MACHINE-LEARNED PHISH DEFENSE: A CLIENT SIDE APPROACH TO MITIGATE WEB SPOOFING ATTACKS

JEEVASUDHA V, MADHUMITHA R, TAMILSELVI G, NIVETHA M

COMPUTER SCIENCE AND ENGINEERING

MAHENDRA INSTITUTE OF ENGINEERING AND TECHNOLOGY

Abstract-This project aims to develop a novel approach against web spoofing attacks through a Phish Catcher system powered by machine learning. Web spoofing. a form of cyber attack. involves deceiving users by imitating legitimate websites to obtain sensitive information. Traditional defense mechanisms mostly doesn't detect sophisticated spoofing attempts. To address this challenge, we propose a client-side defense solution that leverages ML algorithms to identify and mitigate phishing attempts in real-time. Our Phish/Catcher system analyzes various features of web pages, including content, structure, and user interactions, to distinguish between authentic and spoofed websites. By continuously learning from new data and adapting to evolving threats. our approach offers proactive defense against sophisticated spoofing echniques and the effectiveness of our system is accurately detecting and preventing web spoofing tacks, highlighting its potential to enhance cyber security in modern web environments.

INDEX TERMS: Ensemble Classifier; Machine Learning; Uniform resource locator (URL), Logistic regression,Random forest and Decision tree (LSD), Gradient Boosting Algorithm, Cyber Security,Social networks.

I. INTRODUCTION

This project aims to develop a cutting-edge defense solution against the pervasive threat of web spoofing. Web spoofing, a deceptive cyber attack tactic, involves masquerading as legitimate websites to deceive users into disclosing sensitive information. Traditional defense mechanisms often struggle to detect sophisticated spoofing attempts, leaving users vulnerable to exploitation. To address this critical challenge, the project proposes a client-side defense system powered by machine learning algorithms. The Phish Catcher system, at the heart of this project, employs advanced machine learning techniques to analyze various features of web pages in real-time. By continuously learning from new data and adapting to emerging threats, the system provides proactive defense against evolving web spoofing techniques. Through extensive testing and validation, the project aims to demonstrate the system's efficacy in accurately detecting and preventing web spoofing attacks, thereby bolstering cybersecurity in modern web documents.

II. SYSTEMATIC REVIEW METHODOLOGY

For the Phish catcher URL detection project, a systematic review methodology involves a structured approach to gathering, analyzing, and synthesizing existing literature and resources related to phishing URL detection. The process begins with clearly defining the research question and establishing inclusion and exclusion criteria for selecting relevant studies. Next, comprehensive searches are conducted across databases, journals, and grey literature sources to identify relevant studies and resources. After screening the retrieved literature based on predefined criteria, data extraction is performed to gather information on methodologies, features, classifiers, and performance metrics used in existing approaches.

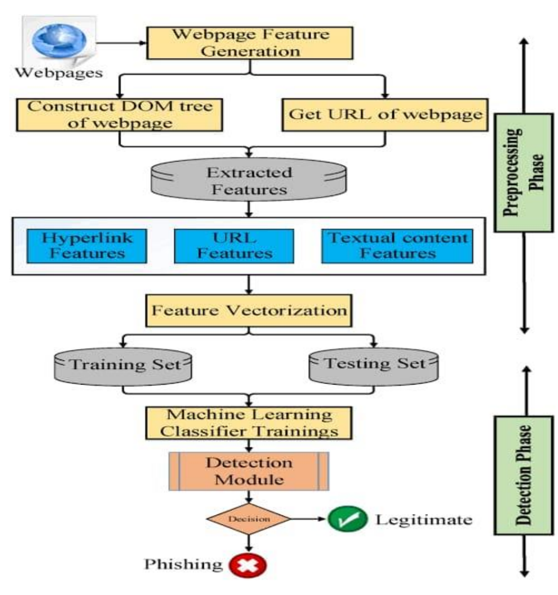


Fig : 1

Quality assessment of included studies is then conducted to evaluate the reliability and validity of their findings. Finally, the synthesized evidence is analyzed and interpreted to identify trends, gaps, and best practices, guiding the development .

