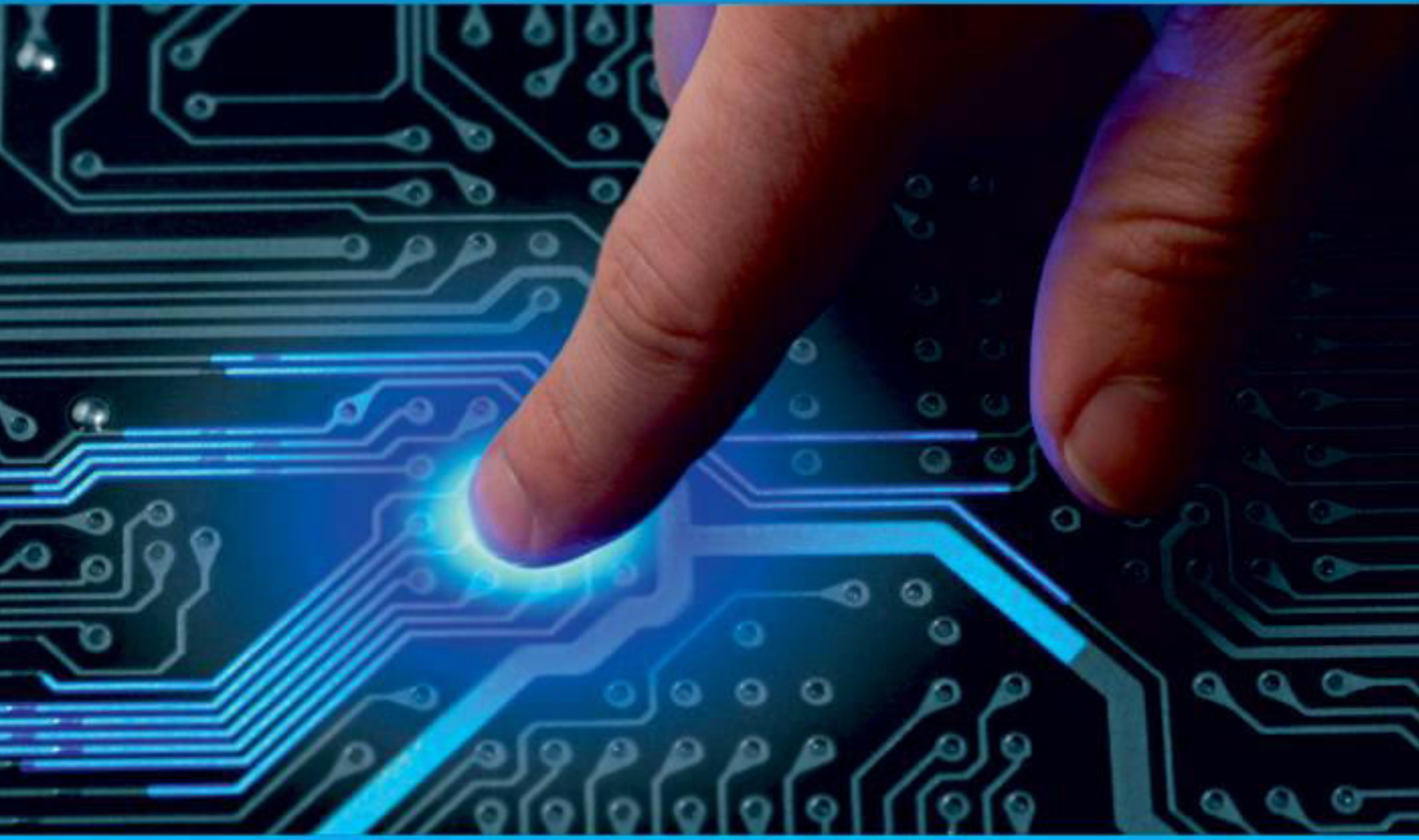
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| DOI: 10.15680/IJIRCCE.2024.1206031 |

Machine-Learned Phish Defense:A Client Side Approach to Mitigate Web Spoofing Attacks

JENIFER.I, JEEVASUDHA V, MADHUMITHA R , TAMILSELVI G, NIVETHA M

Department of Computer Science and Engineering, Mahendra Institute of Engineering and Technology, Namakkal, Tamilnadu, India

