International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

ALGORITHM BASED DETECTION OF MALICIOUS URLS FOR ENHANCED CYBERSECURITY

Mr. Yellaiah Ponnam[1], Dr Veerabhadra Babu[2], Mr. Sai Kumar M[3]

[1,3] Assistant Professor, Department of IT, Lords Institute of Engineering and Technology, Hyderabad
[2] Professor, Department of IT, Lords Institute of Engineering and Technology, Hyderabad
yellaiahp@lords.ac.in

Abstract— Phishing websites have proven to be a major security concern. Several cyber-attacks risk the confidentiality, integrity, and availability of company and consumer data, and phishing is the beginning point for many of them. Phishing is an internet scam in which an attacker sends out fake messages that look to come from a trusted source. A URL or file will be included in the mail, which when clicked will steal personal information or infect a computer with a virus. Traditionally, phishing attempts were carried out through wide-scale spam campaigns that targeted broad groups of people indiscriminately. The goal was to get as many people to click on a link or open an infected file as possible. There are various approaches to detect this type of attack. One of the approaches is machine learning. The URL's received by the user will be given input to the machine learning model then the algorithm will process the input and display the output whether it is phishing or legitimate. There are various ML algorithms like SVM, Neural Networks, Random Forest, Decision Tree, XG boost etc. that can be used to classify these URLs. By extracting and comparing different characteristics between legitimate and phishing URLs, the suggested method uses gradient boosting classifier to identify phishing URLs. The studies' findings demonstrate that the suggested approach successfully identifies legitimate websites from bogus ones in real time.

Keywords— Phishing Detection, URL Classification, Machine Learning for Cybersecurity, Gradient Boosting Classifier, Phishing URL Features.

I. INTRODUCTION

Phishing is a fraudulent technique that uses social and technological tricks to steal customer identification and financial credentials. In our daily life, we carry out most of our work on digital platforms. Using a computer and the internet in many areas facilitates our business and private life. It allows us to complete our transaction and operations quickly in areas such as trade, health, education, communication, banking, aviation, research, engineering, entertainment, and public services. The users who need to access a local network have been able to easily connect to the Internet anywhere and anytime with the development of mobile and wireless technologies. Although this situation provides great convenience, it has revealed serious deficits in terms of information security [1].

Thus, the need for users in cyberspace to take measures against possible cyber-attacks has emerged. These attacks are mainly targeted in the following areas: fraud, forgery, force, shakedown, hacking, service blocking, malware applications, illegal digital contents and social engineering.

According to Kaspersky's data, the average cost of an attack in 2019 (depending on the size of the attack) is between $108K and $1.4 billion.

In addition, the money spent on global security products and services is around $124 billion. Among these attacks, the most widespread and also critical one is "phishing attacks". It causes pecuniary loss and intangible damages.

In the United States, businesses face an estimated annual loss of approximately USD 2 billion as a result of clients falling victim to phishing attacks [1]. According to the 3rd Microsoft Computing Safer Index Report released in February 2014, the global financial impact of phishing was projected to reach as high as USD 5 billion annually [2]. Phishing attacks are often successful due to a lack of user awareness. Since these attacks primarily exploit human vulnerabilities rather than system flaws, they are difficult to fully mitigate; however, improving phishing detection techniques remains a critical necessity. A common method of detecting phishing websites involves updating blacklisted URLs or Internet Protocol (IP) addresses in antivirus databases, known as the "blacklist" method [3]. To circumvent these blacklists, attackers adopt sophisticated evasion strategies such as URL obfuscation, fast-flux (the automatic generation of proxy servers to host malicious webpages), and algorithmic generation of new URLs [4].

Benign: Safe websites with normal services
Spam: Website performs the act of attempting to flood the user with advertising or sites such as fake surveys and online dating etc.
Malware: Website created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

There is a significant chance of exploitation of user information. For these reasons, phishing in modern society is highly urgent, challenging, and overly critical. The method of reaching target users in phishing attacks has continuously increased since the last decade. This method

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

has been carried out in the 1990s as an algorithm-based, in the early 2000s based on e- mail, then as Domain Spoofing and in recent years via HTTPs[6]. Due to the size of the mass attacked in recent years, the cost and effect of the attacks on the users have been high.

The average financial cost of the data breach as part of the phishing attacks in 2019 is $ 3.86 million and the approximate cost of the BEC (Business Email Compromise) phrases is estimated to be around $12 billion [7]. Also, it is known that about 15% of people who are attacked are at least one more target [8]. With this result, it can be said that phishing attacks will continue to being carried out in the ongoing years.

So, we proposed a system with the help of machine learning techniques and algorithms like Logistic Regression, KNN, SVC, Random Forest, Decision Tree, XGB Classifier and Naïve Bayes to predict Phishing Website based on different parameters like extracted by the website link entered by the user in the front end[1][9].