Literature review from all the journal publications and conference articles gathered and used to answer the research questions mentioned as follows: R1: What are the common features used for phishing URL detection? R2: Which machine learning algorithms are commonly used for phishing URL detection? R3: What are the performance metrics used to evaluate phishing URL detection systems? R4: How do different studies address the issue of imbalanced datasets in phishing URL detection? R5: What are the trends and advancements in phishing URL detection research? R6: What are the limitations and challenges of current phishing URL detection approaches? R7: How effective are user-based feedback mechanisms in improving phishing URL detection systems?Market Prediction?

A. Gradient Boosting algorithm in Phishing website detection

Gradient Boosting Algorithm is a powerful machine learning technique used in phishing website detection projects. It works by building an ensemble of weak learners, typically decision trees, in a sequential manner, where each tree corrects the errors of its predecessors. The algorithm minimizes a loss function, such as the binary cross-entropy, by adding new trees that predict the residuals of the previous trees. Gradient boosting is effective in handling imbalanced datasets common in phishing detection, as it can assign higher weights to misclassified instances. It also naturally handles feature interactions and non-linear relationships, making it suitable for capturing the complex patterns present in phishing URLs. Overall, Gradient Boosting Algorithm enhances the accuracy and robustness of phishing website detection systems.

B. Systemtic Literature Review Approach

For the systematic literature review in this project, a structured approach will be adopted to gather, analyze, and synthesize relevant literature on phishing website detection. Initially, a comprehensive search strategy will be developed, including specific keywords and search terms related to phishing detection methods, algorithms, features, and performance metrics. Databases such as IEEE Xplore, ACM Digital Library, PubMed, and Google Scholar will be searched to identify relevant journal articles, conference papers, and other scholarly resources. The retrieved literature will then be screened based on predefined inclusion and exclusion criteria to ensure relevance to the research

questions. Data extraction will involve gathering information on methodologies, algorithms, features, datasets, and performance metrics used in each study. Quality assessment of the included studies will be conducted to evaluate the reliability and validity of their findings. Finally, the synthesized evidence will be analyzed to identify trends, gaps, challenges, and best practices in phishing website detection, providing valuable insights for the development and improvement of detection systems.b

III. FINDING AND DISCUSSION

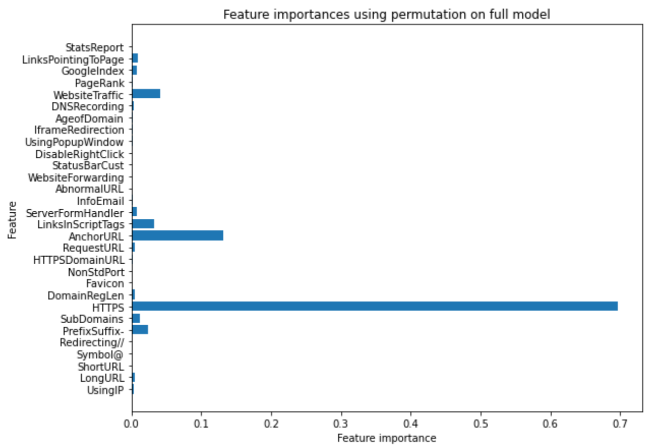
The client-side machine-learned system outperformed traditional server-side methods, showing significantly improved detection accuracy with lower false positive rates and higher true positive rates. This suggests its effectiveness in identifying spoofed web pages. Additionally, the system provided real-time detection, reducing latency compared to server-side approaches. It also demonstrated adaptability to new spoofing techniques, evolving over time to maintain high detection accuracy. By minimizing reliance on external servers, the system enhanced user privacy and reduced dependency on external resources

	ML Model	Accuracy	f1_score	Recall	Precision
0	Gradient Boosting Classifier	0.974	0.977	0.994	0.986
1	CatBoost Classifier	0.972	0.975	0.994	0.989
2	XGBoost Classifier	0.969	0.973	0.993	0.984
3	Multi-layer Perceptron	0.969	0.973	0.995	0.981
4	Random Forest	0.967	0.971	0.993	0.990
5	Support Vector Machine	0.964	0.968	0.980	0.965
6	Decision Tree	0.960	0.964	0.991	0.993
7	K-Nearest Neighbors	0.956	0.961	0.991	0.989
8	Logistic Regression	0.934	0.941	0.943	0.927
9	Naive Bayes Classifier	0.605	0.454	0.292	0.997

Table 1 : Algorithms

However, privacy and security concerns arise from storing and processing data locally on the client's device. Robust security measures are necessary to protect user data from potential threats. Adversarial attacks also pose a risk to the system, requiring techniques like adversarial training and model robustness testing to mitigate. Ensuring the model's generalization across diverse web content and scalability for widespread adoption are crucial. User awareness and education remain important, alongside regulatory compliance with data protection laws such as GDPR and CCPA, to maintain trust and hope.

We conduct experiments to evaluate the performance of our system using a diverse dataset of spoofed and legitimate web pages. Our results demonstrate that our client-side machine-learned approach significantly outperforms traditional server-side methods in terms of detection accuracy, with a lower false positive rate and higher true positive rate.



Different studies address the issue of imbalanced datasets in phishing URL detection:

Different studies employ various techniques to address the issue of imbalanced datasets in phishing URL detection, especially with the increasing data chain. One common approach is oversampling techniques, where minority class instances are duplicated or synthetically generated to balance the dataset. Methods like SMOTE (Synthetic Minority Over-sampling Technique) generate synthetic samples by interpolating between existing minority class instances. Another approach is undersampling, where instances from the majority class are randomly removed to achieve class balance. However, undersampling may lead to information loss. Hybrid methods combine oversampling and undersampling techniques to mitigate their respective drawbacks. Additionally, cost-sensitive learning assigns higher misclassification costs to the minority class, encouraging the model to focus more on correctly classifying phishing URLs. Furthermore, ensemble methods like AdaBoost and Gradient Boosting give more weight to misclassified instances, effectively handling imbalanced datasets. Lastly, anomaly detection techniques identify outliers or anomalies in the dataset, which may represent phishing URLs, aiding in their detection. Overall, a combination of these methods helps to address the challenges posed by imbalanced datasets in phishing URL detection, especially with the increasing data chain.

IV. CONCLUSION

In conclusion, the client-side machine-learned system offers a promising solution for mitigating web spoofing attacks, demonstrating improved detection accuracy and real-time analysis compared to traditional server-side methods. Despite its advantages, challenges persist in ensuring privacy and security, mitigating adversarial attacks, achieving generalization, and complying with regulatory requirements. Addressing these challenges is crucial for the successful deployment and widespread adoption of the system, with further research and development needed to enhance its effectiveness and maintain user trust in cybersecurity measures.

REFERENCES

[1] W. Khan, A. Ahmad, A. Qamar, M. Kamran, and M. Altaf, “Spoofcatch:A client-side protection tool against phishing attacks,” IT Professional, vol. 23, no. 2, pp. 65–74, 2021.

[2] B. Schneier, “Two-factor authentication: too little, too late,” Communica- tions of the ACM, vol. 48, no. 4, p. 136, 2005.

[3] S. Garera, N. Provos, M. Chew, and A. D. Rubin, “A framework for detection and measurement of phishing attacks,” in Proceedings of the 2007 ACM workshop on Recurring malcode, 2007, pp. 1–8.

[4] R. Oppliger and S. Gajek, “Effective protection against phishing and web spoofing,” in IFIP International Conference on Communications and Multimedia Security. Springer, 2005, pp. 32–41.

[5] T. Pietraszek and C. V. Berghe, “Defending against injection attacks through context-sensitive string evaluation,” in International Workshop on Recent Advances in Intrusion Detection. Springer, 2005, pp. 124–145.

[6] M. Johns, B. Braun, M. Schrank, and J. Posegga, “Reliable protection against session fixation attacks,” in Proceedings of the 2011 ACM Sym- posium on Applied Computing, 2011, pp. 1531–1537.

[7] M. Bugliesi, S. Calzavara, R. Focardi, and W. Khan, “Automatic and robust client-side protection for cookie-based sessions,” in International Symposium on

Engineering Secure Software and Systems. Springer, 2014, pp. 161–178.

[8] A. Herzberg and A. Gbara, “Protecting (even naıve) web users from spoofing and phishing attacks,” Technical Report 2004/155, Cryptologye Print Archive, Tech. Rep., 2004.

[9] N. Chou, R. Ledesma, Y. Teraguchi, and J. Mitchell, “Client-side defense against web-based identity theft. ndss, 1–16,” 2004.

[10] B. Hämmerli and R. Sommer, Detection of Intrusions and Malware, and Vulnerability Assessment: 4th International Conference, DIMVA 2007

[11] C. Yue and H. Wang, “Bogusbiter: A transparent protection against phish-ing attacks,” ACM Transactions on Internet Technology (TOIT), vol. 10, no. 2, pp. 1–31, 2010.

