Journal of Artificial Intelligence and Capsule Networks (ISSN: 2582-2012)
www.irojournals.com/aicn/

PHISHSNAP-A Chrome Extension Tool used for Detection of Phishing applying Machine Learning

Arya Nadh T S[1], Binitha P[2], Nimmi Suresh[3], Pranaya V S[4], Unnikrishnan S Kumar[5]

Department of Computer Science and Engineering, JCET, Palakkad,India

Email: [1] aryanadhofficial@gmail.com, [2] binithabala02@gmail.com, [3]nimmisuresh08@gmail.com,

[4] pranayavs28@gmail.com, [5] uksknair@gmail.com

Abstract

This work introduces a novel approach aimed at strengthening the effectiveness of phishing detection systems in the face of evolving cyber threats. Leveraging the power of machine learning-based anomaly detection techniques, this proposed mechanism seeks to significantly enhance both the accuracy and adaptability of current detection methods to effectively combat emerging phishing attacks. Central to this methodology is the utilization of ensemble model mechanisms, which intelligently integrate predictions from a diverse array of machine learning models. Through cautious analysis of URLs utilizing distinct datasets, this system systematically compares and contrasts results with established approaches, thereby enriching the overall detection process. This approach showcases notable improvements in performance metrics, boasting higher success rates that substantially exceed conventional heuristic analysis and blacklist-based detection methodologies. By transcending the limitations inherent in traditional detection strategies, this innovative framework represents a promising leap forward in the ongoing battle against phishing exploits, offering enhanced resilience in safeguarding sensitive user information from malicious cyber threats.

DOI: https://doi.org/10.36548/jaicn.2024.1.008
Received: 12.03.2024, received in revised form: 01.04.2024, accepted: 14.04.2024, published: 26.04.2024

Keywords: Phishing Detection, Machine Learning, Anomaly Detection, Ensemble Models, Cyber Threats, URLs, Datasets, Performance Metrics, Heuristic Analysis, Blacklist-Based Detection, Emerging Threats, Cyber Exploits, User Information, Malicious Threats

1. Introduction

In recent years, the internet has experienced explosive growth, offering a plethora of services ranging from online banking and entertainment to education and social networking[1-5]. However, this surge in online activity has also created opportunities for cybercriminals to exploit, leading to the proliferation of web phishing attacks. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reason. It is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate site, the only difference being the URL of the website in concern[6-10].

These attacks involve the unauthorized acquisition of sensitive personal or financial information such as usernames, passwords, account numbers, and national insurance numbers[11-13]. The prevalence of phishing attacks has escalated significantly in recent times, emerging as a prominent threat to web security. Such attacks pose a severe risk to individuals and organizations alike, undermining confidence in e-commerce and causing substantial harm to various sectors, including online banking, e-commerce platforms, marketing endeavors, customer relationships, and overall business operations[14]. Efforts to combat phishing attacks have led to the development of detection techniques, with conventional methods often relying on fixed black-and-white listing databases. However, these approaches have proven to be insufficiently effective, as cybercriminals can swiftly launch new phishing websites within seconds. Consequently, these techniques struggle to dynamically ascertain the legitimacy of newly created websites, potentially misclassifying many phishing websites as legitimate [15-16].

To address these challenges, a phishing website detection scheme has been devised, utilizing a wrapper feature selection technique in conjunction with machine learning classifiers to achieve high detection accuracy. The classification techniques employed in this scheme include Decision Tree, Support Vector Machine, Random Forest, and Naive Bayes algorithms.

In summary, the proactive identification and mitigation of phishing threats are crucial for safeguarding web users and preserving trust in online interactions. By leveraging advanced feature selection techniques and machine learning classifiers, such as those mentioned above, organizations can enhance their ability to detect and combat phishing attacks effectively.

1.1 Background

The background study involves exploring how these algorithms can be applied in phishing detection:

1. **Support Vector Machines (SVM):** SVMs aim to classify data by finding the hyperplane that best separates different classes. In phishing detection, SVMs can learn patterns in features extracted from phishing emails or websites to distinguish between legitimate and fraudulent content.

2. **Random Forest**: This ensemble learning method constructs multiple decision trees and combines their outputs to make predictions. In phishing detection, Random Forests can handle large feature sets and provide robustness against overfitting while effectively identifying phishing attempts.

3. **Decision Tree**: These hierarchical structures use a series of rules to make decisions. In the context of phishing detection, decision trees can model the features of phishing attempts, such as URL characteristics or content, to classify them as legitimate or fraudulent.

4. **Naive Bayes:** This algorithm calculates the probability of a certain class based on the presence of features, assuming independence among them. In phishing detection, Naive Bayes can assess the likelihood of an email or website being phishing based on the occurrence of specific features.

The background study typically involves understanding how these algorithms handle different types of data, their strengths, limitations, and the features relevant to phishing detection (like URL structure, content analysis, sender information, etc.). Researchers explore datasets, extract meaningful features, and train these algorithms to effectively identify and differentiate phishing attempts from legitimate content.