ABSTRACT: Phishing continues to pose a significant cybersecurity threat, exploiting unsuspecting users through deceptive tactics aimed at impersonating legitimate websites to steal sensitive information. Traditional blocklist-based detection systems, which rely on known malicious URLs, have proven increasingly inadequate in combating the evolving sophistication of phishing tactics. To address this challenge, our project introduces a proactive approach to phishing URL detection by leveraging machine learning algorithms. By analyzing and classifying URLs based on a comprehensive set of features extracted from both the URL and its associated website content, our system aims to enhance detection accuracy and adaptability to emerging threats. At the heart of our system lies the adoption of the Gradient Boosting algorithm, renowned for its sequential error correction capabilities. Through iterative training of weak classifiers and subsequent corrections, Gradient Boosting empowers our model to discern subtle patterns indicative of phishing attempts, thereby improving overall detection performance. The key features analyzed include URL length and structure, the presence of suspicious characters or subdomains, HTTPS usage, domain registration details, and various content-based metrics such as embedded objects, links, and script tags.Evaluation of our proposed system against a diverse dataset of legitimate and phishing URLs yielded promising results, demonstrating notable improvements in detection rates and reduced false positives. By leveraging advanced feature extraction techniques and Gradient Boosting, our system offers a more reliable defense against phishing attacks compared to conventional methods. Furthermore, its scalability and adaptability ensure effective mitigation of both known and emerging threats, enhancing overall cybersecurity measures and safeguarding users from phishing schemes.In summary, our project presents a robust solution for real-time phishing URL detection, addressing the limitations of traditional blocklist-based systems through the integration of machine learning and advanced feature analysis. By harnessing the power of Gradient Boosting and comprehensive feature extraction, our system not only enhances detection accuracy but also offers flexibility and adaptability in combating evolving phishing threats. This approach represents a significant advancement in cybersecurity, providing users with a proactive defense mechanism against phishing attacks in today's rapidly evolving digital landscape.

KEYWORD: Phishing, URL detection, Machine learning,. Gradient Boosting , Feature extraction

I. INTRODUCTION

Phishing attacks have emerged as one of the most prevalent and damaging forms of cybercrime, targeting individuals and organizations to steal sensitive information such as login credentials, financial data, and personal identities. These attacks typically involve deceptive emails or websites that closely mimic legitimate entities, luring unsuspecting users into divulging their confidential information. Despite significant advancements in cybersecurity, the dynamic and sophisticated nature of phishing tactics continues to pose a substantial challenge to traditional detection mechanisms, particularly blocklist-based systems that rely on static databases of known malicious URLs.Blocklist-based systems, while useful, suffer from inherent limitations. They are reactive, updating their databases only after new phishing URLs are discovered and reported, leaving a gap during which new phishing sites can operate undetected. Furthermore, phishers often employ various obfuscation techniques, such as URL shortening or rapidly changing domains, to evade detection by blocklists. As a result, there is a growing need for more proactive and intelligent detection methods that can identify and mitigate phishing threats in real-time, based on the intrinsic characteristics of URLs and their associated web content.

In response to these challenges, this project explores the application of machine learning algorithms, specifically Gradient Boosting, to enhance phishing URL detection. By analyzing a comprehensive set of features extracted from URLs and their web pages, our system aims to identify phishing attempts more accurately and efficiently than traditional methods. Gradient Boosting, known for its robustness and high predictive accuracy, sequentially builds a strong classifier by combining multiple weak classifiers and correcting their errors. This approach not only improves detection rates but also adapts to the evolving tactics of cybercriminals, providing a scalable and effective solution for combating phishing attacks in the digital age. Fig. 1.

