WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Website URL Attack and Email Spam Detection using ML

Soniya Raju Jadhav

Rani Channamma University, Belagavi

ABSTRACT

The "Website URL Attack and Email Spam Detection using Machine Learning" project aims to develop an intelligent system capable of identifying and preventing malicious website URL attacks and email spam. This project involves building, training, and deploying machine learning models to analyse URLs and email content, flagging suspicious activities and preventing cyber threats. The proliferation of internet usage has led to an increase in the number of malicious websites aiming to deceive users through website URL attack. These URLs often mimic legitimate websites to trick users into divulging sensitive information, leading to financial losses and privacy breaches. This study explores the application of machine learning techniques to detect website URLs attack with high accuracy and efficiency. Email spam detection involves applying algorithms and rules to locate and delete unwanted or unwelcome emails. These algorithms and guidelines frequently look at an email's content, the sender's reputation, and other factors to determine if it is likely to be spam. Email spam detection is critical for protecting customers from unsolicited and potentially harmful information that can clog their inboxes and compromise their security.

Keywords: Phishing, Malicious URLs, Email phishing, Spam detection, Machine learning.

Naïve Bayes, K-Nearest Neighbours (KNN), Support Vector Machines (SVM).

1. INTRODUCTION

In recent years, the network of web pages has grown faster with the expansion of the Internet. Online services, business, banking, and online marketing have made the Internet an integral part of our lives. Because of the numerous advantages of this platform for online advertising, it has also become a primary source of malicious activities. Attackers deliberately put malicious links in online advertisements that, when visited, redirect the users to unauthorised websites. Attackers make it easy for people to be steered to phishing or malware websites to steal their confidential data, make a fast buck, or defraud them by injecting dangerous code into these websites. Every year, such illegal activities cost billions of dollars [1]. Most harmful websites are almost identical to genuine websites, and the user cannot distinguish between them. In order to minimise the effects of this scam, organisations and enterprises are investing a significant amount of money in keeping their systems secure against these harmful links and URLs. The researchers made several attempts to distinguish the malicious URL using statistical analysis and the popularity feature of the domain name [2].Email spamming refers to the act of distributing unsolicited messages, optionally sent in bulk, using email; whereas emails of the opposite nature are known as ham, or useful emails [3]. The experiment setup for advertising URLs from 12 distinct datasets includes 3980870 URLs. There are two kinds of URLs in these contained in these datasets: benign and malicious. Furthermore, the malicious URL dataset includes four distinct sub-categories: spam, defacement, malware, and phishing. We also examined all of the URLs using the VirusTotal [4] tool to confirm their authenticity. Each URL is labelled with ’0’ for benign and a ’1’ for malicious in the dataset.

2. Literature Survey

If we enter the URL first it will be checked in the blacklist or whitelist if it is a blacklist that means it is a phishing URL else it is a legitimate URL (whitelist) [5]. "Phishing Website Detection based on Machine Learning: A Survey" is a survey paper that discusses different types of attacks and antiphishing approaches. Also, some defence techniques for phishing are mentioned [6]. This paper illustrates various types of Phishing Techniques and Anti-Phishing technique because phishing attack is one of a version of harmful content which has found recently a wide circulation in an information field of the modern switched communication systems. So, to identify the website is legitimate or not so there is some feature through which we can identify that the website is legitimate or not. If we enter the URL first it will be checked in the blacklist or whitelist if it is a blacklist that means it is a phishing URL else it is a legitimate URL (whitelist) [7].There is some related work that apply machine learning methods in email spam detection, A. Karim, S. Azam, B. Shanmugam, K. Kannoorpatti and M. Alazab [8]. They describe a focused literature survey of Artificial Intelligence Revised (AI) and Machine learning methods for email spam detection. K. Agarwal [9] and T. Kumar. Harisinghaney et al. (2014) [10] and Mohamad & Selamat (2015) [11] have used the “image and textual dataset for the e-mail spam detection with the use of various methods. Harisinghaney et al. (2014) [12] have used methods of KNN algorithm, Naïve Bayes, and Reverse DBSCAN algorithm with experimentation on dataset. For the text recognition, OCR library” is

employed but this OCR doesn't perform well. Mohamad & Selamat (2015) [13] uses the feature selection hybrid approach of TF-IDF (Term Frequency Inverse Document Frequency) and Rough pure mathematics.

