

Phishwiper: Automated Detection and Blocking of Phishing Websites

¹Sarath Krishna S, ²Sidharth M V, ³Sreehari M, ⁴S Shaima, ⁵Anjana Ashok

¹Student, ²Student, ³Student, ⁴Student, ⁵Assistant Professor (CSE)

Computer Science and Engineering Department,

Nehru College of Engineering and Research Centre (NCERC), Thrissur, India

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 PhishWiper 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. PhishWiper uses two separate deep networks, URLBlock and HTMLBlock, 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: decentralized, blockchain, data privacy, DAG, smart contracts

1.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 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.

To prevent these attacks, we propose a system called PhishWiper that uses a predictive attention mechanism with a recurrent neural network to detect and block phishing websites in real-time. The proposed system consists of several stages, including dataset collection, pre-processing, feature extraction (URL and HTML), classification, model building and training, and performance evaluation. The dataset is collected from various sources and pre-processed to extract relevant features such as domain age, IP reputation, and SSL certificate information.

The URL and HTML features are extracted using various techniques, such as domain analysis, HTML parsing, and content analysis. The classification stage involves training a recurrent neural network model using the extracted features to classify a website as either legitimate or phishing. The model is trained and evaluated using various performance metrics such as accuracy, precision, recall, and F1 score.

2. LITERATURE REVIEW

[1] Phishing attacks have become a major concern as advancements in internet technologies facilitate electronic transactions, with cybercriminals creating deceptive replicas of legitimate websites to gain unauthorized access to sensitive user information, leading to financial losses. Traditional detection methods like blacklisting and heuristics have limitations, necessitating more advanced approaches. This study proposes using a recurrent neural network (RNN) for phishing URL detection, eliminating the need for manual feature engineering. Evaluated against conventional methods on a dataset of 7,900 malicious and 5,800 legitimate URLs, the RNN achieved an accuracy of 98.7%, significantly outperforming traditional techniques. Its scalability and rapid response make it a proactive phishing detection system that operates effectively without full content analysis. The findings suggest a shift towards URL-based detection systems for faster processing, encouraging further research into deep learning methods to improve

interpretability and reduce reliance on manual feature extraction. The study highlights the importance of continuous innovation in phishing detection to counter evolving cyber threats.

[2] Phishing is a major cybersecurity threat where attackers impersonate legitimate entities to steal sensitive information, and recent advances in machine learning have shown promise in combating these attacks. This study developed and evaluated seven machine learning models—Logistic Regression, k-Nearest Neighbors, Support Vector Machine, Naive Bayes, Decision Tree, Random Forest, and Gradient Boosting—using the UCI phishing domains dataset. The results showed that Gradient Boosting and Random Forest outperformed the others, demonstrating superior accuracy in phishing detection, consistent with existing research. The findings emphasize the importance of machine learning techniques in detecting phishing websites and addressing the growing cybersecurity threat. By comparing results with other studies, the research highlights Gradient Boosting and Random Forest as particularly effective, positioning them as promising options for real-world phishing detection applications to enhance cybersecurity defenses and protect users.

[3] Phishing remains a widespread cybercrime that uses deceptive emails, messages, and websites to impersonate legitimate entities and steal sensitive user information, often targeting sectors like e-commerce, finance, and government. This study explores the effectiveness of machine learning models—including Logistic Regression, Random Forest, Decision Tree, KNN, Naive Bayes, SVM, and boosting algorithms like Gradient Boosting, XGBoost, LightGBM, and AdaBoost—in detecting phishing URLs by analyzing features such as paths, domains, and subdomains. The findings confirm that machine learning models are effective in classifying phishing sites, with Decision Trees identifying key classification features, Random Forests improving accuracy, and boosting methods like Gradient Boosting and AdaBoost enhancing model performance by focusing on difficult cases. While deep learning could further improve phishing detection, this research highlights the accessibility and interpretability of machine learning techniques, reinforcing their critical role in cybersecurity. As phishing tactics evolve, machine learning-based detection emerges as an essential defense layer, offering high precision in safeguarding users from phishing attacks.