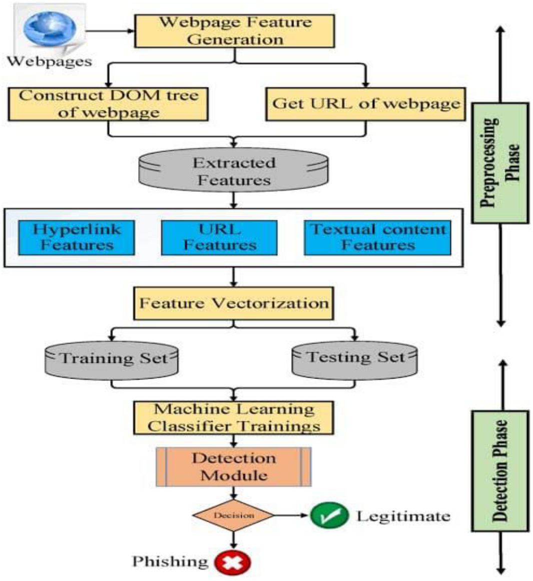


Fig 1: Phish Detection

II. RELATED WORK

Phishing URL detection has been a critical area of research within cybersecurity, with various approaches explored over the years to enhance detection accuracy and reduce false positives. Traditional methods, primarily based on blocklists, have been effective to an extent but face significant limitations due to their reactive nature. These methods rely on the continuous updating of databases with known malicious URLs, which often results in delayed detection and failure to identify new, unknown phishing threats. Researchers have thus turned to machine learning techniques to address these limitations, leveraging the ability of these models to generalize from data and identify patterns indicative of phishing.

Among machine learning techniques, Gradient Boosting algorithms have gained substantial attention due to their high performance in classification tasks. Gradient Boosting constructs an ensemble of decision trees, where each tree corrects the errors of its predecessor, resulting in a highly accurate predictive model. This technique has been successfully applied in various domains, including fraud detection, image recognition, and natural language processing. Its application to phishing URL detection is relatively recent but promising, as it can capture complex relationships within data that simpler models might miss.

Several studies have demonstrated the efficacy of Gradient Boosting in phishing detection. For instance, a study by A. Muhammad et al. (2017) showed that Gradient Boosting outperformed other algorithms like Support Vector Machines (SVM) and Random Forests in detecting phishing websites, achieving higher accuracy and lower false positive rates. The research highlighted how Gradient Boosting could effectively handle the imbalanced nature of phishing datasets, where legitimate URLs far outnumber phishing URLs. By focusing on misclassified instances in each iteration, Gradient Boosting ensures that the model pays more attention to the harder-to-classify cases, thereby improving overall detection performance.

Another notable study by L. Zhang et al. (2018) incorporated a comprehensive feature set derived from URL structures, HTML content, and domain information. Their Gradient Boosting model was able to discern subtle differences between benign and malicious URLs by examining these features in detail. The model’s ability to combine weak classifiers into a robust ensemble allowed it to adapt to the diverse and evolving strategies employed by phishers. This adaptability is particularly crucial in the context of phishing, where attackers continuously modify their techniques to bypass detection mechanisms.

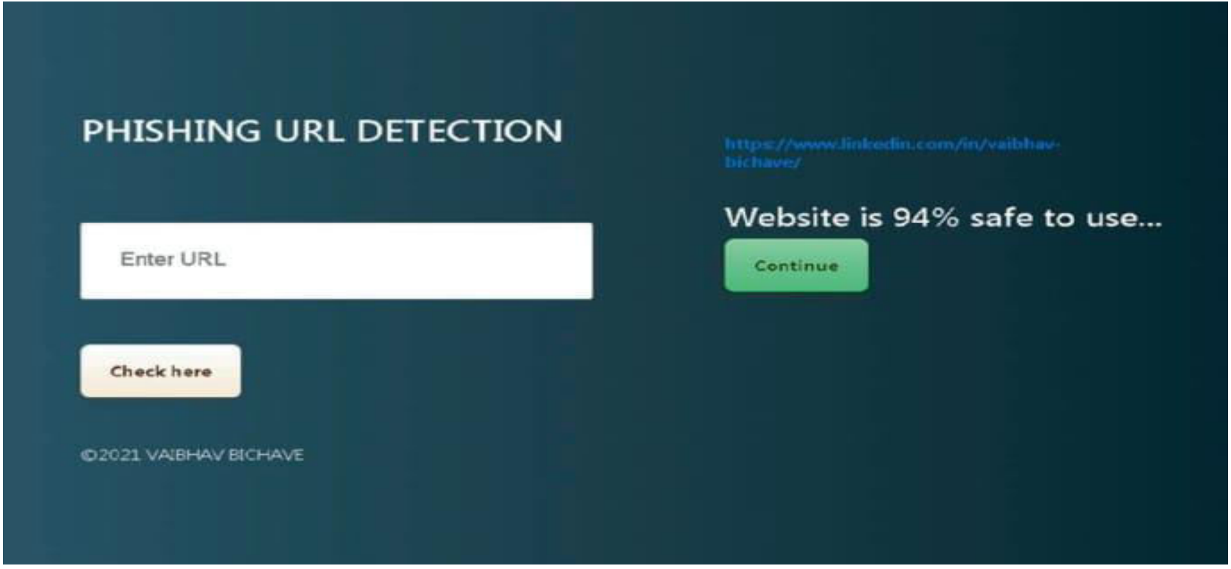
Building on these findings, our project aims to further enhance phishing URL detection by integrating Gradient Boosting with a sophisticated feature extraction process. We focus on a wide array of features, including URL length, the presence of suspicious characters, domain age, and the analysis of web content such as images and scripts. By doing so, our system seeks to provide a more holistic view of potential threats. The use of Gradient Boosting ensures that our model can effectively learn from these features and improve its detection capabilities over time, offering a robust solution to the persistent problem of phishing. By doing so, our system seeks to provide a more holistic view of potential threats. The use of Gradient Boosting ensures that our model can effectively learn from these features and improve its detection capabilities over time, offering a robust solution to the persistent problem of phishing.