3. PROPOSED METHODOLOGY

In a study of phishing, it is attacked through Email, Messages, or any communication media through which the particular link has to be clicked. In this proposed system we deal with User Interface (UI) to detect websites based on URLs. While addressing Machine Learning Algorithm is being approached followed by feature classification moreover based on that websites would be distinguished as phishing or authorized websites. Firstly, user will go with copying and pasting the URL in the provided UI and then if the link is safe or legitimate the user will be addressed directly to that particular website. If the link fails to be safe the UI will pop up the message.

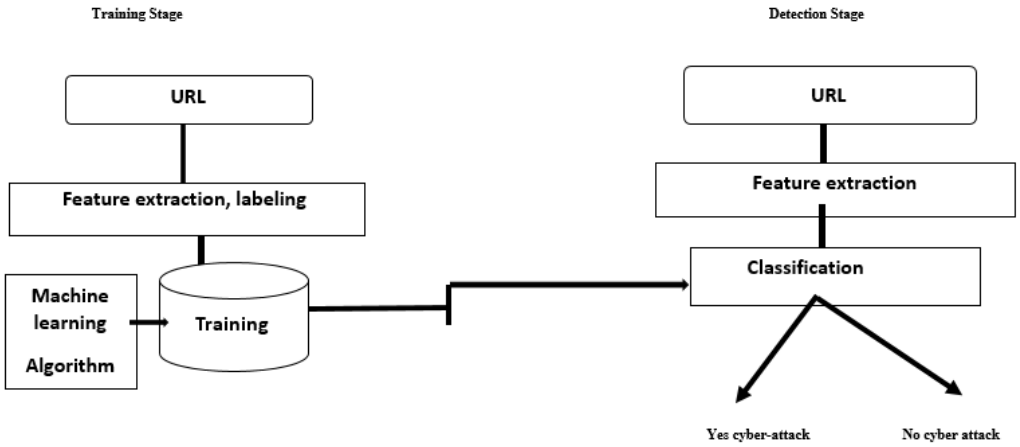


Figure 1. Website URL Attack Approach

Figure 1. Website URL attack shows the cyber-attack When evaluating potential cyber threats, unusual account activity, phishing attempts, or malware alerts should be treated as indicators of a cyber-attack, requiring immediate investigation and action. Similarly, unrecognized URLs and denial-of-service symptoms signal potential risks that need mitigation strategies. In contrast, if activities are confirmed as legitimate—like normal account behaviour or safe emails organizations can continue regular operations while monitoring security. This distinction is crucial for effectively safeguarding systems and data.

