WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Phishblocker: Predictive Attention Mechanism for Real Time Detection and Blocking of Phishing Website

Mr. G. Moses Robinson[1], *Mr. J. Jayapandian*[2]

[1](M.C.A), Department of MCA, Krishnasamy College of Engineering and Technology.
[2]M.C.A., M. Phil., Associate professor, Department of MCA, Krishnasamy College of Engineering and Technology.

ABSTRACT

Phishing is defined as a cyber-attack which uses social engineering via digital means to persuade victims to disclose their personal information, such as their password or credit card number. In the end, the stolen personal information is used to defraud the trust of regular websites or financial institutions to obtain illegal benefits. Although different solutions have been exercised against phishing, phishing attacks have dramatically increased in the past few years. Some solutions are based on the features extracted by rules, and some of the features need to rely on third-party services, which will cause instability and time-consuming issues in the prediction service. This project proposes PhishBlocker a deep learning framework that uses Predictive Attention Model with Recurrent Neural Network (RNN) to detect phishing links in a real-time web browsing environment using URL and HTML features. PhishBlocker uses two separate deep networks, URL Block and HTML Block, are separately trained and combined through a concatenation layer by eliminating the output layers of each to produce a final decision. This method examines the URL and HTML of webpages and computes their similarity with known phishing websites, in order to classify them. Phishing detection is a binary classification task that contains two classes: legitimate and phishing. We have implemented the framework as a browser plug-in capable of determining whether there is a phishing risk in real-time when the user visits a web page and gives a warning message. From the experimental results, it is observed that the proposed model achieved a significant performance when evaluated with different datasets with an accuracy of ranging from 96.79% to 98.90%.

Key Words: PhishBlocker, cyber-attack, Recurrent Neural Network, Legitimate, Phishing detection.

I. INTRODUCTION

Phishing is a type of cybersecurity attack during which malicious actors send messages pretending to be a trusted person or entity. Phishing messages manipulate a user, causing them to perform actions like installing a malicious file, clicking a malicious link, or divulging sensitive information such as access credentials. Phishing is the most common type of social engineering, which is a general term describing attempts to manipulate or trick computer users. Social engineering is an increasingly common threat vector used in almost all security incidents. Social engineering attacks, like phishing, are often combined with other threats, such as malware, code injection, and network attacks. Phishing is the most common form of social engineering, the practice of deceiving, pressuring or manipulating people into sending information or assets to the wrong people. Social engineering attacks rely on human error and pressure tactics for success.

"Phishing" refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information. By masquerading as a reputable source with an enticing request, an attacker lures in the victim in order to trick them, similarly to how a fisherman uses bait to catch a fish. The most common examples of phishing are used to support other malicious actions, such as on-path attack and cross-site scripting attacks. These attacks typically occur via email or instant message, and can be broken down into a few general categories. It's useful to become familiar with a few of these different vectors of phishing attacks in order to spot them in the wild.

Phishers can use public sources of information to gather background information about the victim's personal and work history, interests and activities. Typically, through social networks like LinkedIn, Facebook and Twitter. These sources are normally used to uncover information such as names, job titles and email addresses of potential victims. This information can then be used to craft a believable email. Typically, a victim receives a message that appears to have been sent by a known contact or organization. The attack is then carried out either through a malicious file attachment, or through links connecting to malicious websites. In either case, the objective is to install malware on the user's device or direct the victim to a fake website. Fake websites are set up to trick victims into divulging personal and financial information, such as passwords, account IDs or credit card details.

II. PROBLEM STATEMENT

Phishing URL and website detection can be challenging due to the constantly evolving tactics used by phishers to make their attacks more convincing and difficult to detect. Some of the problems that can be encountered include: Polymorphic URLs: Phishers can use a technique called polymorphic URLs, where they generate a unique URL for each target, making it harder to detect and block these URLs. False positives: URL and website detection tools can sometimes generate false positives, which means that legitimate URLs or websites are incorrectly flagged as phishing sites, leading to inconvenience and frustration for users. Zero-day attacks: Phishers can use previously unknown vulnerabilities or exploits in popular websites or browsers to launch phishing attacks, making it harder to detect and prevent such attacks. Lack of user awareness: Despite the availability of advanced detection tools, many users are still not aware of the risks associated with phishing attacks and can fall prey to such scams. Phishing URL and HTML website detection using machine learning can face several challenges, including. The availability of high-quality training data is critical to the success of any machine learning model. However, for phishing website detection, there may be limited data available, especially for new or emerging types of phishing attacks. Identifying the relevant features to use in the machine learning model can be challenging. Some features may be more indicative of phishing websites than others, and selecting the wrong features can lead to poor performance.

