survey On Big Data Analytics: Challenges, Open Research Issues and Tools" International Journal For Innovative Engineering and Management Research,Vol 08 Issue08, Aug 2019.
28. Vankdothu, R., Hameed, M.A. "An Effective Congestion and Interference Secure Routing Protocol for Internet of Things Applications in Wireless Sensor Network " Wireless Personal Communication Journal 140, 143–161 (2025)
29. Vankdothu, R., Bhukya, H. & Bhukya, R.R. "Hybrid TDR-MI Based Wireless Sensor Network for Underground Water Pipeline Leakage Detection and Localization Using Pressure Residuals and Classifiers Wireless Personal Communications 139, 803–823 (2024).
30. Vankdothu, R., Cheng, X. "Energy Efficient TDMA and Secure Based MAC Protocol for WSN Using AQL Coding and ASGWI Clustering". Wireless Personal Communications 136, 2125–2143 (2024)
31. Vankdothu, R., Hameed, M.A., Fatima, H. *et al.* Multicast Scaling in Heterogeneous Wireless Sensor Networks for Security and Time Efficiency. Wireless Personal Communications (2025).
32. Vankdothu, R., Hameed, M.A., Fatima, H. *et al.* Multicast Scaling in Heterogeneous Wireless Sensor Networks for Security and Time Efficiency. Wireless Personal Communications (2025)
33. Ramdas Vankdothu, Mohd Abdul Hameed" Brain MRI Images for Tumor Detection using Storage Optimization Technique",Mobile Radio Communications and 5G Networks,Lecture Notes in Networks and Systems,425-437, Springer .
34. Bandi Krishna , Ramdas Vankdothu , Varun Revuri and B. Prashanth" A brain tumor identification using convolution neural network in the deep learning" MATEC Web of Conferences 392, 01131 (2024) ,https://doi.org/10.1051/matecconf/202439201131 ICMED 2024

Doi:10.48047/ijiee.2025.15.5.1

XI. BIBILOGRAPHY:

I'm P. Bhavani I am currently in my 8th semester of computer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. MY research interest is done based on"MACHINE LEARNING APPROCH FOR DETECTING PHISHING URL'S ATTACK WEBSITE".

I'm U. Harish I am currently in my 8th semester of computer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. MY research interest is done based on"MACHINE LEARNING APPROCH FOR DETECTING PHISHING URL'S ATTACK WEBSITE".

I'm N. Teja Gopal ReddyI am currently in my 8th semester of computer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. MY research interest is done based on"MACHINE

Doi:10.48047/ijiee.2025.15.5.1

LEARNING APPROCH FOR DETECTING PHISHING URL'S ATTACK WEBSITE".

I'm V. Rakshith I am currently in my 8th semester of computer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. MY research interest is done based on"MACHINE LEARNING APPROCH FOR DETECTING PHISHING URL'S ATTACK WEBSITE".

Doi:10.48047/ijiee.2025.15.5.1