[4] Phishing is a major threat to organizations, leading to significant financial losses by exploiting deceptive emails, SMS, and social media messages to steal sensitive information like login credentials and credit card details. This study proposes using URL lexicon, HTML content, JavaScript behavior, and page reputation features for phishing detection via machine learning. Multiple models were trained using WEKA software, with Random Forest achieving the highest accuracy of 95.043% and a low false positive rate of 0.052, making it the preferred model for classification. The dataset included 6,231 legitimate URLs from Alexa and 4,824 phishing URLs from PhishTank, totaling 11,055 instances with 24 features. Performance evaluations confirmed that these selected features are highly effective, with supervised learning models such as SVM, J48, Logistic Regression, and REP Tree also tested, but Random Forest delivered the best results. This research underscores the importance of machine learning in phishing detection, demonstrating that Random Forest is a

reliable and efficient model for identifying phishing websites and enhancing cybersecurity defenses.

[5] As phishing attacks become more prevalent, improved detection methods are crucial. This study introduces a CNN-based approach for accurately classifying phishing websites using the PhishTank dataset, which contains URL-based features. The CNN model, with its deep seven-layer architecture and feature-rich training, achieved a 98.77% accuracy, outperforming other methods. Trained on 10,000 phishing and 10,000 legitimate URLs, the model was evaluated using precision, accuracy, recall, and F1-score. Compared to KNN (87%), RNN (97.98%), NLP (97.4%), and Random Forest (94.26%), CNN excelled due to its advanced layered structure and comprehensive feature extraction. The Area Under the ROC curve further validated its effectiveness in distinguishing phishing from non-phishing sites. This research reinforces the potential of deep learning in phishing detection, demonstrating that CNN provides a high-performance framework for improving security and reducing phishing threats.

[6] Recent advancements in AI have transformed phishing website detection, with machine learning, ensemble learning, and deep learning proving more effective than traditional methods. However, these models remain vulnerable to adversarial examples (AEs) designed to evade detection. This study addresses this challenge by evaluating 15 learning-based models, particularly multimodal models, to enhance phishing and adversarial detection. To mitigate the issue of limited adversarial website data, the study introduces the Adversarial Website Generation (AWG) framework, leveraging GANs and black-box attacks to create realistic AEs that closely resemble phishing sites. Experimental results from datasets sourced from OpenPhish, PhishTank, Phishing Database, and Alexa demonstrate a high AE generation rate (over 90%) and an evasion rate of up to 88%. The multimodal model Shark-Eyes showed exceptional resilience, achieving a 99% detection rate against AEs, while traditional models like SVM struggled, detecting only 10.02%. The proposed defense strategy further improved model robustness, ensuring detection rates above 90% across all models. These findings highlight the effectiveness of multimodal and deep learning approaches in phishing detection and emphasize the need for stronger defenses against adversarial attacks to enhance cybersecurity.

[7] Phishing is a prevalent cyber-attack where attackers create fake websites or emails to deceive individuals into revealing sensitive information like passwords and financial data. Machine learning has become a powerful tool for detecting phishing websites by analyzing features such as URL structure, website content, keywords, SSL certificates, and domain age. Algorithms like Decision Trees, SVM, and Random Forest are widely used to identify patterns distinguishing phishing sites from legitimate ones. Supervised learning techniques train models using labeled datasets, while detection methods include black/whitelisting, content analysis, and visual similarity checks. As phishing tactics evolve, deep learning methods like neural networks are being explored to enhance adaptability. Research indicates that hybrid machine learning models, especially those incorporating Random Forest, can achieve accuracy rates above 99%, though single-method approaches may not be effective against all phishing

variations, emphasizing the need for multi-technique strategies to strengthen cybersecurity defenses.