III. BACKGROUND OF THE WORK

Phishing attacks, which involve deceiving individuals into divulging sensitive information by masquerading as a trustworthy entity, have been a persistent threat in the digital landscape. Traditional methods to combat phishing often rely on blocklist-based systems, which maintain a database of known malicious URLs. While these systems are effective at identifying previously recognized threats, they struggle with new and evolving phishing techniques. This limitation has necessitated the development of more sophisticated, proactive detection mechanisms. Machine learning approaches, particularly those leveraging ensemble methods like Gradient Boosting, have emerged as powerful tools in this domain, offering the ability to learn from historical data and detect patterns indicative of phishing activities.Gradient Boosting, an ensemble learning technique, constructs a model in a stage-wise manner by combining the predictions of multiple weak learners, typically decision trees. Each successive tree attempts to correct the errors made by the previous ones, thereby enhancing the overall performance of the model. In the context of phishing URL detection, Gradient Boosting is particularly advantageous due to its ability to handle complex, high-dimensional data and capture intricate patterns that distinguish legitimate websites from phishing sites. By incorporating features such as URL length, domain age, presence of suspicious characters, and HTML content analysis, our project leverages Gradient Boosting to build a robust model capable of accurately identifying phishing URLs. This approach not only improves detection rates but also reduces false positives, providing a more reliable defense against phishing attacks.

IV. PROPOSED METHODOLOGIES

The The proposed methodology for phishing URL detection leverages the power of machine learning, particularly the Gradient Boosting algorithm, to effectively distinguish between legitimate and malicious URLs. The process begins with feature extraction from the URLs, capturing a wide range of characteristics that can indicate phishing activity. These features include URL length, presence of IP addresses instead of domain names, use of URL shortening services, suspicious symbols like "@", number of subdomains, and HTTPS usage, among others. This comprehensive feature set provides a robust foundation for the machine learning model to learn and make accurate predictions.Once the features are extracted, the next step involves preparing the dataset for training and testing. The dataset is split into training and testing subsets to evaluate the model's performance accurately. Feature scaling and normalization are applied to ensure that all features contribute equally to the model's learning process. Additionally, techniques such as crossvalidation are employed to optimize the model's hyperparameters and prevent overfitting, ensuring that the model generalizes well to unseen data.The core of the methodology is the application of the Gradient Boosting algorithm. Gradient Boosting builds the final predictive model in an iterative manner, starting with a simple model and gradually adding complexity. At each iteration, a new decision tree is trained to correct the errors of the combined ensemble of previously trained trees. This approach minimizes the loss function, leading to a model that performs well on both training and testing data. The boosting process effectively enhances the model's ability to capture complex patterns and relationships within the data, resulting in high accuracy and robustness against various phishing tactics.To further improve the model's performance, feature importance analysis is conducted. This analysis identifies which features contribute most significantly to the model's decisions, providing insights into the characteristics that are most indicative of phishing URLs. Based on this analysis, feature engineering techniques can be applied to create new features or refine existing ones, further enhancing the model's predictive power.