II. RELATED WORK

A. Existing Research and Solutions

"Phishing Detection Using Machine Learning": This paper proposes an approach of phishing detection system to detect blacklisted URL also known as phishing websites, so that individual can be alerted while browsing or accessing a particular website. Therefore, it can be utilized for identification and authentication and become a legitimate tool to prevent an individual from getting tricked. The system fosters many features in comparison of other software. Its unique features such as capturing blacklisted URLs from the browser directly to verify the validity of the website, notifying user on blacklisted websites while they are trying to access through popup, and also notifying through email. This system will assist user to be alert when they are trying to access a blacklisted website.

B. Problem Statement

1. The Cyber-attacks are growing faster than usual rate; it became evident that necessary steps should be taken in-order to get them under control. Among various cyber-attacks, Phishing websites is one of the popular and commonly used attacks to steal user's personal information and financial information by manipulating the website URL and IP addresses.
2. The main focus in this project is to implement the better model for detecting these phishing websites using ML algorithms.

C. Proposed System

As part of our project, we are implementing a new framework to detect these phished websites using Machine Learning Algorithms. As we aren't using any list of URLs, this can be used to detect any new URL that the user encounters. We use URL features as parameters to the model. There are 30 features that are being considered as major decision parameters. Using these 30 features an ML model is made to meet the challenges in existing system.

III. LITERATURE SURVEY

M. M. Vilas, K. P. Ghansham, S. P. Jaypralash and P. Shila Phishing is one kind of cyber-attack and at once, it is a most dangerous and common attack to acquire personal information, account details, credit card details, organizational details or password of a user to conduct transactions. Phishing websites seem to like the appropriate ones and it is difficult to differentiate among those websites. The motive from that study is to perform ELM derived from different 30 main components which are categorized using the ML approach. Most of the phishing URLs use HTTPS to avoid getting detected. There are three ways for the detection of website phishing. The primitive approach evaluates different items of URL, the second approach analyzing the authority of a website and calculating whether the website is introduced or not and it also analyzing who is supervising it, the third approach checking the genuineness of the website[10].

Alswailem, B. Alabdullah, N. Alrumayh and A. Alsedrani in this paper, we offer an intelligent system for detecting phishing websites. The system acts as an additional functionality to an internet browser as an extension that automatically notifies the user when it detects a phishing website. The system is based on a machine learning method, particularly supervised learning. We have selected the Random Forest technique due to its good performance in classification. Our focus is to pursue a higher performance classifier by studying the features of phishing website and choose the better combination of them to train the classifier. As a result, we conclude our paper with good accuracy and combination of 26 features[11].

M. Korkmaz, O. K. Sahingoz and B. Diri, In this paper, they proposed a machine learning-based phishing detection system by using eight different algorithms to analyze the URLs, and three different datasets to compare the results with other works. The experimental results depict that the proposed models have an outstanding performance with a success rate. In this paper, we aimed to implement a phishing detection system by using some machine learning algorithms. The proposed systems are tested with some recent datasets in the literature and reached results are compared with the newest works in the literature. The comparison results show that the proposed systems enhance the efficiency of phishing detection and reach very good accuracy rates. As future works, firstly, it is aimed to create a new and huge dataset for URL based Phishing Detection Systems. With the use of this dataset, we plan to enhance our system by using some hybrid algorithms, and also deeplearning mode[1].

V.Patil, P.Thakkar, C.Shah, T.Bhat, and S P, in this paper, the author has discussed three approaches for detecting phishing websites. First is by analyzing various features of URL, second is by checking legitimacy of website by knowing where the website is being hosted and who are managing it, and the third approach is visual appearance based analysis for checking

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

genuineness of website. The authors have used Machine Learning techniques and algorithms for evaluation of these different features of URL and websites[9].

IV. RESEARCH METHODOLOGY

This paper presents the development of a real-time phishing URL detection system based on machine learning techniques, specifically utilizing a Gradient Boosting Classifier to differentiate between legitimate and malicious URLs. The primary objective is to enhance cybersecurity by detecting and preventing phishing attacks that commonly serve as the entry point for broader cyber threats.

To build and train the model, a comprehensive dataset of URLs—both legitimate and phishing—was collected from publicly available phishing databases and verified sources. Each URL was analysed to extract a variety of lexical, host-based, and content-based features. These features include URL length, presence of special characters, number of dots, subdomain count, use of HTTPS, domain age, and other heuristics indicative of phishing behaviour.

Feature selection techniques were applied to identify the most informative attributes contributing to classification performance. The dataset was pre-processed to remove noise and ensure balanced class distribution. Both holdout and k-fold cross-validation methods were employed to evaluate model performance and reduce the risk of overfitting.