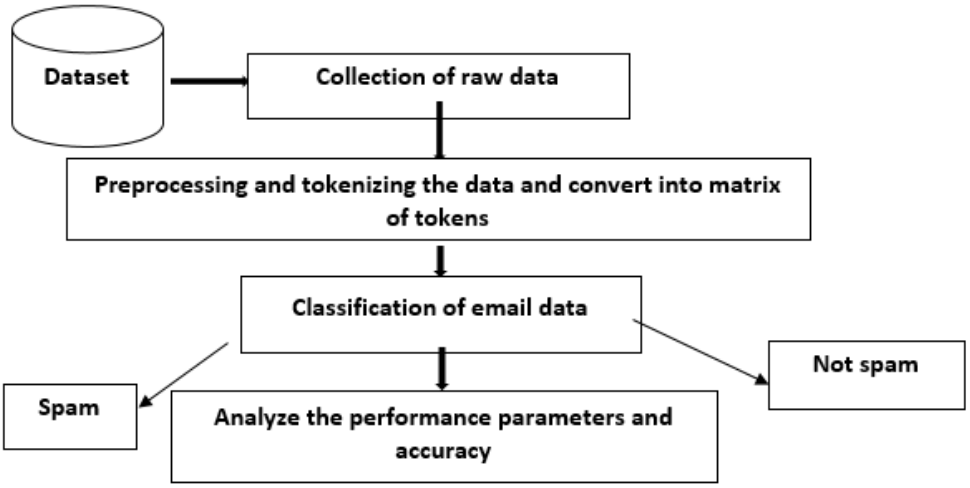


Figure 2: Email spam detection Approach

Figure 2. The email spam detection Approach outlines a systematic process for filtering spam emails. It begins by checking the sender's reputation against known spam lists. Next, the subject line and email content are analysed for spammy keywords and suspicious links. User engagement with similar emails is then assessed to determine legitimacy. Finally, based on these evaluations, the email is classified as either spam, which is moved to the spam folder, or legitimate, allowing it to reach the inbox. This approach enhances the accuracy of spam detection, protecting users from unwanted emails.

4. EXPERIMENTAL RESULTS & DISCUSSION

The results section presents the outcomes of the implementation of the "Website URL Attack and Email Spam Detection using Machine Learning" project. This includes the performance metrics of the machine learning models, the effectiveness of the system in detecting malicious URLs and spam emails, and overall system performance.

4.1 DATASET

Website URL attack data refers to the collection and analysis of information related to various cyber-attacks targeting web applications through manipulated URLs. Common types of attacks include SQL injection, where malicious SQL queries are inserted into URL parameters; cross-site scripting (XSS), which involves injecting harmful scripts; and cross-site request forgery (CSRF), and exploiting authenticated sessions through crafted URLs. Data collected during these attacks typically includes the source IP address, timestamp, request method, user-agent, the targeted URL, and any injected payloads.

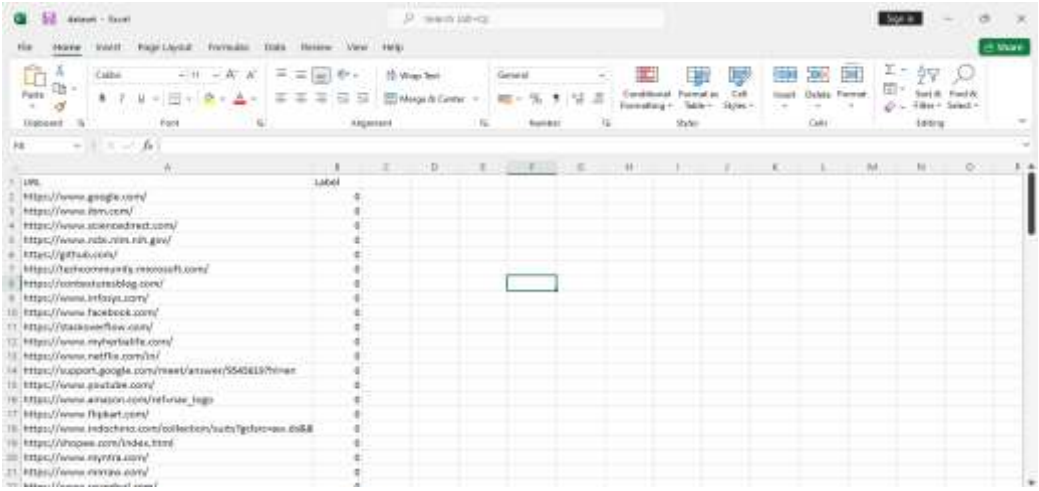


Figure 3. Website URL table

Figure 3. Shows website URL attack dataset is designed to analyse and detect various cyber-attacks involving URLs, such as phishing and malware distribution. It typically includes features like the URL, a label indicating its maliciousness, and characteristics such as URL length, suspicious keywords, and domain age. Additionally, it may contain traffic data and timestamps for when the URLs were collected. The primary goal of this dataset is to train machine learning models to automatically classify URLs and enhance cyber security measures, providing insights into evolving threats and improving defences.