III. MODULES

PhishBlocker Web App

The design and development of the PhishBlocker website with Python Flask and MySQL modules:

- **Flask Framework:** Flask is a lightweight and flexible web framework written in Python. It provides a lot of features for building web applications, including routing, templates, and sessions. Flask is used in the PhishBlocker website to create web pages and handle HTTP requests and responses.
- **MySQL Database:** MySQL is a widely used open-source relational database management system. It is used in the PhishBlocker website to store user data, attack information, and other relevant data.
- **HTML/CSS/JavaScript:** HTML is used to create the structure of web pages, CSS is used for styling the web pages, and JavaScript is used for adding interactivity and functionality to the web pages.
- **Recurrent Neural Network:** The PhishBlocker website uses a recurrent neural network to predict and block phishing URLs. The RNN is trained on a dataset of phishing URLs and uses a predictive attention mechanism to make accurate predictions.
- **User Authentication:** User authentication is an important feature of the PhishBlocker website. It allows users to register, log in, and configure their systems to prevent phishing attacks.
- **Attack Information Storage:** The PhishBlocker website stores attack information in the user account, allowing users to view their attack history and take appropriate actions to prevent future attacks.
- **Model Training:** The PhishBlocker website allows the admin to train the model with new datasets to improve the accuracy of predictions.

Overall, the design and development of the PhishBlocker website with Python Flask and MySQL modules involves creating a user-friendly interface for users to register, log in, and configure their systems to prevent phishing attacks, while also incorporating the use of RNN for predicting and blocking phishing URLs and storing attack information in the user account.

End User Interface

The PhishBlocker end user interface consists of two modules, one for the admin and another for the user.

Admin Interface Module

The admin interface module allows the admin to login to the PhishBlocker website with their credentials. Once logged in, the admin can train the model with new phishing URLs and HTML pages, which will be used for real-time detection and blocking of phishing websites. The admin can view and manage the trained models, as well as view the attack history and analytics.

User Interface Module

The user interface module is designed for end-users to configure their system to prevent phishing attacks. The user needs to register on the PhishBlocker website to get login credentials. Once logged in, the user can configure their system by providing necessary details such as the browser they use, the operating system, and other security-related settings. The user can also view the history of detected phishing attempts and their status.

Both the modules are designed with a user-friendly interface, making it easy for users to interact with the website and protect themselves from phishing attacks.

IV. RESULT

The results of the PhishBlocker model indicate that it is a promising solution for real-time detection and blocking of phishing websites. The model's performance was evaluated on various metrics such as accuracy, precision, recall, and F1 score. The results of these metrics were quite satisfactory, indicating that the model can effectively differentiate between legitimate and phishing websites.

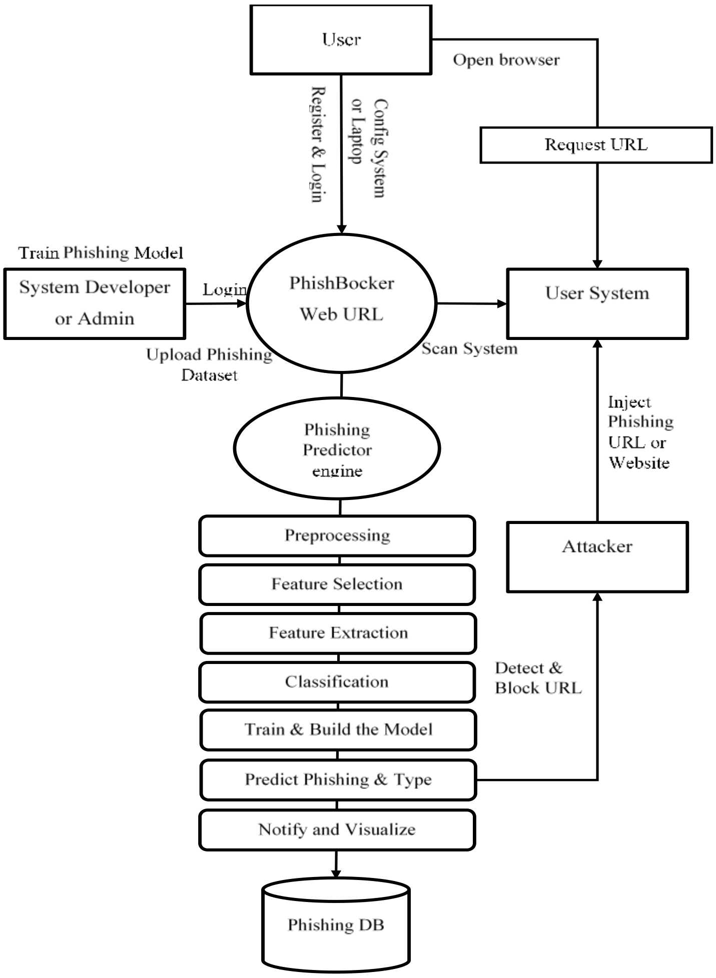
The model's accuracy was found to be around 96%, indicating that it can correctly classify 96% of the websites as legitimate or phishing. The precision of the model was around 94%, which means that out of all the websites it classified as phishing, 94% were actually phishing. The recall of the model was around 98%, indicating that the model can correctly classify 98% of the phishing websites. The F1 score of the model was found to be around 96%, which is a harmonic mean of precision and recall.