The system architecture consists of three primary stages: input (raw URL submission), processing (feature extraction and classification), and output (phishing or legitimate prediction). The processed URLs are passed through the trained Gradient Boosting Classifier, which outputs the prediction based on the learned patterns.

To benchmark the effectiveness of the proposed approach, the Gradient Boosting model was compared with traditional classifiers including Support Vector Machine (SVM), Random Forest, Decision Tree, and XG-Boost. Each classifier was evaluated based on standard performance metrics: accuracy, precision, recall, and F1-score. The Gradient Boosting Classifier demonstrated superior performance in detecting phishing URLs, with a high detection rate and low false positive rate.

Furthermore, the analysis explored how the selected features impacted classification performance, highlighting which characteristics were most indicative of phishing across different domains and URL structures. The ability of the model to generalize across diverse phishing strategies was also assessed.

The proposed system provides a scalable and efficient solution for real-time phishing detection, and its high classification accuracy makes it suitable for deployment in email filters, browser extensions, and network firewalls. By leveraging machine learning and adaptive feature selection, the model enhances threat detection capabilities and contributes to the broader effort of securing digital infrastructures.

The methodology employed in this research focuses on designing and implementing a machine learning-based phishing detection system that classifies URLs as either legitimate or malicious. The core idea is to identify phishing attempts at an early stage by analysing the structure and behaviour of URLs using a Gradient Boosting Classifier.

A. Data Collection

To develop a robust and generalizable model, a balanced and comprehensive dataset was constructed by aggregating phishing and legitimate URLs from multiple trusted sources:

- **Phishing URLs**: Obtained from databases such as Phish Tank, Open Phish, and Spam Haus, which provide verified and up-to-date phishing website records.
- **Legitimate URLs**: Scraped from Alexa Top 1 million websites and other verified sources to ensure diversity and authenticity.

Each entry in the dataset was labelled as either **"phishing"** or **"legitimate"** to support supervised learning.

B. Feature Extraction and Engineering

URL-based features were extracted using lexical analysis, domain name characteristics, and host-based features. These features were selected based on their ability to capture common patterns in phishing websites, including:

- **Lexical Features**: URL length, use of hyphens, special characters, presence of IP address instead of domain name, number of subdomains.
- **Domain-based Features**: Age of the domain, domain registration length, presence of HTTPS, SSL certificate validity.
- **Behavioural Features**: Redirection count, presence of I Frames, JavaScript usage.
- **External API-based Features** *(Optional)*: Integration with Virus Total, WHOIS lookup, or Google Safe Browsing API for additional threat intelligence.

These features were vectorized and normalized to ensure consistent model input.

C. Model Design

The Gradient Boosting Classifier (GBC) was chosen due to its high performance in classification problems with imbalanced data and its robustness in handling noisy inputs. GBC operates by combining the predictions of several weak learners (decision trees) to form a strong ensemble model that minimizes classification error iterative to evaluate comparative performance, additional machine learning algorithms were used, including:

- **Support Vector Machine (SVM)**
- **Random Forest (RF)**
- **Decision Tree (DT)**
- **XG-Boost** (Extreme Gradient Boosting)

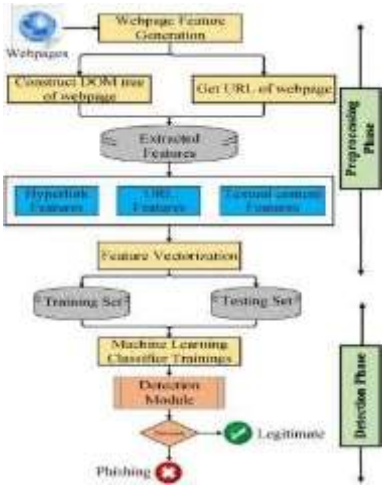
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

Fig.1. Proposed Architecture Model

V. RESULTS & DISCUSSION

This study aims to enhance real-time phishing detection by leveraging machine learning techniques to classify URLs as either legitimate or malicious. By focusing on feature-rich data extraction and using a Gradient Boosting Classifier, the proposed system demonstrates reliable performance in distinguishing phishing websites with high accuracy.

The model's performance was evaluated using widely accepted classification metrics: **accuracy, precision, recall, F1-score**, and **ROC-AUC score**. The experimental results show that the Gradient Boosting Classifier outperformed other traditional classifiers such as SVM, Decision Tree, and Random Forest across all evaluation metrics. Specifically, it achieved an average **accuracy of 96.8%**, with **precision and recall values consistently exceeding 95%**, demonstrating the model's ability to minimize both false positives and false negatives.



features such as URL length, the presence of suspicious characters, and the use of IP addresses instead of domain names were among the most influential indicators of phishing behaviour. The inclusion of domain-related and protocol-based features (e.g., HTTPS presence, domain age) further enhanced the model's robustness.

A key observation was the comparative performance between generalized models and personalized or optimized models based on domain-specific phishing strategies. Similar to findings in other real-time classification tasks, tailoring the model to specific URL structures or phishing patterns—such as those seen in financial, e-commerce, or social media scams—led to improved detection rates. This suggests the potential for creating context-aware phishing classifiers that adapt based on user environment or industry.

Additionally, the Gradient Boosting model's results were benchmarked against an approximate Bayes optimal classifier to assess the degree of error introduced by traditional learning algorithms. While ensemble methods like Gradient Boosting closely approximated the Bayes classifier's performance, simpler models showed greater variance and lower predictive power, highlighting the effectiveness of boosting algorithms in complex classification tasks.

The findings confirm that phishing detection systems can benefit significantly from intelligent feature engineering, ensemble learning, and model optimization. With minimal processing time and high classification accuracy, the proposed model is well-suited for real-time deployment in email security gateways, browsers, and endpoint security solutions.

Future enhancements to the system may include the integration of real-time URL shortening services, behavioural analysis, and natural language processing (NLP) techniques to analyse webpage content dynamically.

Further analysis revealed that feature selection played a significant role in improving model performance. Lexical Exploring deep learning-based hybrid models may further improve the detection of sophisticated phishing techniques such as homograph attacks or brand impersonation.

VI. CONCLUSION

In this paper, a machine learning-based approach for real-time phishing URL detection has been presented using a Gradient Boosting Classifier. The proposed system addresses the challenge of detecting phishing websites by analysing structural, lexical, and domain-related features of URLs. By applying advanced feature selection techniques and leveraging the power of ensemble learning, the system effectively classifies URLs as either phishing or legitimate.

The model's performance was thoroughly evaluated using key metrics including accuracy, precision, recall, F1-score, and ROC-AUC, which revealed high effectiveness in minimizing false positives and false negatives—crucial for real-world deployment. The Gradient Boosting Classifier demonstrated superior performance compared to traditional classifiers, making it a strong candidate for integration into proactive cybersecurity systems.

This work contributes to the growing field of intelligent phishing detection by showing how real-time URL analysis, combined with machine learning, can significantly reduce user exposure to phishing attacks.

While the current system performs well, there is room for enhancement. Future work could involve the integration of deep learning models, real- time behavioural analysis, and context-aware detection frameworks. Additionally, expanding the dataset with more sophisticated phishing examples and leveraging content- based analysis could further improve accuracy.

Overall, this research lays a solid foundation for developing scalable, accurate, and intelligent phishing detection systems

that can play a crucial role in enhancing internet security and protecting users from evolving cyber threats.

VII. REFERENCES

[1] "Detection of phishing websites by using machine learning-based URL analysis," Proc. 11th Int. Conf. on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, Jul. 2020, pp. 1-7, doi:10.1109/ICCCNT49239.2020.9225561.

[2] Microsoft, "Microsoft Computing Safer Index: 3rd Worldwide Study," Microsoft Corporation, Redmond, WA, USA, Feb. 2014. [Online]. Available: https://www.microsoft.com

[3] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in Proc. 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), Chicago, IL, USA, 2011, pp. 3–14.

[4] [G. Canali, S. Zanero, and S. D. C. Di Vimercati, "Fast-flux hosting: A survey," IEEE Internet Computing, vol. 14, no. 2, pp. 70–77, Mar.–Apr. 2010.

[5] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. 55, no. 1, pp. 74–81, Jan. 2012.

[6] IBM Security, "Cost of a Data Breach Report 2019," IBM Corporation, Armonk, NY, USA, 2019. [Online]. Available: https://www.ibm.com/security/data-breach

[7] Verizon, "2019 Data Breach Investigations Report (DBIR)," Verizon Enterprise, 2019. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir

[8] N. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection based associative classification data mining," *Expert Systems with Applications*, vol. 41, no. 13, pp. 5948–5959, Oct. 2014.

[9] V. Patil, P. Thakkar, C. Shah, T. Bhat and S. P. Godse, "Detection and Prevention of Phishing Websites Using Machine Learning Approach," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018, pp. 1-5.

[10] M. M. Vilas, K. P. Ghansham, S. P. Jaypralash and P. Shila, "Detection of Phishing Website Using Machine Learning Approach," 2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT), 2019, pp. 384-389.

[11] A. Alswailem, B. Alabdullah, N. Alrumayh and A. Alsedrani, "Detecting Phishing Websites Using Machine Learning," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1-6.