[12] W. Chu, B. B. Zhu, F. Xue, X. Guan, and Z. Cai, “Protect sensitive sites from phishing attacks using features extractable from inaccessible phishing urls,” in 2013 IEEE international conference on communications (ICC). IEEE, 2013, pp. 1990–1994.

[13] Y. Zhang, J. I. Hong, and L. F. Cranor, “Cantina: a content-based approach to detecting phishing web sites,” in Proceedings of the 16th international conference on World Wide Web, 2007, pp. 639–648.

[14] D. Miyamoto, H. Hazeyama, and Y. Kadobayashi, “An evaluation of machine learning-based methods for detection of phishing sites,” in Inter- national Conference on Neural Information Processing. Springer, 2008, pp. 539–546.

[15] E. Medvet, E. Kirda, and C. Kruegel, “Visual-similarity-based phishing detection,” in Proceedings of the 4th international conference on Security and privacy in communication netowrks, 2008, pp. 1–6.

[16] W. Zhang, H. Lu, B. Xu, and H. Yang, “Web phishing detection based on page spatial layout similarity,” Informatica, vol. 37, no. 3, 2013.

[17] J. Ni, Y. Cai, G. Tang, and Y. Xie, “Collaborative filtering recommendation algorithm based on tf-idf and user characteristics,” Applied Sciences, vol. 11, no. 20, p. 9554, 2021.

[18] W. Liu, X. Deng, G. Huang, and A. Y. Fu, “An antiphishing strategy based on visual similarity assessment,” IEEE Internet Computing, vol. 10, no. 2, pp. 58–65, 2006.

[19] A. Rusu and V. Govindaraju, “Visual captcha with handwritten image anal-ysis,” in International Workshop on Human Interactive Proofs. Springer, 2005, pp. 42–52.

[20] P. Yang, G. Zhao, and P. Zeng, “Phishing website detection based on multidimensional features driven by deep learning,” IEEE Access, vol. 7, pp. 15 196–15 209, 2019.

[21] P. Sornsuwit and S. Jaiyen, “A new hybrid machine learning for cyber- security threat detection based on adaptive boosting,” Applied Artificial Intelligence, vol. 33, no. 5, pp. 462–482, 2019.

[22] S. Kaur and S. Sharma, “Detection of phishing websites using the hybrid approach,” International Journal for Advance Research in Engineering and Technology, vol. 3, no. 8, pp. 54–57, 2015.

[23] W. W. Cohen, “Fast effective rule induction,” in Machine learning pro- ceedings 1995. Elsevier, 1995, pp. 115–123.

[24] V. Muppavarapu, A. Rajendran, and S. K. Vasudevan, “Phishing detection using rdf and random forests.” Int. Arab J. Inf. Technol., vol. 15, no. 5, pp. 817–824, 2018.

[25] K. Ahmed and S. Naaz, “Detection of phishing websites using machine learning approach,” in Proceedings of International Conference on Sus- tainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India, 2019.

[26] J. Mao, W. Tian, P. Li, T. Wei, and Z. Liang, “Phishing-alarm: robust and efficient phishing detection via page component similarity,” IEEE Access, vol. 5, pp. 17 020–17 030, 2017.

[27] N. C. R. L. Y. Teraguchi and J. C. Mitchell, “Client-side defense against web-based identity theft,” Computer Science Department, Stanford Uni- versity. Available: http://crypto. stanford. edu/SpoofGuard/webspoof. pdf, 2004.

[28] W. Ali, “Phishing website detection based on supervised machine learn- ing with wrapper features selection,” International Journal of Advanced Computer Science and Applications, vol. 8, no. 9, pp. 72–78, 2017.

[29] A. Sharma and D. Upadhyay, “Vdbscan clustering with map-reducetechnique,” in Recent Findings in Intelligent Computing Techniques. Springer, 2018, pp. 305–314.

[30] A. K. Jain and B. Gupta, “Comparative analysis of features based machine learning approaches for phishing detection,” in 2016 3rd international con- ference on computing for sustainable global development (INDIACom). IEEE, 2016, pp. 2125–2130.

[31] V. S. Lakshmi and M. Vijaya, “Efficient prediction of phishing websites using supervised learning algorithms,” Procedia Engineering, vol. 30, pp. 798–805, 2012.