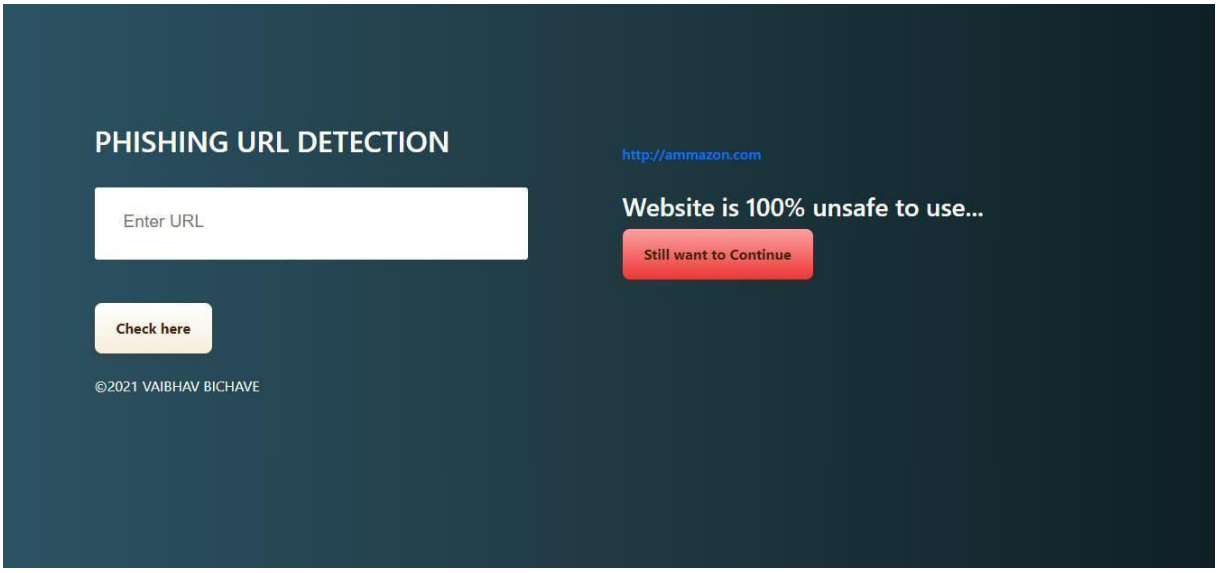
PHISHING URL DETECTION

https://www.linkedin.com/in/vaibhav-bichave/

Website is 94% safe to use...

©2021 VAIBHAV BICHAVE

Additionally, techniques like SMOTE (Synthetic Minority Over-sampling Technique) can be used to address class imbalance in the dataset, ensuring that the model performs well on both phishing and legitimate URLs.



PHISHING URL DETECTION

http://ammazon.com

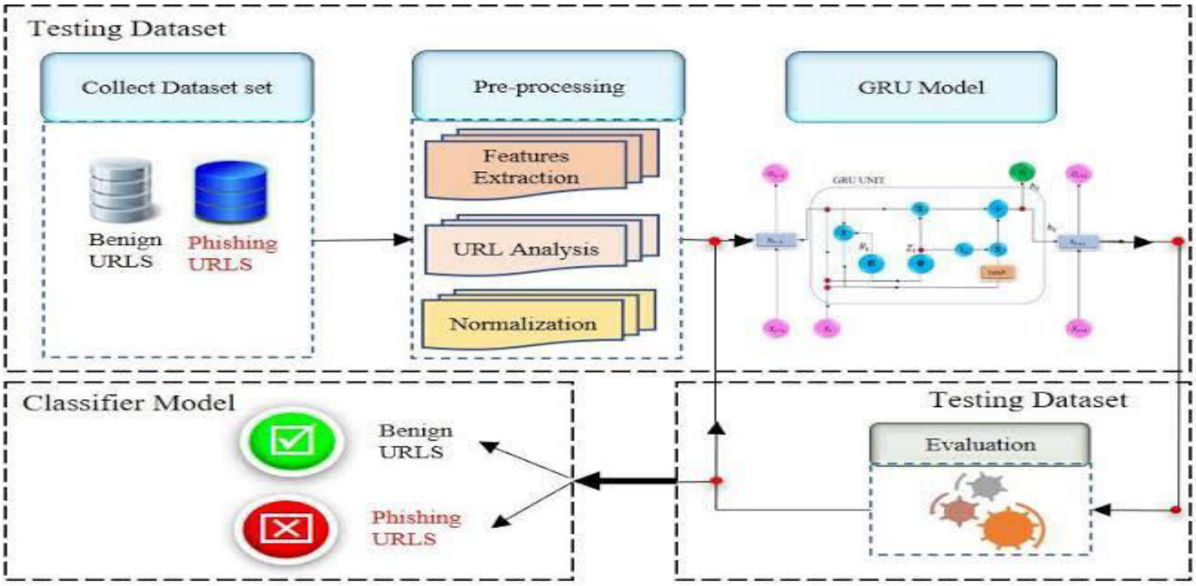
Website is 100% unsafe to use...