[8] Phishing is a cyber-attack where attackers impersonate trusted entities to deceive users into revealing sensitive information like passwords and financial details. A Systematic Literature Survey (SLR) analyzed 80 scientific papers from the past five years, comparing phishing detection methods such as Lists Based, Visual Similarity, Heuristic, Machine Learning, and Deep Learning techniques. The study identified Machine Learning as the most prevalent approach, used in 71.25% of studies, with PhishTank and Alexa being the primary data sources. Among the 25 datasets reviewed, Random Forest was the most frequently used algorithm (38.75%), while Convolutional Neural Networks (CNN) achieved the highest accuracy of 99.98%. This survey updates previous reviews by providing insights into emerging trends, dataset usage, and algorithm performance, emphasizing the need for diverse and adaptive phishing detection strategies in response to evolving cyber threats.

[9] Phishing remains a major cyber threat as malicious websites impersonate legitimate ones to steal sensitive information. Traditional detection methods like blacklists and heuristics are often ineffective, necessitating advanced solutions. This study proposes a machine learning-based URL detection technique using recurrent neural networks (RNN), evaluated on 7,900 malicious and 5,800 legitimate sites, outperforming existing approaches. By leveraging Long Short-Term Memory (LSTM) networks, the model achieves higher accuracy and F1 scores. Future research aims to develop unsupervised deep learning models for deeper insights into phishing patterns while ensuring user privacy, strengthening cybersecurity defenses against evolving threats.

[10] Phishing remains a widespread cybercrime method where attackers trick individuals into revealing sensitive data through deceptive emails, messages, and calls. Despite ongoing preventive efforts, phishing attacks continue to rise, exposing the limitations of existing filtering techniques. This study is the first survey focused on using Natural Language Processing (NLP) and Machine Learning (ML) for phishing email detection, analyzing state-of-the-art NLP strategies and their application in various attack stages. A comparative assessment highlights challenges in phishing detection, emphasizing the inefficiency of traditional approaches reliant on source code features and third-party services. While ML methods exist, they struggle to detect emerging phishing scams without extensive manual feature engineering. The survey identifies a gap in research specifically targeting phishing email detection using NLP and underscores the need for deep learning techniques like Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs) to enhance detection accuracy, alongside developing robust tools for combating phishing threats.

3. 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

4. PhishWiper: THE PROPOSED SYSTEM

Phishing attacks are one of the most common cyber threats nowadays. To prevent these attacks, we propose a system called PhishWiper that uses a predictive attention mechanism with a recurrent neural network to detect and block phishing websites in real-time. The proposed system consists of several stages, including dataset collection, pre-processing, feature extraction (URL and HTML), classification, model building and training, and performance evaluation. The dataset is collected from various sources and pre-processed to extract relevant features such as domain age, IP reputation, and SSL certificate information.

The system is developed using Python Flask and MySQL. The admin is responsible for training the model and updating the database with new phishing information. Users can open their browser and input the URL into PhishWiper, which predicts and blocks the URL if it is identified as a phishing website. The system also stores attack information in the user's account on the PhishWiper website, enabling users to track their activity and take necessary measures. The system consists of two main modules: the training module and the detection module.

Training: It involves collecting and pre-processing a dataset of legitimate and phishing URLs, extracting features from both URL and HTML content, building and training a recurrent neural network model, and evaluating the performance of the model.

Detection: It is responsible for predicting whether a given URL is phishing or legitimate in real-time. It takes a URL input from the user, extracts its features, feeds it into the trained model, and returns the prediction along with blocking the URL if it is identified as phishing.

The system also stores the attack information in the user account on the PhishWiper website for further analysis. The proposed system aims to provide a more accurate and efficient solution for detecting and blocking phishing websites in real-time compared to traditional approaches. It also offers a user-friendly interface and a convenient way to store and analyse attack information.