2. Related Work

The research in [1] proposes a smart method for spotting phishing websites . It uses a mix of different computer programs to decide if a website is real or fake. Then, a new way of combining their decisions is used. This new method gives more importance to the better programs and less to the weaker ones. This helps in accurately differentiating the phishing websites from real ones.

In [2] Phishing and pharming deceive users into sharing credentials on fake sites resembling real ones. Traditional methods like blacklists are incomplete. The AIWL creates personalized whitelists of familiar login interface

URL-based phishing attacks are widespread threats online. Attackers exploit human vulnerability, not software flaws, tricking individuals and organizations into clicking secure-looking URLs to steal data or inject malware [3] .

In the study by [4], a novel method is suggested for generating a current blacklist of phishing sites. It involves searching for a company's name on Google and comparing the page's domain with top search results. If there's a match, the page is considered legitimate

3. Proposed Work

we propose a comprehensive framework for a phishing detection Chrome extension, designed to provide users with enhanced protection against malicious websites. Figure 1. depicts the system architecture.

3.1 System Architecture

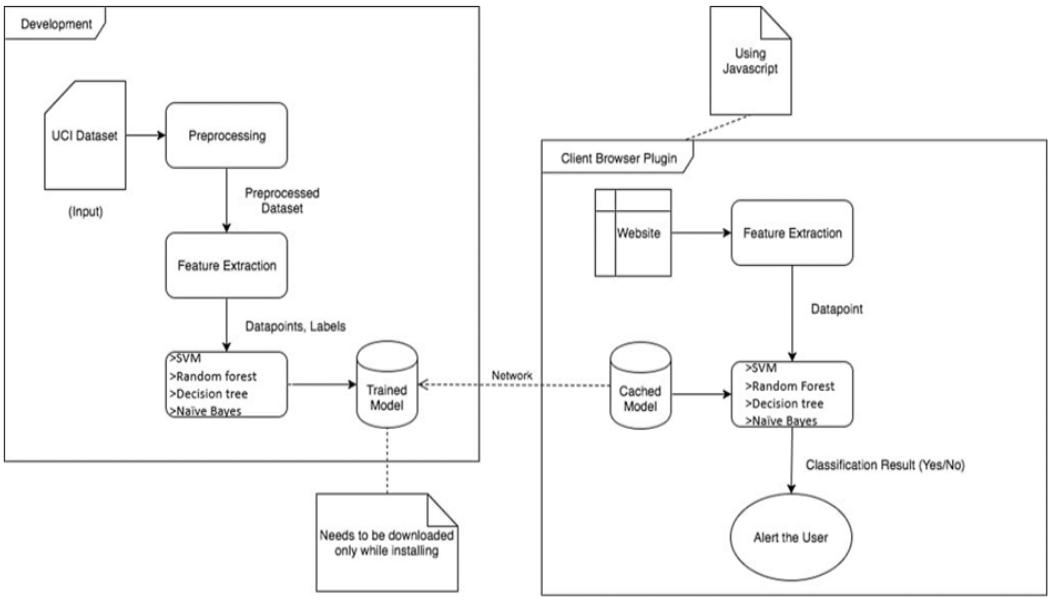


Figure 1. System Architecture

- **Data Acquisition and Pre-processing**

Machine learning relies heavily on two main components: data and models. Adequate data acquisition is crucial, ensuring a sufficient amount of diverse data with populated features to train our learning model effectively. Raw data sourced from online platforms often comprises unformatted statements, numerical values, and qualitative terms, necessitating preprocessing to clean and organize it. Initially, data is collected from reputable sources such as UCI and Kaggle proprietary websites.

- **Feature Selection**

The selection of data features for training machine learning models significantly impacts their performance. Employing wrapper feature selection methods aids in identifying the most relevant features.

- **Model Building and Training**

Training a machine learning model involves furnishing an algorithm with training data to learn from. Various algorithms are utilized for this purpose, including Decision Trees, Random Forest Algorithm, Support Vector Machine, and Naïve Bayes.

- **Dynamic Feature Extraction from Entered URL**

The phishing detection system begins by receiving a URL input from the user. Next, it employs web scraping or crawling techniques using libraries like BeautifulSoup or Scrapy in Python to gather essential information from the webpage. Feature extraction follows, where relevant attributes such as domain reputation, URL length, and the presence of suspicious characters are identified. Additionally, lexical analysis of the URL path and parameters is conducted. These extracted features serve as input for machine learning models. Subsequently, data processing steps are undertaken to clean and refine the extracted features as needed. Common techniques such as URL normalization and tokenization are applied to standardize and deconstruct URLs into meaningful components for further analysis.

3.2 Software Components

- **Chrome Extension Development Environment**

  a. Development IDE such as Visual Studio Code or JetBrains WebStorm.

  b. Chrome Extension manifest file (manifest.json).

  c. HTML, CSS, and JavaScript for building the extension's user interface and functionality.

  d. Knowledge of Chrome Extension APIs for interacting with browser features and data.

- **Machine Learning Libraries and Frameworks**

  a. Python environment for running machine learning algorithms.

  b. Libraries/frameworks such as scikit-learn for implementing SVM, Random Forest, Decision Tree, and Naive Bayes algorithms.

  c. Required dependencies like NumPy, pandas, and matplotlib for data manipulation and visualization.

- **Communication between Extension and ML Models**

  a. The APIs or message passing mechanisms are used for exchanging data between the extension and the ML backend.

- **Backend Infrastructure**

  a. Servers or cloud infrastructure for hosting and running the machine learning models.

  b. APIs or endpoints for the Chrome extension to send data for phishing detection.

3.3 Algorithm

1. **Data Collection**: The very first step is collecting a variety of data sets including phishing and legitimate websites. Some features that can be included in this dataset are URL length, domain age and presence of HTTPS protocol among others.

2. **Data Pre-processing**: After collecting the data, it should undergo a pre-processing process. This includes tasks such as handling missing values, encoding categorical variables and splitting the dataset into separate subsets for training and testing. The Scikit-learn is used for preprocessing.

3. **Feature Engineering**: At this point features are selected from the dataset that will be relevant to improving model performance. Feature selection techniques together with knowledge about particular domains play a great role in this undertaking. The NumPy, pandas are employed for feature engineering.

4. **Model Selection and Training**: Various classification algorithms like Support Vector Machines (SVM), Random Forests, Decision Trees, Naive Bayes are trained using the training dataset prepared. Hyper-parameter optimization techniques such as cross-validation are used to refine these models so that they can perform better. The prepared dataset is spilt for the purpose of training (80%) and testing (20%) and the performance of the machine learning models SVM, Random Forest, Decision Trees, and Naive Bayes implemented are evaluated to ensure its performance in terms of accuracy, recall and f1 measure. The flow diagram is illustrated in Figure.2.

3.4 Flow Diagram

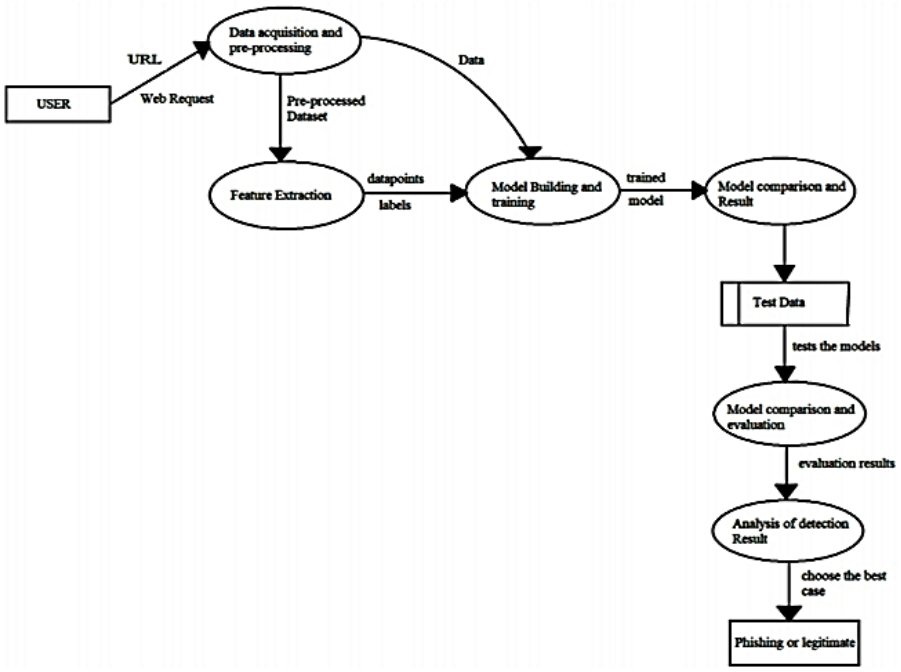


Figure 2. Flow Diagram

4. Results and Discussion

The evaluation of a phishing detection system utilizing machine learning algorithms such as SVM, Random Forest, Decision Trees, and Naive Bayes involves rigorous assessment. These evaluations collectively provide insights into the models' generalization ability, discriminative power, feature relevance, comparative performance across algorithms, effectiveness compared to existing solutions, and resilience against different types of phishing threats, ensuring the development of a robust and reliable phishing detection system.

- **Output Obtained in Various Stages**

This section shows the results obtained during module testing.

4.1 Pre processing

The output the preprocessing module is shown in Figure.3 below.

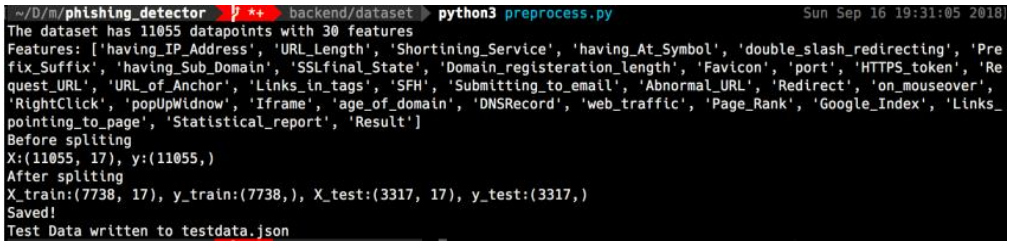


Figure 3. Preprocessing Output

4.2 Training

The output the training module is shown in Figure.4 below.

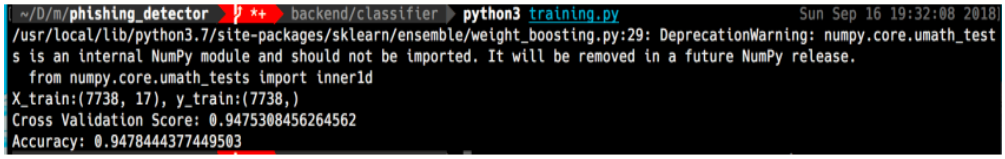


Figure 4. Training Output

4.3 F1 Score

F1 score is a measure of a test's accuracy. It considers both the precision and the recall of the test to compute the score the aggregate performance score is depicted in Figure.5

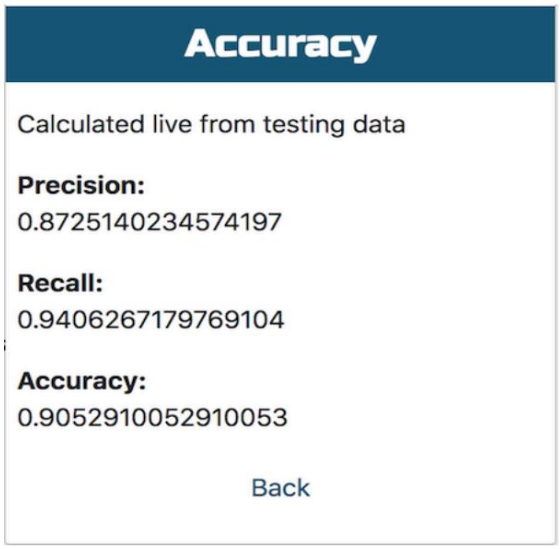


Figure 5. Performance Score

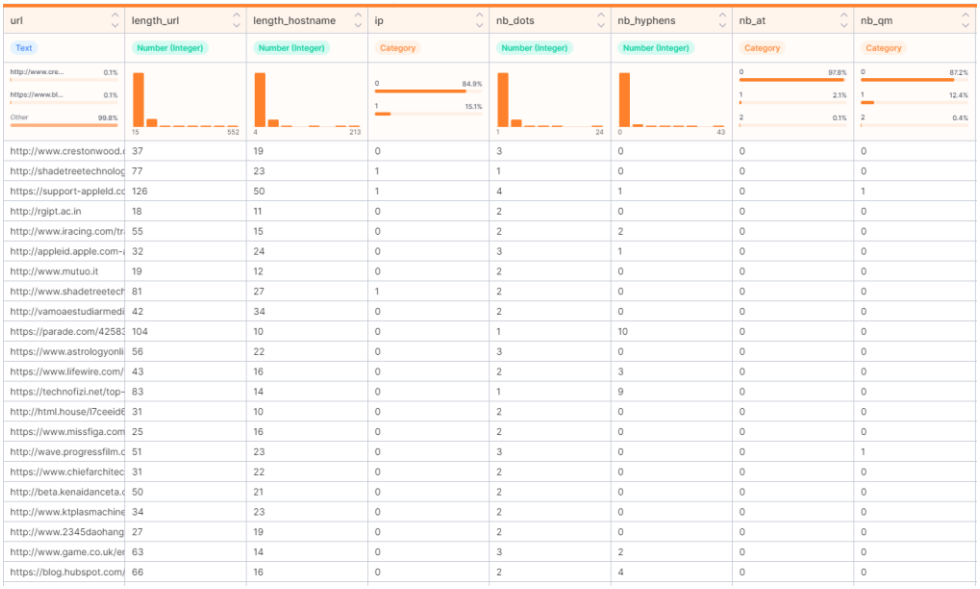
4.4 Accuracy Table

Table 1. Accuracy

Classifier	Accuracy	Time
Decision Tree	79.1%	0.015sec
Random Forest	86.3%	0.1sec
Support Vector Machine	81.9%	0.01sec
Naïve Bayes	62.2%	0.015sec

4.5 Dataset

The Figure.6 below shows the sample of dataset used in the evaluation of the proposed models



url	length_url	length_hostname	ip	nb_dots	nb_hyphens	nb_at	nb_qm
Text	Number (Integer)	Number (Integer)	Category	Number (Integer)	Number (Integer)	Category	Category
http://www.crestonwood.c	37	19	0	3	0	0	0
http://shadetreetechnolog	77	23	1	1	0	0	0
https://support-appleid.cc	126	50	1	4	1	0	1
http://rgipt.ac.in	18	11	0	2	0	0	0
http://www.iracing.com/tr	55	15	0	2	2	0	0
http://appleid.apple.com-c	32	24	0	3	1	0	0
http://www.mutuo.it	19	12	0	2	0	0	0
http://www.shadetreetech	81	27	1	2	0	0	0
http://vamoaestudiarmedi	42	34	0	2	0	0	0
https://parade.com/42583	104	10	0	1	10	0	0
https://www.astrologyonli	56	22	0	3	0	0	0
https://www.lifewire.com/	43	16	0	2	3	0	0
https://technofizi.net/top-	83	14	0	1	9	0	0
http://html.house/l7ceeid6	31	10	0	2	0	0	0
https://www.missfiga.com	25	16	0	2	0	0	0
http://wave.progressfilm.c	51	23	0	3	0	0	1
https://www.chiefarchitec	31	22	0	2	0	0	0
http://beta.kenaidanceta.c	50	21	0	2	0	0	0
http://www.ktplasmachine	34	23	0	2	0	0	0
http://www.2345daohang	27	19	0	2	0	0	0
http://www.game.co.uk/en	63	14	0	3	2	0	0
https://blog.hubspot.com/	66	16	0	2	4	0	0

Figure 6. Dataset [14]

4.6 Results

The results observed through the interface are depicted in Figures 7 to 10

- **Safe Website**

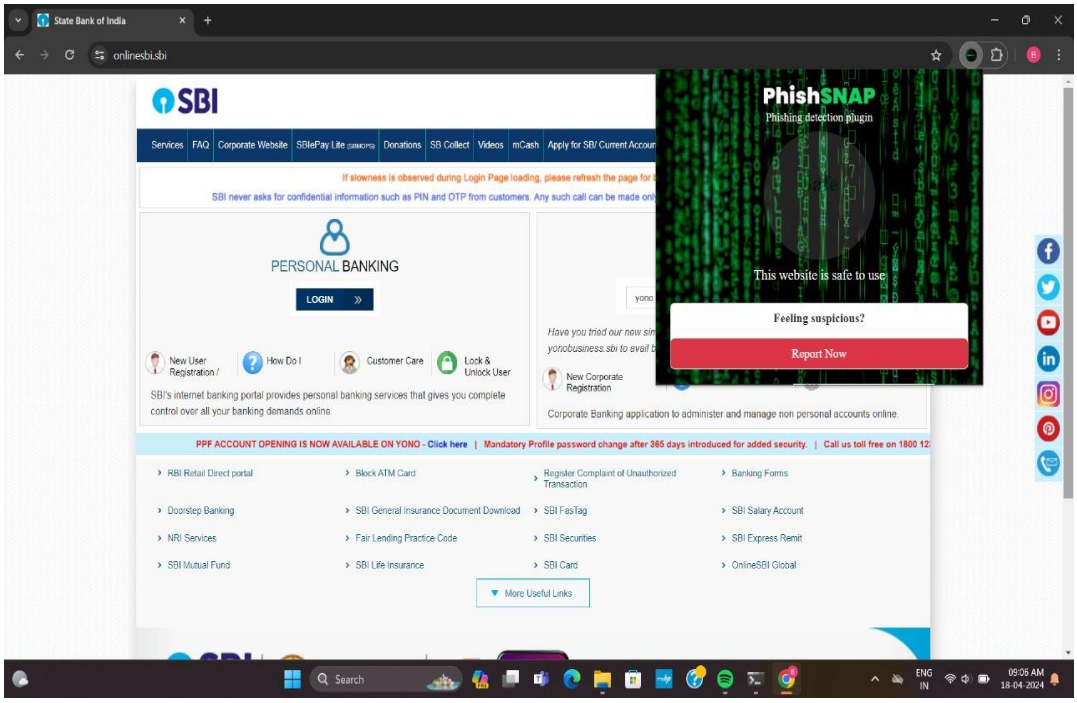


Figure 7. Safe Website

- **Phishing Website**

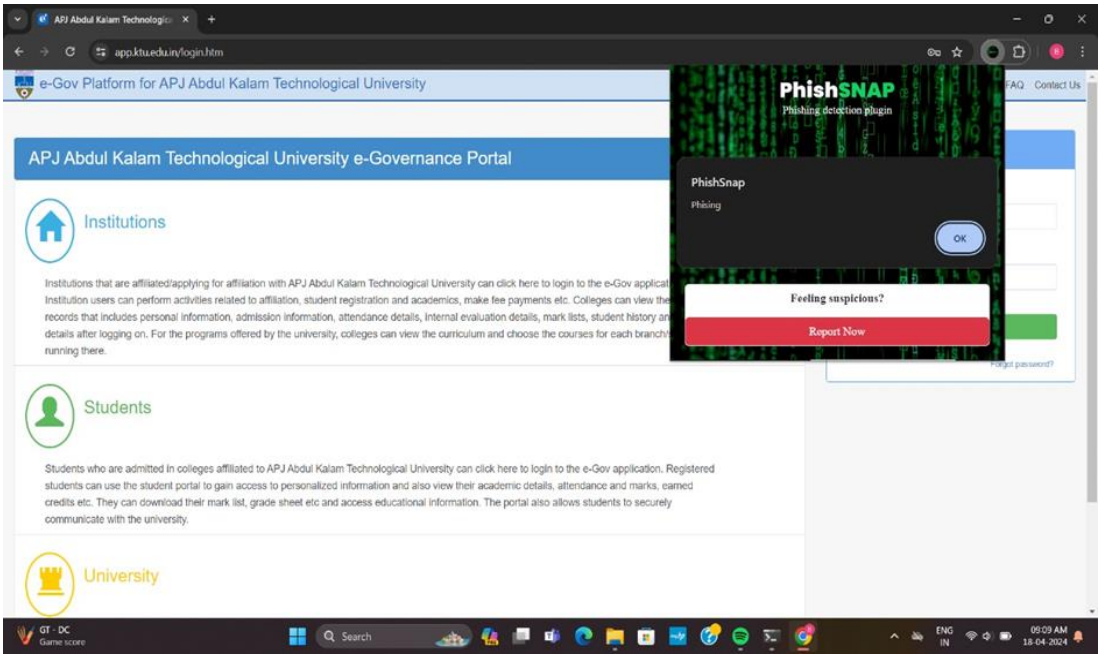


Figure 8. Phishing

- **Report Option**

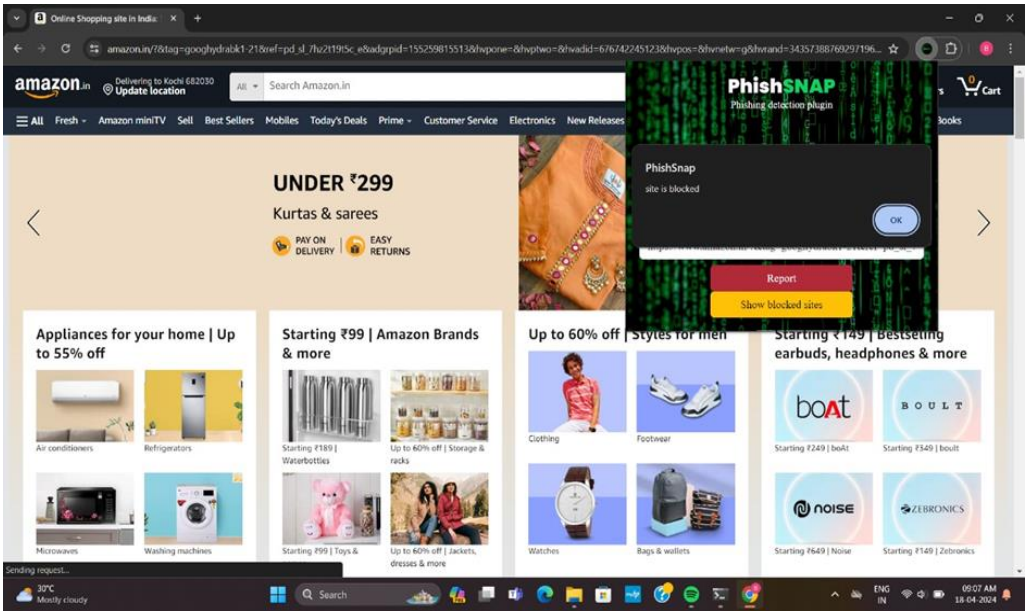


Figure 9(a). Report Option

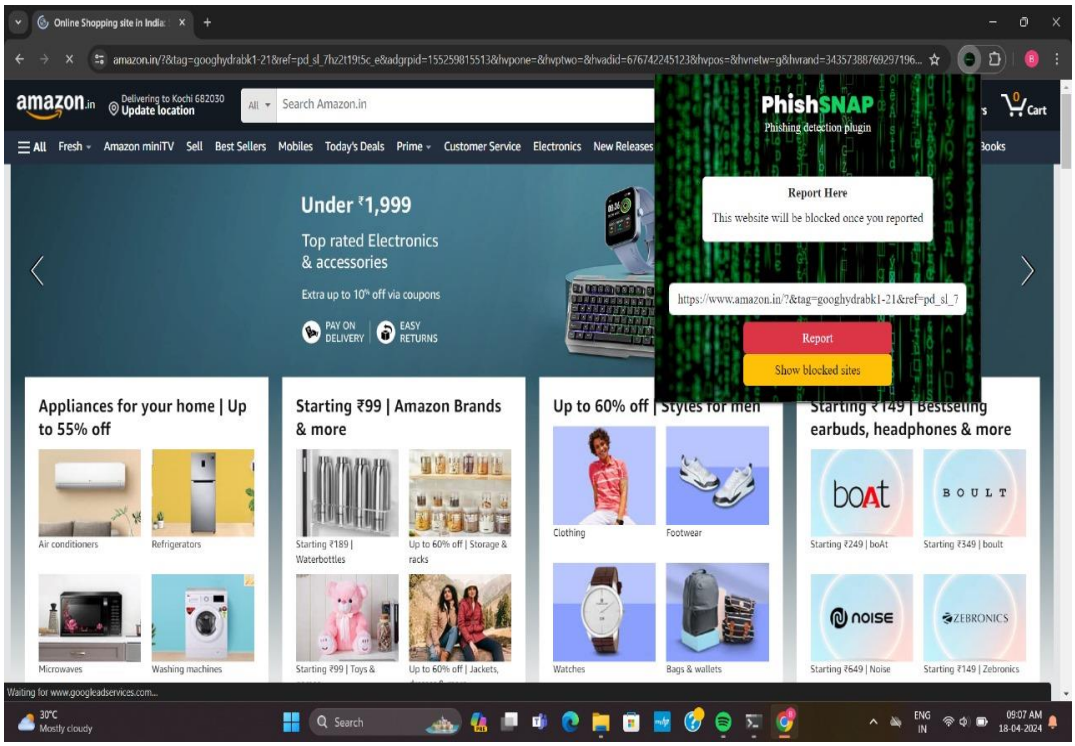


Figure 9(b). Report Option

- **Blocked Sites List**

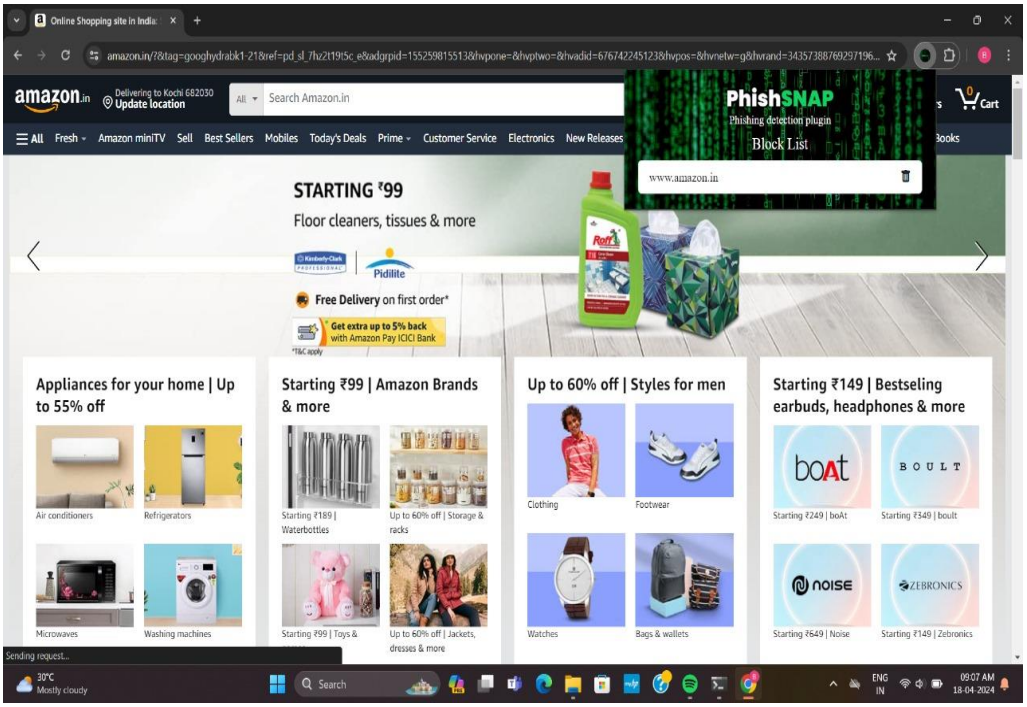


Figure 10. Blocked Sites List

5. Conclusion

In recent years, the proliferation of networking technologies has extended beyond traditional web applications to include mobile and social networking tools, leading to an alarming rise in phishing attacks within cyberspace. These attacks pose significant threats due to their ability to create deceptive webpages that closely resemble legitimate sites in terms of interface and Uniform Resource Locator (URL). Compounded by the inadequacy of existing security measures, this has resulted in a staggering increase in the number of victims falling prey to such scams.

As a primary line of defense, companies often rely on educating employees about the nature of phishing attacks. However, additional protective measures can be instituted by security managers, either in the form of decision support systems for users or as preventative mechanisms implemented on servers. Machine learning (ML) based phishing detection techniques leverage website functionalities to gather information crucial for classifying websites and identifying phishing sites. While the complete eradication of phishing may be

unattainable, proactive measures aimed at improving targeted anti-phishing procedures and enhancing public awareness regarding the detection of fraudulent websites can significantly mitigate its impact.

In response to the ever-evolving and increasingly sophisticated nature of phishing attacks, ML-based anti-phishing techniques have emerged as essential tools. These techniques involve implementing a phishing detection system that utilizes various machine learning algorithms. Notably, ensemble learning, coupled with a second-layer Support Vector Machine (SVM), has been deployed to enhance the efficiency of phishing detection, resulting in notably high accuracy rates. By combining the strengths of multiple machine learning models, this approach produces a more robust logic for identifying phishing attempts.

In summary, combating phishing attacks requires a multifaceted approach that incorporates both technological advancements and user awareness initiatives. ML-based anti-phishing techniques play a pivotal role in this endeavor, offering enhanced detection capabilities and bolstering overall cybersecurity resilience.

References

[1] Taha, “Intelligent ensemble learning approach for phishing website detection based on weighted soft voting,” Mathematics, vol. 9, no. 21, p. 2799, 2021.

[2] Cao, W. Han, and Y. Le, “Anti-phishing based on automated individual whitelist,” in Proceedings of the 4th ACM workshop on Digital identity management, 2008, pp. 51–60.

[3] Maneesha, K. Rajasekhar, K. Prema Latha, and N. Venkata Prasad, “Detection of phreaking website using various algorithms.” International Research Journal on Advanced Science Hub Vol. 05, Issue 05S May pp305 -313

[4] M. Sharifi and S. H. Siadati, “A phishing sites blacklist generator,” in 2008 IEEE/ACS international conference on computer systems and applications. IEEE, 2008, pp. 840–843.

[5] R Kiruthiga and D Akila. Phishing websites detection using machine learning. International Journal of Recent Technology and Engineering, 8(2):111–114, 2019.

[6] S Carolin Jeeva and Elijah Blessing Rajsingh. Intelligent phishing url detection using association rule mining. Human-centric Computing and Information Sciences, 6(1):1–19, 2016.

[7] Ankit Kumar Jain, Brij B Gupta, et al. Phishing detection: analysis of visual similarity based approaches. Security and Communication Networks, 2017, pp 1-20

[8] SA Al-Saaidah. Detecting phishing emails using machine learning techniques. International Journal of Applied Information Systems. Volume 12 – No. 7, October 2017. Pp 21-24

[9] Ashit Kumar Dutta. Detecting phishing websites using machine learning technique. PloS one, 16(10): e0258361, 2021. Pp 1-17

[10] Moitrayee Chatterjee and Akbar-Siami Namin. Detecting phishing websites through deep reinforcement learning. In 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), volume 2, pages 227–232. IEEE, 2019.

[11] Ram B Basnet, Andrew H Sung, and Quingzhong Liu. Learning to detect phishing urls. International Journal of Research in Engineering and Technology, 3(6):11–24, 2014.

[12] Lawrence Abrams. What are google chrome extensions?, 2017.

[13] Subasi, Abdulhamit, Esraa Molah, Fatin Almkallawi, and Touseef J. Chaudhery. "Intelligent phishing website detection using random forest classifier." In 2017 International conference on electrical and computing technologies and applications (ICECTA), pp. 1-5. IEEE, 2017.

[14] "UCI Machine Learning Repository: Phishing Websites Data Set," [Online]. Available: https://archive.ics.uci.edu/ml/datasets/ phishing websites.

[15] Li, Jhen-Hao, and Sheng-De Wang. "PhishBox: An approach for phishing validation and detection." In 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pp. 557-564. IEEE, 2017.

[16] Ahmed, Abdulghani Ali, and Nurul Amirah Abdullah. "Real time detection of phishing websites." In 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 1-6. IEEE, 2016.

Author's biography

ARYA NADH T S :- The author is a final year student pursuing a B.Tech in Computer Science and Engineering at Jawaharlal College of Engineering and Technology. With a passion for innovation and problem-solving, they are dedicated to leveraging their academic training and practical experiences to contribute meaningfully to the field of computer science.

BINITHA P :- The author is a final year student pursuing a B.Tech in Computer Science and Engineering at Jawaharlal College of Engineering and Technology. With a passion for innovation and problem-solving, they are dedicated to leveraging their academic training and practical experiences to contribute meaningfully to the field of computer science.

NIMMI SURESH:- The author is a final year student pursuing a B.Tech in Computer Science and Engineering at Jawaharlal College of Engineering and Technology. With a passion for innovation and problem-solving, they are dedicated to leveraging their academic training and practical experiences to contribute meaningfully to the field of computer science.

PRANAYA V S:- The author is a final year student pursuing a B.Tech in Computer Science and Engineering at Jawaharlal College of Engineering and Technology. With a passion for innovation and problem-solving, they are dedicated to leveraging their academic training and practical experiences to contribute meaningfully to the field of computer science.

UNNIKRISHNAN S KUMAR:-Assistant Professor at Jawaharlal College of Engineering and Technology, Palakkad. He received his B.Tech Degree in Information Technology from Govt. Engineering College, Palakkad and M.Tech in Computer Science and Engineering from the University of Calicut. He has more than ten years of experience in the teaching field and prior experience in the software industry. He has also worked with Sree Narayana Guru Open University, Kerala and written several technical books for BCA students. His research interests include artificial intelligence, image processing, machine learning, computer vision, expert systems, network security, and deep learning**.**