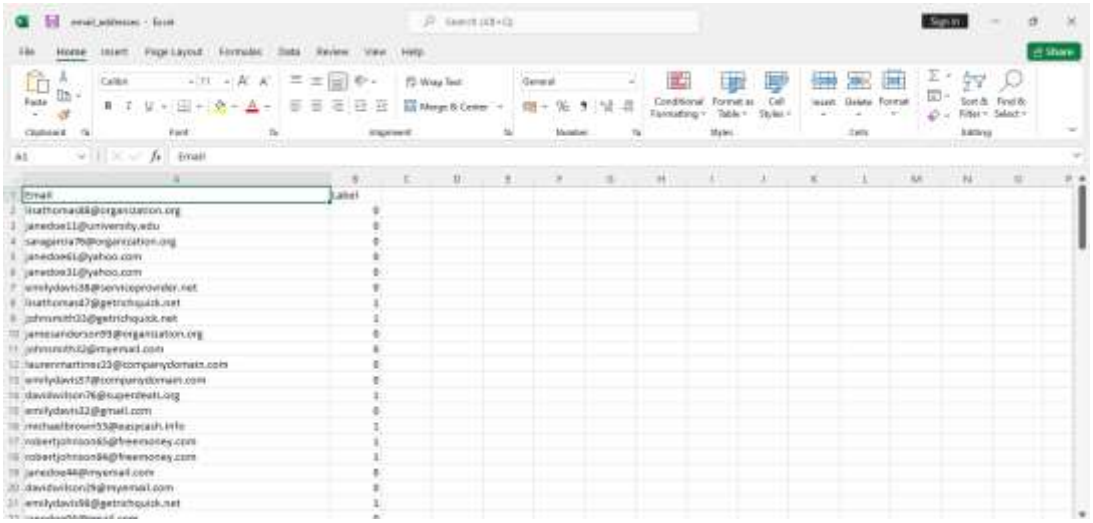


Figure 4. Email spam table

Figure 4. Shows an email spam dataset consists of records used to classify emails as spam or legitimate. Each entry typically includes features such as the email content, sender information, subject line, and various metadata points like the presence of suspicious keywords or links. The dataset is labelled to indicate whether each email is spam or not, aiding in the development of machine learning models for spam detection. By analysing these features, researchers can improve algorithms to filter unwanted emails effectively, enhancing overall email security and user experience.

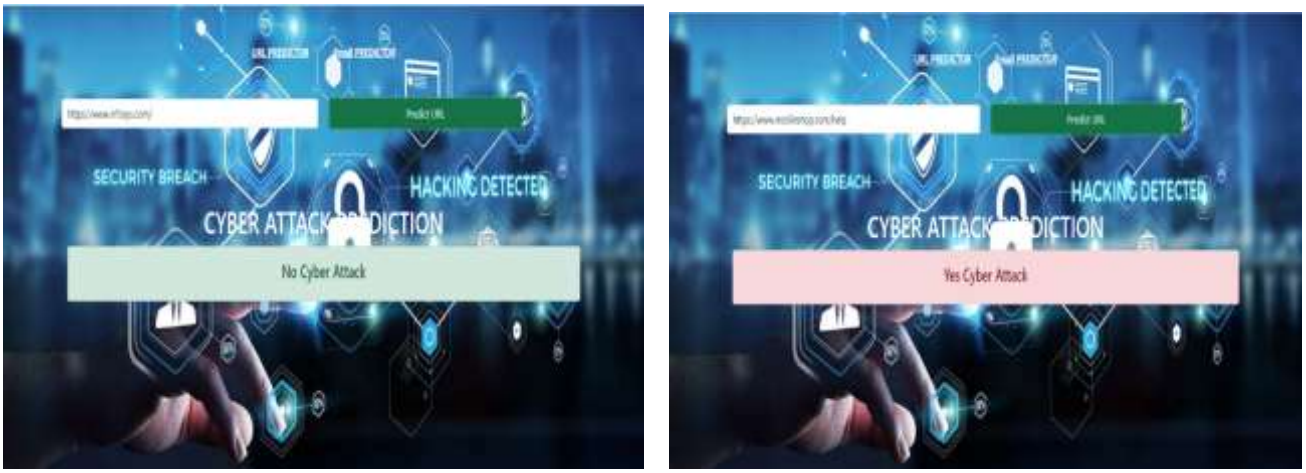
4.2 IMPLEMENTATION PLATFORM

Implementing a platform to combat email spam and website URL attacks using machine learning involves several key steps. First, data collection is essential; for email spam, this includes gathering labelled datasets of both spam and legitimate emails, while for URL attacks, historical data on URL requests, attack patterns, and outcomes is needed. Next, feature extraction plays a critical role, where relevant attributes such as sender reputation, email content, and URL characteristics are identified and processed. Machine learning algorithms, such as decision trees, support vector machines, or neural networks, can then be trained on this data to distinguish between malicious and benign inputs.

(A) Sign In Page **(B) Sign Up Page**

Figure 5. (A) Sign in Page and (B) Sign Up Page

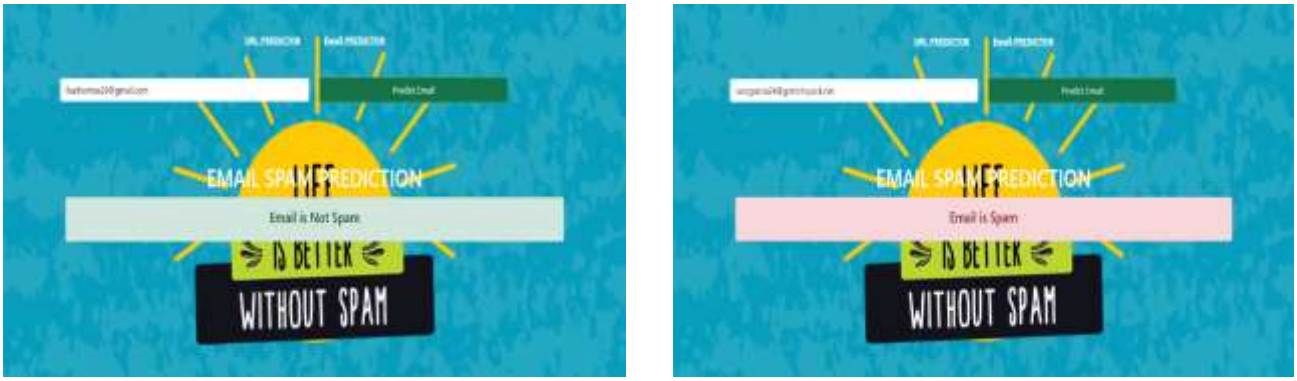
Figure 5. (A) Sign in Page and (B) Sign up Page Shows The login form must enable users to authenticate using a username and password, with multi-factor authentication (MFA) required for administrators to enhance security. Input validation is essential, ensuring that passwords meet criteria such as minimum length and complexity, which includes a mix of uppercase letters, lowercase letters, numbers, and special characters. Additionally, the username must adhere to specified formats, such as avoiding special characters. These measures collectively ensure secure access and reduce the risk of unauthorized entry.



(A) (**B**)

Figure 6. (A) & (B) Checking website URL attack

Figure 6. (a) & (b) Shows Checking website URL attack determining whether a URL could lead to a cyber-attack involves analysing several factors. First, check if the URL is on known blacklists for phishing or malware. Look for suspicious characteristics, such as unusual domain names, excessive length, or misleading keywords. Additionally, assess if the site uses HTTPS and has a valid SSL certificate, as this indicates a level of security. If any red flags are identified, the URL may pose a risk for a cyber-attack.