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

1. **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 PhishWiper website to create web pages and handle HTTP requests and responses.
2. **MySQL Database:** MySQL is a widely used open-source relational database management system. It is used in the PhishWiper website to store user data, attack information, and other relevant data.
3. **Wamp Server:** WampServer is a Windows web development environment. It allows you to create web applications with Apache2, PHP and a MySQL database. Alongside, PhpMyAdmin allows you to manage easily your database.
4. **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.
5. **Recurrent Neural Network:** The PhishWiper 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.
6. **User Authentication:** User authentication is an important feature of the PhishWiper website. It allows users to register, log in, and configure their systems to prevent phishing attacks.
7. **Attack Information Storage:** The PhishWiper website stores attack information in the user account, allowing users to view their attack history and take appropriate actions to prevent future attacks.
8. **Model Training:** The PhishWiper website allows the admin to train the model with new datasets to improve the accuracy of predictions.

5. FUTURE SCOPE

Some potential areas of future enhancement for PhishWiper include:

- **Integration with additional web browsers:** Currently, it is designed to work with specific web browsers. Future enhancements could involve expanding compatibility to include additional browsers.
- **Integration with additional security tools:** This project 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.
- **User feedback and reporting:** Allowing users to report potential phishing attacks and providing feedback on the accuracy of predictions could help improve the system's effectiveness and accuracy over time.
- **Multi-language support:** Currently, it 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.
- **Mobile application development:** The development of a mobile application for this project could help protect users on the go, allowing them to access the system from their smartphones and other mobile devices.
- **Social engineering attacks detection:** Currently, it 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.

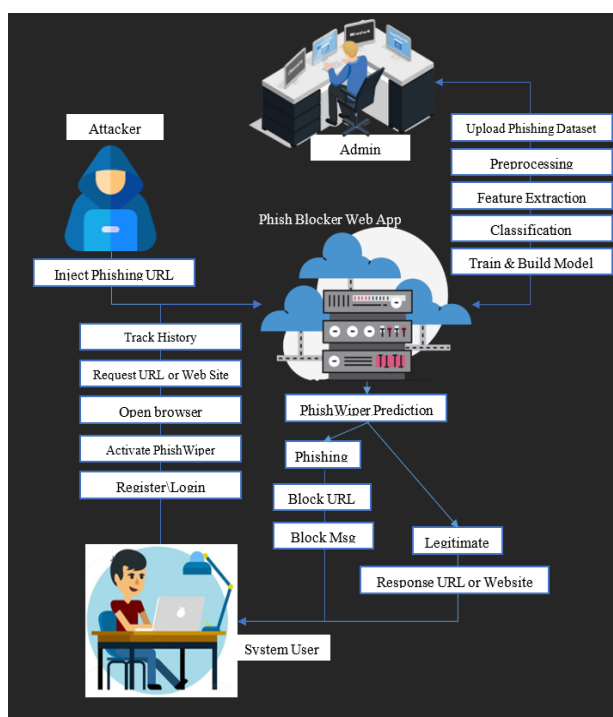


Fig 1: A diagram representing the working of Phishwiper

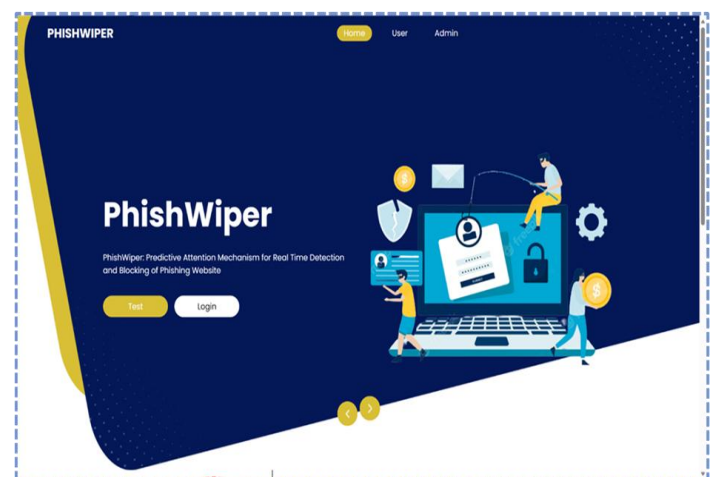


Fig 1: Home Page

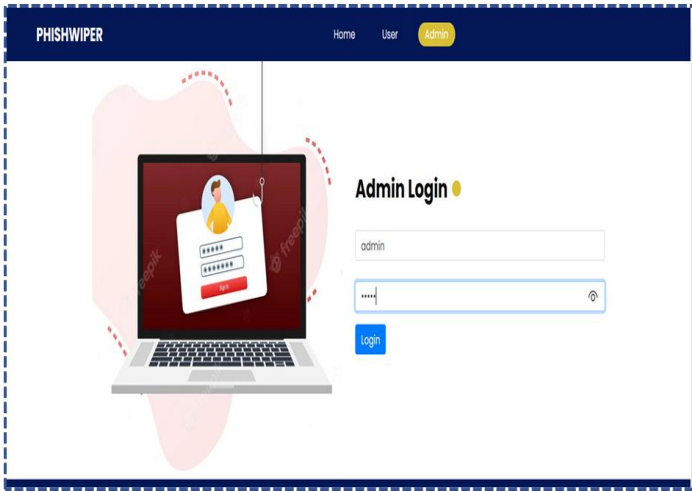


Fig 2: Admin Login

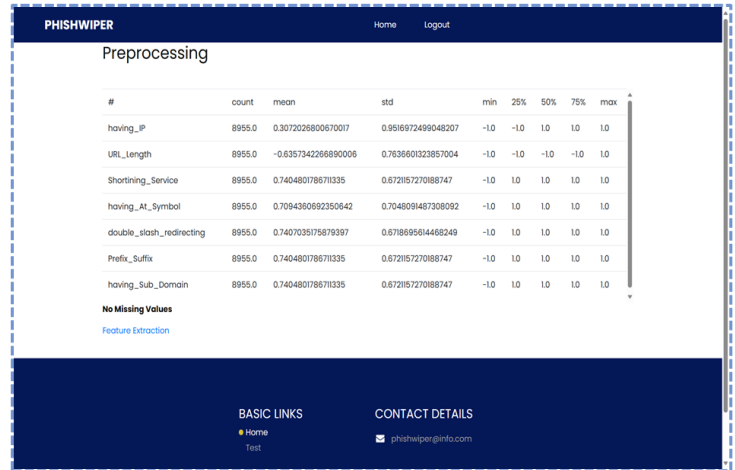


Fig 5: Preprocessing

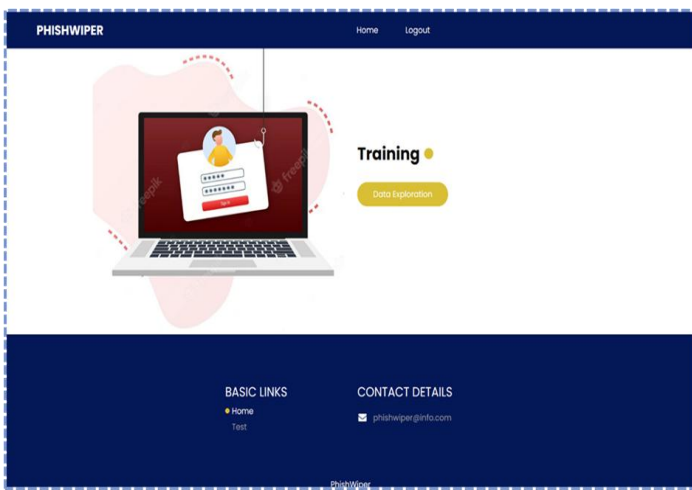


Fig 3: Training Interface

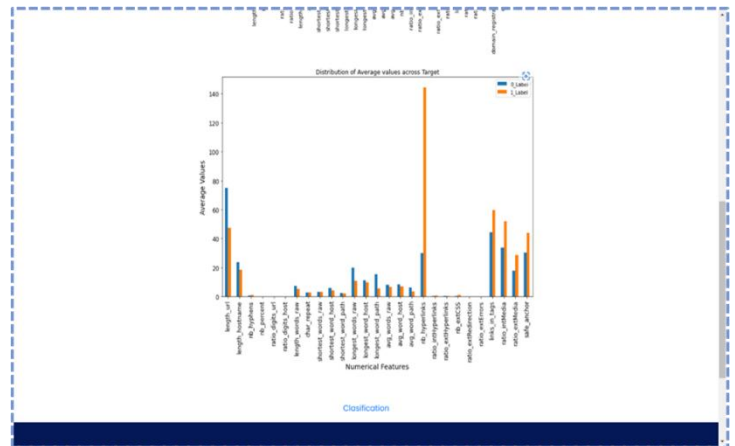


Fig 6: Classification

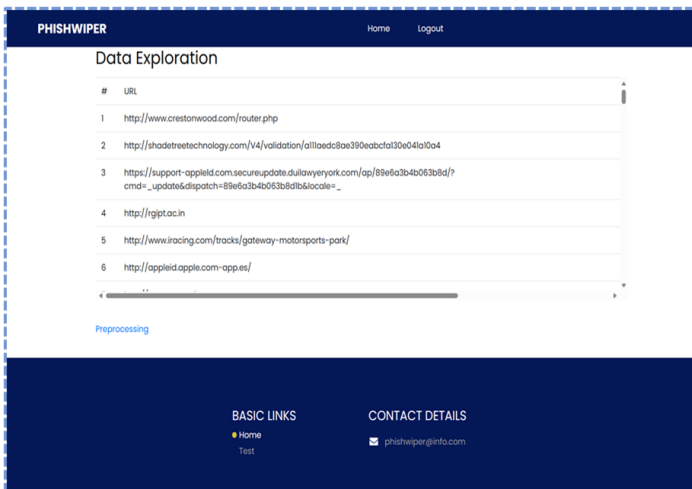


Fig 4: Data Exploration

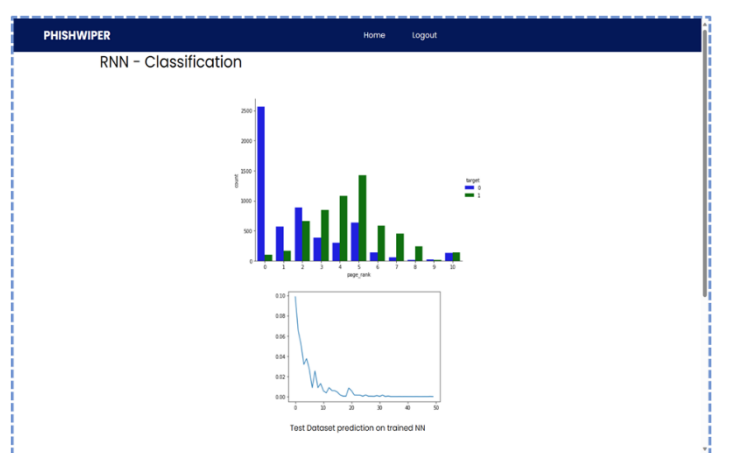
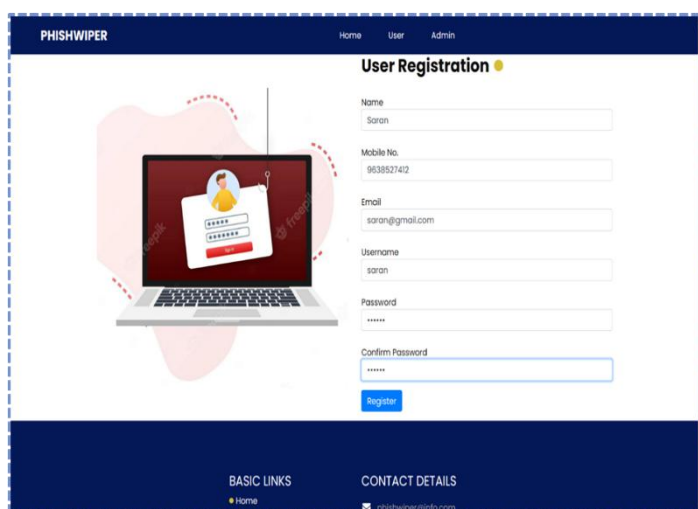


