AI-enabled phishing link detection and alert system

Bhalarubeni.V S
Computer Technology

Susil kumar K
Computer Technology

Harish kumar S
Computer Technology

LakshmanaPraksah V
Information Technology

bhalarubeni.ct20@bitsathy.ac.in susilkumar.ct20@bitsathy.ac.in harishkumar.ct20@bitsathy.ac.in lakshmanaprakashs@bitsathy.ac.in

ABSTRACT

Phishing attacks are an ever-present and substantial menace in the realm of cybersecurity. They are cunningly designed to deceive both individuals and organizations, ultimately leading to the unauthorized acquisition of sensitive personal information, account credentials, credit card details, organizational data, or even client passwords, all for malicious purposes. These malicious actors create phishing websites with remarkable skill, expertly mimicking legitimate ones, making it exceptionally challenging to distinguish them from genuine sites. Consequently, phishing attacks stand as one of the most perilous and frequently encountered threats faced by both individuals and organizations. It is important to understand that web URLs serve as gateways to access information on the internet, and these very gateways are exploited by phishing attackers. Recognizing the gravity of this issue, this review paper is dedicated to raising awareness about phishing attacks, bolstering detection methods, and advocating proactive measures for preventing phishing among its readership. Given the staggering volume of phishing emails and messages inundating inboxes daily, it is increasingly arduous for companies and individuals to identify and counter every instance of phishing at tempts. Hence, it becomes paramount to develop and implement effective strategies for combating this persistent and evolving threat

.I. **INTRODUCTION**

The rapid proliferation of technology has firmly entrenched the internet as an indispensable component of our daily lives. A significant portion of our daily activities now relies on internet connectivity. Moreover, the prevalence of social networking sites has witnessed exponential growth in recent years. However, this increased internet usage exposes users to

frequent and malicious threats, one of the most pervasive being 'Phishing.' Phishing involves the deceptive impersonation of legitimate websites to dupe users into divulging

their personal data, including usernames, passwords, account numbers, national insurance numbers, and more. Phishing scams have become one of the most widespread forms of cybercrime in existence today, with countless domains susceptible to attacks, such as online payments, webmail services, financial institutions, file hosting, and cloud storage networks, among others. Notably, webmail and online payment sectors have borne the brunt of phishing attacks. These attacks manifest through various means, including email phishing scams and spear phishing, necessitating user vigilance and a cautious approach to commonly used security applications. In this context, Machine Learning stands out as one of the most effective techniques for detecting phishing attempts, addressing limitations inherent in existing approaches.

The primary objectives of this proposed project are to enhance website validation by identifying and flagging blacklisted URLs. This includes providing users with real-time alerts in the form of pop-ups when attempting to access a blacklisted website. Additionally, it aims to establish a user-friendly platform enabling individuals to independently verify the integrity of any URL they intend to access.

II. LITERATURE REVIEW

The rapid evolution of technology and its pervasive influence across industries have introduced complex security challenges that plague employers and home users alike. Incidents exploiting human vulnerabilities have witnessed a notable surge in recent times. Consequently, a growing emphasis has been placed on bolstering security systems to prioritize prevention and thwart cyberattacks. Cybersecurity professionals are tirelessly searching for robust and dependable techniques to detect phishing websites, given the widespread use of the internet for various activities, including online bill payments, banking transactions, and online shopping. Users face a multitude of security threats, including cybercrime, encompassing spam, fraud, identity theft, cyberterrorism, and phishing, which stands out as one of the most prevalent forms of cybercrime today. Recent reports indicate that phishing ranks among the top three methods of cybercrime, with both the frequency of incidents and user vulnerabilities on the rise. The convergence of these factors poses a significant economic risk.

Phishing, a social engineering attack targeting and exploiting vulnerabilities at the user's end, is the subject of this paper. The paper proposes the use of the Agile Unified Process (AUP) to detect duplicate websites capable of harvesting sensitive user information. The system examines blacklisted sites within a dataset, learns patterns employed by phishing websites, and applies these patterns to incoming inputs. If a user clicks on a phishing link and is redirected to the site, the system triggers a pop-up notification and sends an email alert. It's important to note that this system does not support real-time phishing site detection; users must manually input the website link. The system is developed using Microsoft Visual Studio 2010 Ultimate and relies on MySQL for data storage and database implementation.

Phishing exacts a substantial financial toll on internet users, often exploiting vulnerabilities on the user's side. The proposed solution integrates three hybrid elements: blacklist and whitelist mechanisms, heuristics, and visual similarity analysis. The system follows a series of steps before generating results. Initially, it tracks all "http" traffic on the client system by creating a browser extension. It then compares the domain of each URL with a whitelist of trusted domains and a blacklist of illegitimate ones. Various URL characteristics are considered, including the number of '@' symbols, the number of '-' symbols, and more. The next step involves extracting and comparing the CSS of doubtful URLs with the CSS of legitimate domains in the queue. This approach incorporates visual-based features of phishing websites and employs machine-learning classifiers such as decision trees, logistic regression, and random forests to analyze collected data and generate a score. Both match and similarity scores are evaluated, and if the score exceeds a predefined threshold, the URL is marked as phishing and blocked, thereby providing a three-tiered security approach.

Phishing poses a severe threat aimed at stealing private user data, including addresses, Aadhar numbers, PAN card details, credit or debit card information, bank account details, and personal data. This paper comprehensively discusses various types of phishing attacks, such as spoofing, instant spam spoofing, hosts file poisoning, malware-based phishing, man-in-the-middle attacks, session hijacking, DNS-based phishing, deceptive phishing, keyloggers/loggers, web Trojans, data theft, content-injection phishing, search engine phishing, email/spam attacks, web-based delivery attacks, link manipulation, system reconfiguration, phone phishing, and more. The paper also explores recent approaches to prevent these attacks, including heuristics, blacklists, fuzzy rule-based methods, and machine learning techniques. Ultimately, the paper proposes a framework for detecting and preventing phishing attacks by combining supervised and unsupervised machine learning methods to identify malicious activities based on accuracy and performance metrics.

III. IMPLEMENTATION

A. Feature Extraction

The process of feature extraction involves analyzing URLs and assigning binary values to indicate whether a website is a phishing site or not. The following are the features that can be extracted to detect fraudulent URLs:

IP address in URL: If an IP address is present in the URL, the feature is set to 1; otherwise, it's set to 0. Legitimate websites typically do not use IP addresses in URLs to download webpages. The presence of an IP address suggests an attacker trying to collect sensitive information.

'@' symbol in URL: If the '@' symbol is present in the URL, the feature is set to 1; otherwise, it's set to 0. Hackers often add the '@' symbol to URLs, causing the browser to ignore everything before the '@' symbol and leading users to a different, often malicious, address.

Prefix or Suffix separated by '-' in the domain: If the domain name is separated by a hyphen '-' symbol, the feature is set to 1; otherwise, it's set to 0. Legitimate URLs rarely use hyphens in their domain names, but phishers may add hyphens to make their fraudulent websites appear more legitimate. For instance, a legitimate site could be "http://www.onlineamazon.com," while a phisher might create a fake site like "http://www.onlineamazon.com" to deceive users.

Length of Host name: The average length of benign URLs is approximately 25 characters. If a URL's length exceeds 25 characters, the feature is set to 1; otherwise, it's set to 0.

'HTTPS' token in URL: If the 'HTTPS' token is present in the URL, the feature is set to 1; otherwise, it's set to 0. Phishers may add the "HTTPS" token to the domain part of a URL to trick users.

URL redirection: If "//" is present in the URL path, the feature is set to 1; otherwise, it's set to 0. The presence of "//" within the URL path indicates that the user will be redirected to another website.

B. LOGISTIC REGRESSION

The LOGISTIC REGRESSION, a machine-learning technique, is a core component of this system. It falls under supervised learning and is applicable to both classification and regression problems. The essence of Random Forest lies in associative learning, where multiple classifiers are combined to address complex problems and enhance model efficiency. Instead of relying on a single decision tree, Random Forest employs numerous decision trees on various subsets of the dataset. It then takes the average of their predictions to improve predictive accuracy.

C. Multinomial naive bays

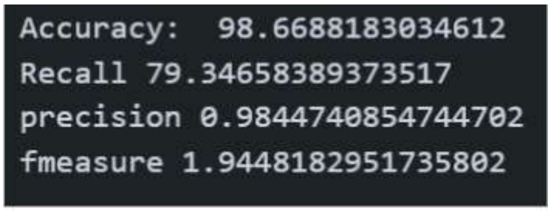
The Multinomial naive bays is another key element of our system, commonly used for classification problems. It utilizes a tree structure where internal nodes represent dataset features, branches indicate decision rules, and leaf nodes signify outcomes. Decision nodes make decisions based on various branches, while leaf nodes represent final outcomes.

The data flow diagram for the proposed system is illustrated above. Additionally, a homepage is presented to users within our system.

IV. RESULTS AND DISCUSSION

The proposed system enhances user safety during browsing and transactions, safeguarding vital credentials from potential leaks. It provides users with a convenient browser extension that quickly determines the legitimacy of a given website. The results demonstrate the system's efficiency, achieved through a hybrid solution involving heuristic and visual features, along with various machine-learning approaches. However, the ever-evolving strategies of notorious hackers pose a continuous challenge. To address this, we have integrated online learning algorithms, ensuring the system adapts to new examples and features of phishing URLs. While the system demonstrates impressive accuracy, there is room for improvement in minimizing minor false positives and false negatives. This can be achieved by incorporating enhanced features for machine learning algorithms, resulting in even greater accuracy.

LET FIND SUSPICIOUS



```
Accuracy:  98.6688183034612
Recall 79.34658389373517
precision 0.9844740854744702
fmeasure 1.9448182951735802
```

V. FUTURE WORK

Future work should focus on directly implementing the project as a Chrome extension. When a user clicks on a URL, the extension can provide a pop-up warning message if the URL is determined to be a phishing site. This streamlined integration would further enhance user protection and convenience. Additionally, ongoing efforts should aim to refine and expand the feature set used for machine learning algorithms to achieve even higher accuracy in phishing detection.

References

[1] Anita S. Kini, A. Nanda Gopal Reddy, Manjit Kaur, S. Satheesh, Thomas Martinetz, Hammam Alshazly, "Ensemble Deep Learning and Internet of Things-Based AutomatedCOVID-19 Diagnosis Framework", Contrast Media & Molecular Imaging, vol. 2022, Article ID 7377502, 10 pages, 2022. https://doi.org/10.1155/2022/7377502

[2] Aditi Sharan, “Term Co-occurrence and Context Window based Combined Approach for Query Expansion with the Semantic Notion of Terms”, International Journal of Web Science(IJWS), Inderscience, Vol. 3, No. 1, 2017.

[3] Saurabh Kumar, S.K. Pathak, "A Comprehensive Study of XSS Attack and the Digital Forensic Models to Gather the Evidence". ECS Transactions, Volume 107, Number 1, 2022.

[4] Yadav, C.S.; Pradhan, M.K.; Gangadharan, S.M.P.; Chaudhary, J.K.; Khan, A.A.; Haq, M.A.; Alhussen, A.; Wechtaisong, C.; Imran, H.; Alzamil, Z.S.; Pattanayak, H.S. “Multi-Class Pixel Certainty Active Learning Model for Classification of Land Cover Classes Using Hyperspectral Imagery”. Electronics 2022, 11, 2799. https://doi.org/10.3390/electronics11172799.

[5] Yadav, C.S.; Yadav, A.; Pattanayak, H.S.; Kumar, R.; Khan, A.A.; Haq, M.A.; Alhussen, A.; Alharby, S. “Malware Analysis in IoT & Android Systems with Defensive Mechanism”. Electronics 2022, 11, 2354. https://doi.org/10.3390/electronics11152354.

[6] A Goswami, D Sharma, H Mathuku, SMP Gangadharan, CS Yadav, “Change Detection in Remote Sensing Image Data Comparing Algebraic and Machine Learning Methods”, Electronics, Article id: 1505208, 2022

[7] Singh, J. “An Efficient Deep Neural Network Model for Music Classification”, Int. J. Web Science, Vol. 3, No. 3, 2022.

[8] Vijay Kumar Bohat, “Neural Network Model for Recommending Music Based on Music Genres”, In 10th IEEE International Conference on Computer Communication and Informatics (ICCCI - 2021), Jan. 27-29, 2021, Coimbatore, INDIA.

[9] Singh, J., “Learning based Driver Drowsiness Detection Model”, In 3rd IEEE International Conference on Intelligent Sustainable Systems (ICISS 2020), , pp. 1163-1166, Palladam, India, Dec. 2020.

[10] A. Sharan, “Rank fusion and semantic genetic notion based automatic query expansion model”, Swarm and Evolutionary Computation, Vol-38, Elsevier, 2018.

[11] R. Singh, “Ranks Aggregation and Semantic Genetic Approach based Hybrid Model for Query Expansion ", International Journal of Computational Intelligence Systems, Vol. 10 (2017) 34– 55.

[12] A. Sharan, “A new fuzzy logic based query expansion model for efficient information retrieval using relevance feedback approach”, Neural Computing And Applications, Vol 28, Springer, 2017.

[13] Chin-Teng Lin, Mukesh Prasad, Chia-Hsin Chung, Deepak Puthal, Hesham El-Sayed, Sharmi Sankar, Yu-Kai Wang, Jagendra Singh, Arun Kumar Sangaiah, “IoT-based Wireless Polysomnography Intelligent System for Sleep Monitoring", IEEE Access, Vol 6, Oct 2017

[14] Mukesh Prasad, Yousef Daraghmi, Prayag Tiwari, Pranay Yadav, Neha Bharill, “Fuzzy Logic Hybrid Model with Semantic Filtering Approach for Pseudo Relevance Feedback- based Query Expansion”, 2017 IEEE Symposium Series on Computational Intelligence (SSCI), 2017.

[15] Rakesh Kumar, “Lexical Co-Occurrence and Contextual Window-Based Approach with Semantic Similarity for Query Expansion”, International Journal of Intelligent Information Technologies (IJIIT), IGI, Vol. 13, No. 3, pp. 57-78, 2017.

[16] Aditi Sharan, “Term Co-occurrence and Context Window based Combined Approach for Query Expansion with the Semantic Notion of Terms”, International Journal of Web Science(IJWS), Inderscience, Vol. 3, No. 1, 2017.

[17] Mukesh Prasad, Om Kumar Prasad, Er Meng Joo, Amit Kumar Saxena and Chin- Teng Lin, “A Novel Fuzzy Logic Model for Pseudo-Relevance Feedback-Based Query Expansion”, International Journal of Fuzzy Systems, Springer, Vol 18, 2016.

[18] A. Sharan, “Ranks aggregation and semantic genetic approach based hybrid model for query expansion”, International Journal of Computational Intelligence Systems, Taylor & Francis, Vol. 10, Issue 1, 2017, Pages 34 - 55

[19] A. Sharan, “Relevance Feedback based Query Expansion Model using Ranks Combining and Word2vec Approach”, IETE- Journal of Research, Taylor & Francis, Vol 62, 2016.

[20] K. Singh and Aditi Sharan, “Relevance feedback based query expansion model using Borda count and semantic similarity approach”, Computational Intelligence and Neuroscience, Article ID: 568197, pp. 1-14, 2015.