(A) (B)

Figure 7. (A) & (B) Checking Email Spam

Figure 7. (A) & (B) shows Checking Email Spam to determine if an email is spam, evaluate several key factors. Check the sender's email address for legitimacy, as many spam emails come from unfamiliar or suspicious domains. Analyse the subject line and content for common spam keywords, promotional language, or urgent requests that could indicate deceit. Additionally, look for unusual attachments or links that could be harmful. If these red flags are present, the email is likely spam.

5. Conclusion

The current system can be significantly enhanced by integrating real-time monitoring tools to provide continuous protection against new and emerging threats. This would involve developing APIs that allow the machine learning model to interface with network security tools, browsers, and email clients, enabling real-time detection and alerts. Expanding the training dataset is crucial for improving accuracy; incorporating a diverse set of URLs and emails from various languages and regions will enhance the system's ability to generalize across different threats.

Adaptive learning techniques could further bolster the system, allowing it to update based on new data through periodic retraining or online learning methods. Future enhancements may also explore multi-algorithm ensemble models, which combine the strengths of various machine learning algorithms to improve overall accuracy and robustness. Incorporating deep learning techniques, such as Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs), could capture nuances in email content and URLs, leading to higher detection accuracy.

Acknowledgement

I am grateful to Dr.Parashuram Bannigidad Chairman & Professor, Department of Computer Science, Rani Channamma University, Belagavi for his valuable guidance for completion of this work.\

REFERENCES

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

[2] D. Sahoo, C. Liu, and S. C. Hoi, (2017). "Malicious url detection using machine learning: A survey," arXiv preprint arXiv: 1701.07179.

[3]. O. Saad, A. Darwish and R. Faraj, (2012)"A survey of machine learning techniques for Spam filtering", *Int. J. Comput. Sci. Netw. Secure.* vol. 12, pp. 66, Feb.

[4] "Virus Total," https://www.virustotal.com/gui/home/url, accessed: 2022- 03-24.

[5]. Anti-Phishing Working Group. (2015. March.) APWG Phishing Activity Trend Report 2nd Quarter 2014. [Online]. Available: http://docs.apwg.org/reports/apwg_report_q2_2 010.pdf.

[6]. Ma, Justin, et al. (2009). "Beyond blacklists: learning to detect malicious web sites from suspicious URLs." Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM.

[7]. Anti-Phishing Working Group. (2015. March.) APWG Phishing Activity Trend Report 2nd Quarter 2014. [Online]. Available: http://docs.apwg.org/reports/apwg_report_q2_2 010.pdf [4].

[8]. Suryawanshi, Shubhangi & Goswami, Anurag & Patil, Pramod. (2019). Email Spam Detection: An Empirical Comparative Study of Different ML and Ensemble Classifiers. 69-74. 10.1109/IACC48062.2019.8971582.

[9]. Karim, A., Azam, S., Shanmugam, B., Krishnan, K., & Alazab, M. (2019). A Comprehensive Survey for Intelligent Spam Email Detection. IEEE Access, 7, 168261-168295. [08907831]. https://doi.org/10.1109/ACCESS.2019.2954791

[10]. K. Agarwal and T. Kumar, "Email Spam Detection Using Integrated Approach of Naïve Bayes and Particle Swarm Optimization," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2018, pp. 685-690.

[11]. Harisinghaney, Anirudh, Aman Dixit, Saurabh Gupta, and Anuja Arora. (2014) "Text and image-based spam email classification using KNN, Naïve Bayes and Reverse DBSCAN algorithm." In Optimization, Reliability, and Information Technology (ICROIT), 2014 International Conference on, pp.153-155. IEEE.

[12]. Mohamad, Masurah, and Ali Selamat (2015). "An evaluation on the efficiency of hybrid feature selection in spam email classification." In Computer, Communications, and Control Technology (I4CT), 2015 International Conference on, pp. 227-231. IEEE.

[13]. Shradhanjali, Prof. Toran Verma (2017). "E-Mail Spam Detection and Classification Using SVM and Feature Extraction "in International Journal of Advance Research, Ideas and Innovation In Technology, ISSN: 2454-132X Impact factor: 4.295.