Fig 7: RNN classification



PHISHWIPER

Home User Admin

User Registration

Name
saran

Mobile No.
9638527412

Email
saran@gmail.com

Username
saran

Password

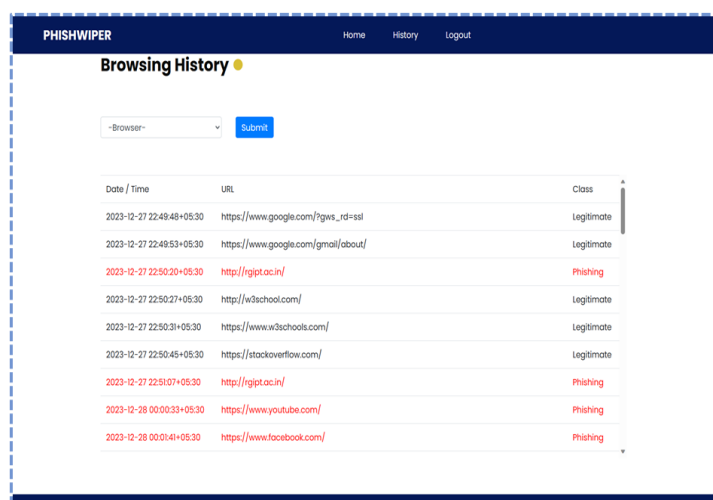
Confirm Password

Register

BASIC LINKS
Home

CONTACT DETAILS
phishwiper@gmail.com

Fig 8: User Registration



PHISHWIPER

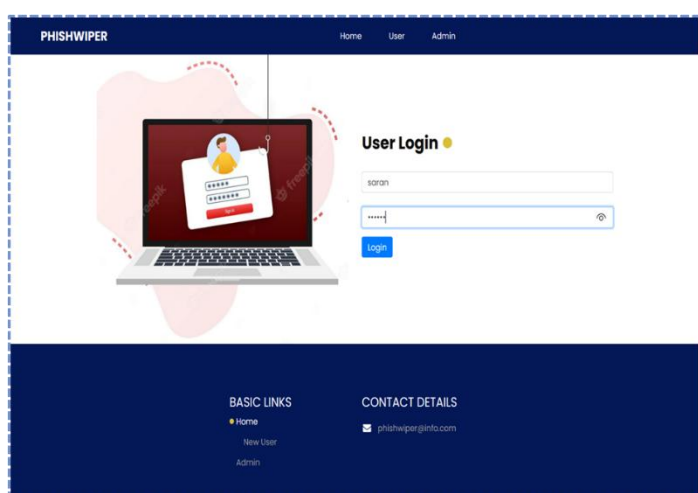
Home History Logout

Browsing History

-Browser- Submit

Date / Time	URL	Class
2023-12-27 22:48:48+05:30	https://www.google.com/?gws_rd=ssl	Legitimate
2023-12-27 22:49:53+05:30	https://www.google.com/gmail/about/	Legitimate
2023-12-27 22:50:20+05:30	http://ngjpt.ac.in/	Phishing
2023-12-27 22:50:27+05:30	http://w3school.com/	Legitimate
2023-12-27 22:50:31+05:30	https://www.w3schools.com/	Legitimate
2023-12-27 22:50:45+05:30	https://stackoverflow.com/	Legitimate
2023-12-27 22:51:07+05:30	http://ngjpt.ac.in/	Phishing
2023-12-28 00:00:33+05:30	https://www.youtube.com/	Phishing
2023-12-28 00:01:41+05:30	https://www.facebook.com/	Phishing

Fig 9: Browser History



PHISHWIPER

Home User Admin

User Login

saran

Login

BASIC LINKS
Home
New User
Admin

CONTACT DETAILS
phishwiper@gmail.com

Fig 9: User Login

6. CONCLUSION

In conclusion, this project 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, the proposed system of the project 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. PhishWiper is a useful tool in the fight against phishing attacks and can help users stay safe online.

REFERENCES

- [1] Classifying phishing URLs using recurrent neural networks, APWG Symposium on Electronic Crime Research (eCrime), IEEE, 12 June 2023.
- [2] Comparative Study of Machine Learning Algorithms for Phishing Website Detection, Kamal Omari, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 14, No. 9, 2023.
- [3] A Machine Learning Approach to Identify Phishing Websites: A Comparative Study of Classification Models and Ensemble Learning Techniques, Bhogesh Karthik Gontla, Priyanka Gundu, Padma Jyothi Uppalapati, ICST Transactions on Scalable Information Systems, 23 June 2023.
- [4] A hybrid approach for phishing detection in web application through machine learning, Pradip

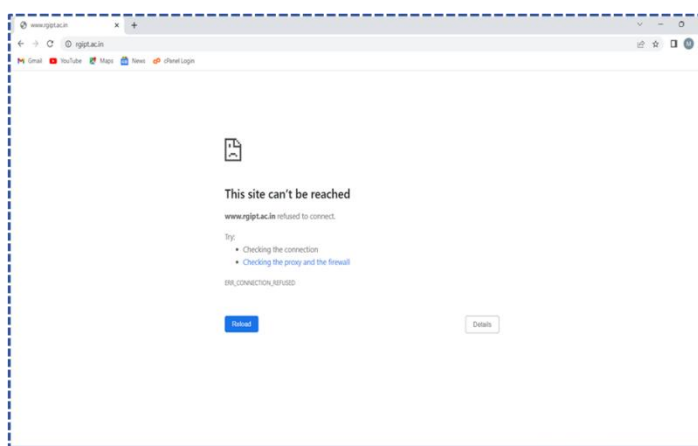


Fig 8: Blocked phishing site

Maliwad, Deepak Upadhyay, Kaushal Bhavsar, JETIR June 2019, Volume 6, Issue 6.

- [5] A Deep Learning-Based Innovative Technique for Phishing Detection in Modern Security with Uniform Resource Locators, Eman Abdullah Aldakheel, Mohammed Zakariah, Ghada Abdalaziz Gashgari, AI & Blockchain Assisted Innovative Techniques & Solutions to Modern CPS Security for Industry 4.0/5.0, 30 April 2023.
- [6] A Study on Adversarial Sample Resistance and Defense Mechanism for Multimodal Learning-Based Phishing Website Detection, Phan The Duy, Vo Quang Minh, Bui Tan Hai Dang, Ngo Duc Hoang Son, IEEE Access Volume 12, 01 August 2024.
- [7] Phishing Website Detection Using Machine Learning: A Review, Wasit Journal for Pure Sciences, Vol. (2) No. (2), 2022.
- [8] A systematic literature review on phishing website detection techniques, Journal of King Saud University– Computer and Information Sciences 35 (2023) 590–611, 3 January 2023.
- [9] Detecting phishing websites using machine learning technique, PLoS ONE16(10): e0258361, October 11, 2021.
- [10] Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey, 5th International Conference on AI in Computational Linguistics, Procedia Computer Science 189 (2021) 19–28.