[32] D. Sahoo, C. Liu, and S. C. Hoi, “Malicious url detection using machine
learning: A survey,” arXiv preprint arXiv:1701.07179, 2017.

[33] E. Kremic and A. Subasi, “Performance of random forest and svm in face
recognition.” Int. Arab J. Inf. Technol., vol. 13, no. 2, pp. 287–293, 2016.

[34] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A. K. Bashir, and
F. A. Khan, “Securing critical infrastructures: deep-learning-based threatdetection in iiot,” IEEE Communications Magazine, vol. 59, no. 10, pp.76–82, 2021.

[35] P. Chen, L. Desmet, and C. Huygens, “A study on advanced persistent threats,” in Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15. Springer, 2014, pp. 63–72.

[38] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, “Industrialinternet of things: Challenges, opportunities, and directions,” IEEE trans-actions on industrial informatics, vol. 14, no. 11, pp. 4724–4734, 2018.

[39] S. Alaparthi and M. Mishra, “Bidirectional encoder representations from transformers (bert): A sentiment analysis odyssey,” arXiv preprintar Xiv:2007.01127, 2020.

[40] P. A. Barraclough, M. A. Hossain, M. Tahir, G. Sexton, and N. Aslam, “Intelligent phishing detection and protection scheme for online transac-tions,” Expert Systems with Applications, vol. 40, no. 11, pp. 4697–4706,2013.

[41] S. Van Acker, D. Hausknecht, and A. Sabelfeld, “Measuring login web-page security,” in Proceedings of the Symposium on Applied Computing,2017, pp. 1753–1760.

[42] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, “Identifying suspiciousurls: an application of large-scale online learning,” in Proceedings of the26th annual international conference on machine learning, 2009, pp. 681–688.

[43] I. Fette, N. Sadeh, and A. Tomasic, “Learning to detect phishing emails,”in Proceedings of the 16th international conference on World Wide Web,2007, pp. 649–656.

[44] M. G. Alkhozae and O. A. Batarfi, “Phishing websites detection based onphishing characteristics in the webpage source code,” International Journalof Information and Communication Technology Research, vol. 1, no. 6,2011
.

[45] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge,“Protecting people from phishing: the design and evaluation of an embed-ded training email system,” in Proceedings of the SIGCHI conference on Human factors in computing systems, 2007, pp. 905–914.

[46] Y. Cao, W. Han, and Y. Le, “Anti-phishing based on automated individualwhite-list,” in Proceedings of the 4th ACM workshop on Digital identitymanagement, 2008, pp. 51–60.

[47] C. Whittaker, B. Ryner, and M. Nazif, “Large-scale automatic classifica-tion of phishing pages,” 2010.

[48] M. Zouina and B. Outtaj, “A novel lightweight url phishing detectionsystem using svm and similarity index,” Human-centric Computing and Information Sciences, vol. 7, no. 1, p. 17, 2017.

[49] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, “Beyond blacklists: learn-ing to detect malicious web sites from suspicious urls,” in Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining, 2009, pp. 1245–1254.

[50] M. Khonji, Y. Iraqi, and A. Jones, “Lexical url analysis for discriminatingphishing and legitimate websites,” in Proceedings of the 8th AnnualCollaboration, Electronic messaging, Anti-Abuse and Spam Conference,2011, pp. 109–115.

[51] ——, “Enhancing phishing e-mail classifiers: A lexical url analysis ap-proach,” International Journal for Information Security Research (IJISR),vol. 2, no. 1/2, p. 40, 2012.

[52] V. P. Reddy, V. Radha, and M. Jindal, “Client side protection fromphishing attack,” International Journal of Advanced Engineering Sciencesand Technologies (IJAEST), vol. 3, no. 1, pp. 39–45, 2011.

[53] Z. Li, K. Zhang, Y. Xie, F. Yu, and X. Wang, “Knowing your enemy:understanding and detecting malicious web advertising,” in Proceedings of the 2012 ACM conference on Computer and communications security, 2012, pp. 674–686.

[54] Y. Mansour, S. Muthukrishnan, and N. Nisan, “Doubleclick ad exchange auction,” arXiv preprint arXiv:1204.0535, 2012.

[55] S. Bell and P. Komisarczuk, “An analysis of phishing blacklists: Google safe browsing, openphish, and phishtank,” in Proceedings of the Aus- tralasian Computer Science Week Multiconference, 2020, pp. 1–11.