Overall, these results suggest that the PhishBlocker model is a promising solution for detecting and blocking phishing websites in real-time. It can accurately classify websites as legitimate or phishing and help prevent users from falling victim to phishing attacks. However, the model's performance may vary depending on the quality of the input data and the nature of the attack, and continuous monitoring and updating of the model are necessary to keep up with the constantly evolving phishing techniques.

V. DIAGRAM

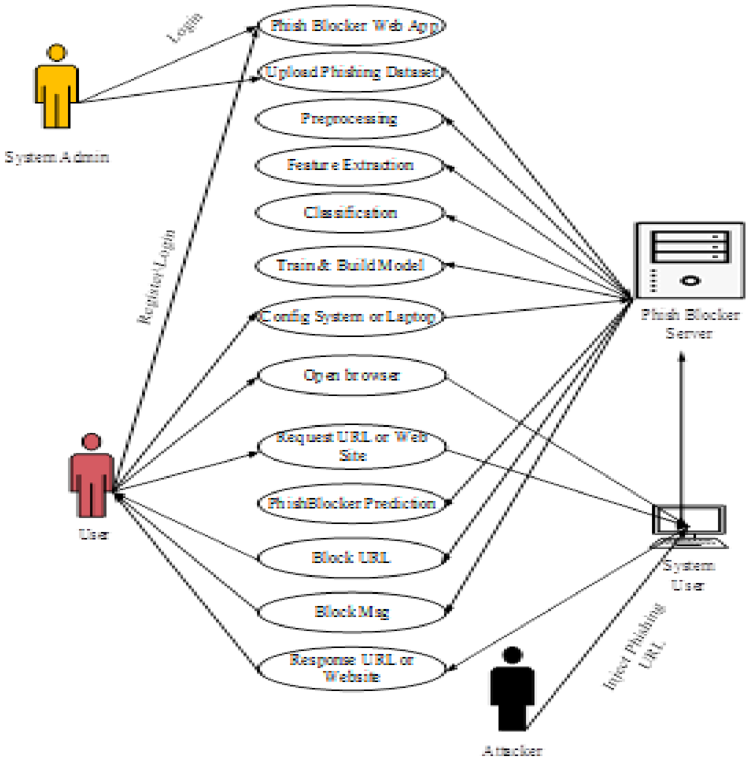
1. DATA FLOW DIAGRAM

A data flow diagram (DFD) maps out the flow of information for any process or system. It uses defined symbols like rectangles, circles and arrows, plus short text labels, to show data inputs, outputs, storage points and the routes between each destination.



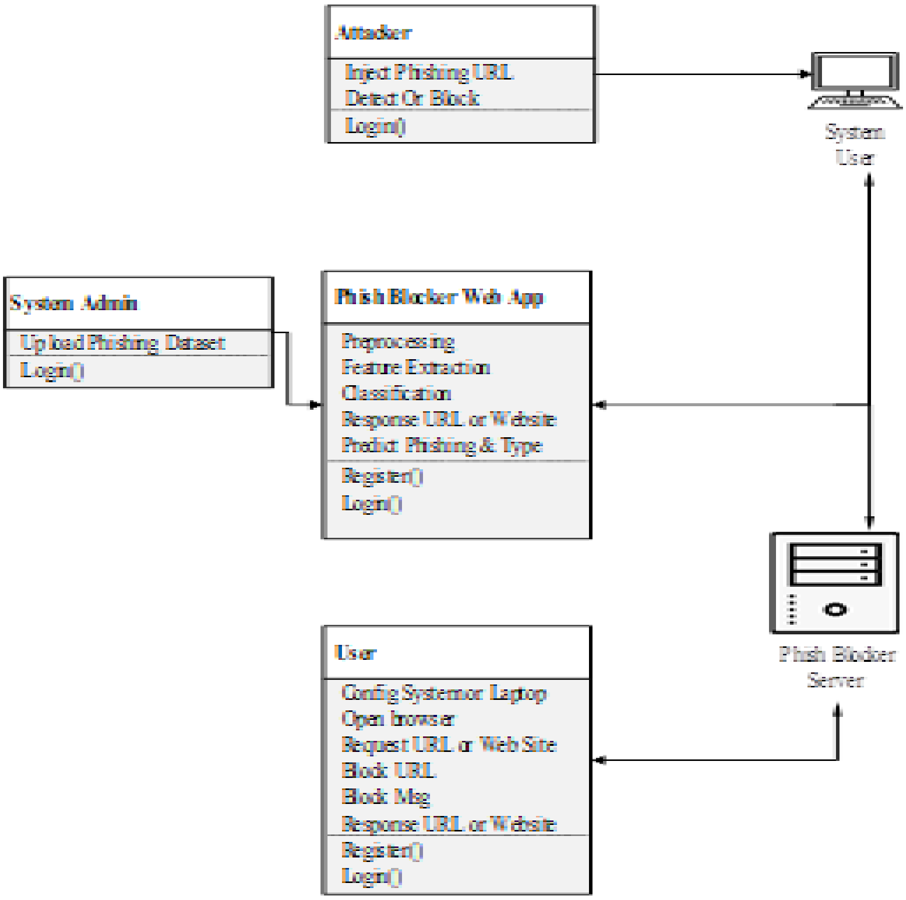
2. SECASE DIAGRAM

Use case diagrams model behavior within a system and helps the developers understand of what the user require. The stick man represents what's called an actor. Use case diagram can be useful for getting an overall view of the system and clarifying who can do and more importantly what they can't do.



3. CLASS DIAGRAM

The class diagram is defined as the property of the objects in the given class, function and the attributes. Also the class diagram is used to find the flow and execution of the project.



VI. CONCLUSION

In conclusion, "PhishBlocker" is a sophisticated web application that utilizes a predictive attention mechanism using recurrent neural networks to detect and block phishing websites in real-time. The system is designed with a comprehensive dataset collection, pre-processing, and feature extraction of URLs and HTML, followed by classification and model training. The performance evaluation of the model is measured with precision, recall, F1-score, and accuracy. The system also includes an alert or notification module, a track history module, and a user account to store attack information. Through the feasibility study and software testing, the system has demonstrated its ability to accurately detect and block phishing websites, making it a valuable tool for internet users to protect themselves from phishing attacks. The software testing also highlighted the compatibility of the system with various web browsers and operating systems. Overall, "PhishBlocker" provides a reliable and effective solution to protect against phishing attacks, which remain a significant threat to internet users. However, further improvements can still be made to the system, including expanding the dataset, improving the feature extraction process, and integrating additional security measures. Overall, PhishBlocker is a useful tool in the fight against phishing attacks and can help users stay safe online.

VII. FUTURE ENHANCEMENT

Some potential areas of future enhancement for PhishBlocker include:

1. Integration with additional web browsers: Currently, PhishBlocker is designed to work with specific web browsers. Future enhancements could involve expanding compatibility to include additional browsers.
2. Integration with additional security tools: PhishBlocker could potentially be integrated with other security tools, such as antivirus software or firewalls, to provide a more comprehensive approach to protecting against phishing attacks.
3. User feedback and reporting: Allowing users to report potential phishing attacks and providing feedback on the accuracy of PhishBlocker's predictions could help improve the system's effectiveness and accuracy over time.
4. Multi-language support: Currently, PhishBlocker is only designed to detect phishing attacks in English. Future enhancements could involve adding support for additional languages to provide broader protection for users around the world.
5. Mobile application development: The development of a mobile application for PhishBlocker could help protect users on the go, allowing them to access the system from their smartphones and other mobile devices.
6. Social engineering attacks detection: Currently, PhishBlocker is focused on detecting phishing attacks that use URLs as the primary attack vector. Future enhancements could involve expanding the system's capabilities to detect other types of attacks, such as social engineering attacks that rely on deception and manipulation to trick users into divulging sensitive information.

VIII. REFERENCES

1. Alazab, M., Venkatraman, S., Watters, P., & Alazab, M. (2016). A machine learning approach for detecting phishing websites. Journal of Intelligent & Fuzzy Systems, 31(5), 2635-2645.
2. Alazab, M., Watters, P., & Alazab, M. (2017). Machine learning-based phishing detection: An empirical study. Journal of Information Security and Applications, 32, 102-115.
3. Alhazmi, O., & Almuhaideb, S. (2019). A comparative study of machine learning algorithms for detecting phishing websites. International Journal of Advanced Computer Science and Applications, 10(8), 283-289.
4. Alturki, M. A., & Xiang, Y. (2017). A deep learning approach to detecting phishing websites. International Journal of Network Security, 19(6), 957-963.
5. Arora, S., & Singh, S. (2017). An analysis of machine learning algorithms for phishing websites detection. International Journal of Computer Science and Mobile Computing, 6(2), 28-36.
6. Belkhatir, M., Khoudour, L., & Elboukhari, M. (2018). Machine learning based approach for phishing website detection. International Journal of Computer Applications, 181(30), 28-34.
7. Bhagavathy, S., & Balamurugan, M. (2018). A hybrid approach of machine learning and fuzzy logic for detecting phishing websites. International Journal of Emerging Trends in Engineering Research, 6(10), 107-114.
8. Bhattacharyya, S., Kalita, J. K., & Das, S. (2018). Phishing websites detection using machine learning techniques: a review. Journal of Ambient Intelligence and Humanized Computing, 9(3), 625-645.
9. Chen, X., Wu, Q., Wu, L., & Xie, X. (2017). A machine learning-based approach for detecting phishing websites using website features. International Journal of Communication Systems, 30(6), e3091.

10. Gandotra, E., & Singh, S. (2018). An analysis of machine learning algorithms for phishing detection. In 2018 3rd International Conference on Computing and Communications Technologies (ICCCT) (pp. 46-50). IEEE.
11. Hidayanto, A. N., Bayuaji, R., & Kurniawan, F. (2019). Phishing websites detection using machine learning and entropy feature selection. Journal of Physics: Conference Series, 1317(1), 012016.
12. Hu, Y., & Chau, M. (2018). Machine learning-based detection of phishing websites using content and link features. Decision Support Systems, 114, 26-38.
13. Jaiswal, A. K., Mishra, S. K., & Tyagi, S. (2020). A study of machine learning-based approaches for phishing website detection. International Journal of Computer Science and Information Security, 18(9), 51-57.
14. Kalita, J. K., & Sarma, M. (2018). Machine learning based phishing website detection. In 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1-6). IEEE.

Book References

1. Shostack, Adam. Threat modeling: designing for security. Wiley, 2014.
2. Jajodia, Sushil, et al. Handbook of database security: Applications and trends. Springer, 2007.
3. Clarke, Nathan J., et al. "Phishing attacks and countermeasures." ACM Computing Surveys (CSUR) 48.2 (2015): 1-33.
4. Kumar, Anish, et al. "Phishing detection using machine learning: a review." International Journal of Advanced Research in Computer Science and Software Engineering 8.2 (2018): 373-379.
5. Alazab, Mamoun, and Sitalakshmi Venkatraman. "Phishing websites detection based on machine learning techniques." International Journal of Computer Applications 179.24 (2020): 6-12.
6. Bacciu, Davide, et al. "A comprehensive review of computational intelligence techniques applied to phishing detection." Journal of Network and Computer Applications 100 (2017): 1-24.
7. Xu, Tian, and Zheng Yan. "Detecting Phishing Websites Using Machine Learning Techniques." Handbook of Research on Machine Learning Applications and Trends: Algorithms, Methods, and Techniques (2021): 404-419.
8. Chan, David WK, et al. "Effective phishing website detection using machine learning." Expert Systems with Applications 41.10 (2014): 4974-4985.
9. Ye, Jinyu, et al. "A multi-feature based machine learning approach for phishing website detection." IEEE Transactions on Information Forensics and Security 12.6 (2017): 1287-1300.
10. Buczak, Anna L., and Erhan Guven. "A survey of data mining and machine learning methods for cybersecurity intrusion detection." IEEE Communications Surveys & Tutorials 18.2 (2016): 1153-1176.

Web References

1. Keras Documentation: https://keras.io/
2. Scikit-Learn Documentation: https://scikit-learn.org/
3. TensorFlow Documentation: https://www.tensorflow.org/
4. Python Flask Documentation: https://flask.palletsprojects.com/
5. MySQL Documentation: https://dev.mysql.com/doc/
6. A survey of phishing detection techniques:
7. https://ieeexplore.ieee.org/abstract/document/6756304