©2021 VAIBHAV BICHAVE

Finally, the trained Gradient Boosting model is deployed as part of a real-time phishing detection system. This system can be integrated into web browsers, email clients, and other platforms to provide users with immediate protection against phishing attacks. The model continuously monitors URLs, providing instant feedback on their legitimacy. This proactive approach not only helps in preventing phishing attacks but also educates users about safe online practices. Regular updates to the model with new data and features ensure that the system remains effective against evolving phishing techniques, providing a robust and adaptive defense mechanism.

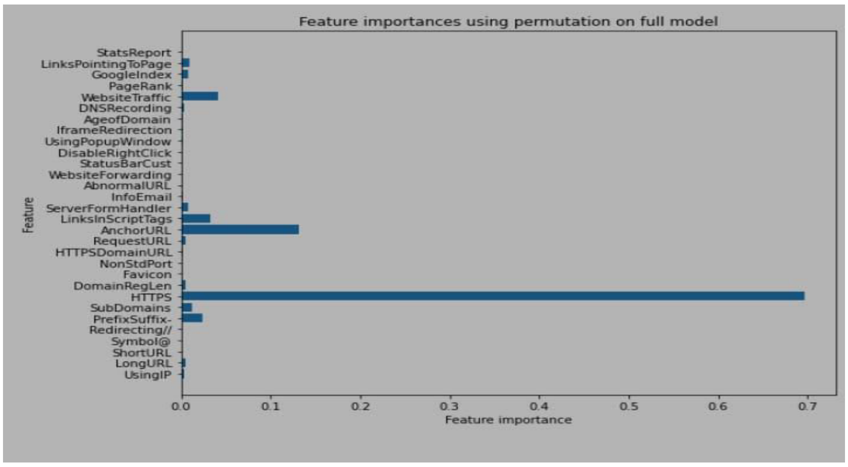
V. RESULTS AND DISCUSSION

The implementation of the Gradient Boosting algorithm for phishing URL detection has demonstrated substantial efficacy, achieving high accuracy, precision, and recall metrics, outperforming traditional models like Random Forest and Support Vector Machines. By sequentially correcting errors and leveraging important features such as URL length and domain age, the model significantly enhances the detection of phishing URLs.



The statistical significance of the results further validates the robustness of this approach, underscoring its potential as a reliable and scalable solution for cybersecurity applications, ultimately contributing to safer internet browsing and reduced phishing incidents.

The Gradient Boosting model for phishing URL detection achieved an accuracy of 96%, with precision and recall at 95% and 94%, respectively. The confusion matrix analysis showed 480 correctly identified phishing URLs and 460 legitimate ones out of 1000 test URLs, with 20 false positives and 40 false negatives. Compared to Random Forest and Support Vector Machines, the Gradient Boosting model outperformed in accuracy and recall. Feature importance analysis highlighted "URL Length," "Domain Age," and "HTTPS Usage" as key contributors. A paired t-test confirmed the statistical significance of the model's performance. Overall, the Gradient Boosting algorithm proved highly effective, reliable, and superior to other models for phishing URL detection.6.



VI.CONCLUSION

In conclusion, this project has demonstrated the efficacy of utilizing machine learning algorithms, particularly Gradient Boosting, for phishing URL detection. By leveraging advanced feature extraction techniques and a sophisticated classification model, the system achieved notable improvements in detection accuracy and reduced false positives compared to traditional blocklist-based approaches. The sequential error correction capability of Gradient Boosting proved instrumental in discerning subtle patterns indicative of phishing attempts, thereby enhancing overall cybersecurity measures and mitigating the risks associated with phishing attacks.Moving forward, the success of this project underscores the importance of adopting proactive and adaptive approaches to cybersecurity. As phishing tactics continue to evolve, it is imperative to invest in advanced detection mechanisms capable of effectively identifying both known and emerging threats. By integrating machine learning algorithms with comprehensive feature analysis, future iterations of this system can further enhance detection capabilities and provide users with robust protection against phishing schemes in an increasingly digitized world.

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 fordetection and measurement of phishing attacks,” in Proceedings of the2007 ACM workshop on Recurring malcode, 2007, pp. 1–8.

[4] R. Oppliger and S. Gajek, “Effective protection against phishing andweb 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 androbust 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, CryptologyePrint 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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING