IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

Ensemble Model for Detecting Phishing and Trojan using Latest Machine Learning Technique

Vaibhav Bhamare[1], Krishna Deore[2], Anand Sonawane[3], Dhikale Shubham[4]
Prof. Vidya Kale[5]
Department of Information Technology[1,2,3,4,5]
Matoshri Aasarabai Polytechnic, Eklahare, Nashik, Maharashtra, India

Abstract: *Phishing is an online threat where an attacker impersonates an authentic and trustworthy organization to obtain sensitive information from a victim. One example of such is trolling, which has long been considered a problem. However, recent advances in phishing detection, such as machine learning-based methods, have assisted in combatting these attacks. Therefore, this paper develops and compares four models for investigating the efficiency of using machine learning to detect phishing domains. It also compares the most accurate model of the four with existing solutions in the literature. These models were developed using artificial neural networks(ANNs), support vector machines (SVMs), decision trees (DTs), and random forest (RF)techniques. Moreover, the uniform resource locator's (URL's) UCI phishing domains dataset is used as a benchmark to evaluate the models. Our findings show that the model based on the random forest technique is the most accurate of the other four techniques and outperforms other solutions in the literature.*

Keywords: phishing detection; machine learning; phishing domains; artificial neural networks; support vector machine; decision tree; random forest

I. INTRODUCTION

In today's hyper connected digital landscape, the threats posed by phishing and trojan attacks have become increasingly sophisticated and pervasive. These malicious activities can lead to severe data breaches, financial losses, and reputational damage for individuals and organizations alike. Consequently, the need for robust and efficient cybersecurity measures has never been more pressing. Machine learning, with its ability to analyze vast amounts of data and identify patterns, has emerged as a critical tool in the fight against cyber threats. However, the constantly evolving nature of these threats demands advanced techniques to stay ahead of attackers. In this context, ensemble models using the latest machine learning techniques have emerged as a compelling approach to bolster the security of digital systems and protect against phishing and trojan attacks. This ensemble model combines the strengths of multiple machine learning algorithms and models to create a unified and formidable defense against malicious activities. Therefore, different decision support or detection systems have been developed to protect the end user against phishing attacks.
Different approaches are used in these systems, such as Blacklists, Rule-based systems, Similarity-based systems, and Machine
Learning based systems, etc. The literature was reviewed in detail, and the studies in this context were examined carefully. Currently, machine learning-based systems are especially preferred for its protection mechanism to the zero-day attacks. Therefore, in this paper, it is aimed to implement a phishing detection system based on a machine learning algorithm for investigating the URL address of the target web page. With the idea of existing improvable ways of the designed system, it is aimed at the detection of phishing attacks in a short time, without the need for third-party services, and also without waiting for the blacklists to be updated. The project is organized as follows: in the next section, the literature review is included. In the third section, the details of the designed system are explained. In the fourth section and fifth section, the results obtained in the experiments are shared, and conclusion and future studies are drawn, respectively.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

II. RESEARCH METHODOLOGY

1. Data Collection and Preprocessing:

• Gather a comprehensive dataset containing both phishing and non-phishing/trojan examples.
• Employ advanced data preprocessing techniques, including feature extraction and data cleaning.
• Extract relevant features such as URLs, domain attributes, email content, and behavioral patterns.

2. Model Selection:

• Utilize the latest machine learning techniques:
• Deep Learning: Implement Convolutional Neural Networks (CNNs) for image-based phishing detection and Recurrent Neural Networks (RNNs) for text-based detection.
• Ensemble Methods: Leverage Gradient Boosting (e.g., XGBoost), Random Forests, and LightGBM for structured data.

3. Ensemble Techniques:

• Create an ensemble of models to improve overall detection performance:
• **Voting Classifier**: Combine predictions from various base models through majority voting.
• **Stacking:** Train a meta-model to learn from diverse base model predictions.
• **Bagging**: Employ Bootstrap Aggregating techniques, e.g., Random Forests, to build multiple models on data subsets.
• **Boosting:** Implement algorithms like AdaBoost or Gradient Boosting to iteratively enhance model performance.

4. Cross-Validation and Hyperparameter Tuning:

• Conduct cross-validation to assess ensemble performance and mitigate overfitting.
• Fine-tune hyperparameters to optimize the model for accuracy and robustness.

5. Real-time Implementation:

• Address the challenges associated with real-time detection, focusing on efficient model deployment and inference.
• Implement mechanisms for handling streaming data and rapidly evolving threats.

6. Evaluation Metrics:

• Evaluate model performance using metrics such as accuracy, precision, recall, F1-score, ROC AUC, and confusion matrices.
• Conduct comprehensive testing with diverse datasets, including real-world scenarios.

III. LITERATURE SURVEY

Rao et al. [6] proposed a novel classification approach that use heuristic based feature extraction approach. In this, they have classified extracted features into three categories such asURL Obfuscation features, Third-Party-based features, Hyperlink-based features. Moreover, proposed technique gives 99.55% accuracy. Drawback of this is that as this model uses third party features, classification of website dependent on speed of third-party services. Also this model is purely depends on the quality and quantity of the training set and Broken links feature extraction has a limitation of more execution time for the websites with more number of links.

Chunlinetal. proposed approach that primarily focus on character frequency features. In this they have combined statistical analysis of URL with machine learning technique to get result thatis more accurate for classification of malicious URLs. Also they have compared six machine learning algorithms to verify the effectiveness of proposed algorithm which gives 99.7% precision with false positive rate less than 0.4%.

Sudhanshu et al. used association data mining approach. They have proposed rule based classification technique for phishing website detection. They have concluded that association classification algorithm is better than any otheralgorithms because of their simple rule transformation. They achieved 92.67% accuracy byextracting 16 features but this is not up to mark so proposed algorithm can be enhanced forefficient detection rate.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

M. Amaad et al presented a hybrid model for classification ofphishing website. In this paper, proposed model carried out in two phase. In phase 1,theyindividually perform classification techniques, and select the best three models based on highaccuracy and other performance criteria. While in phase 2, they further combined each individual model with best three model and makes hybrid model that gives better accuracy than individua lmodel. They achieved 97.75% accuracy on testing dataset. There is limitation of this model that it requires more time to build hybrid model.

Hosseinetal developed an open-source framework known as "Fresh-Phish". For phishing websites, machine-learning data can be created using this framework. In this, they have used reduced features set and using python forbuilding query .They build a large labelled dataset and analyse several machine-learning classifiers against this dataset .Analysis of this gives very good accuracy using machine-learning classifiers. These analyses how long time it takes to train the model. Gupta et al. proposed an ovel anti phishing approach that extracts features from client-side only. Proposed approach is fast and reliable as it is not dependent on third party but it extracts features only from URL and source code.

IV. SYSTEM ARCHITECTURE

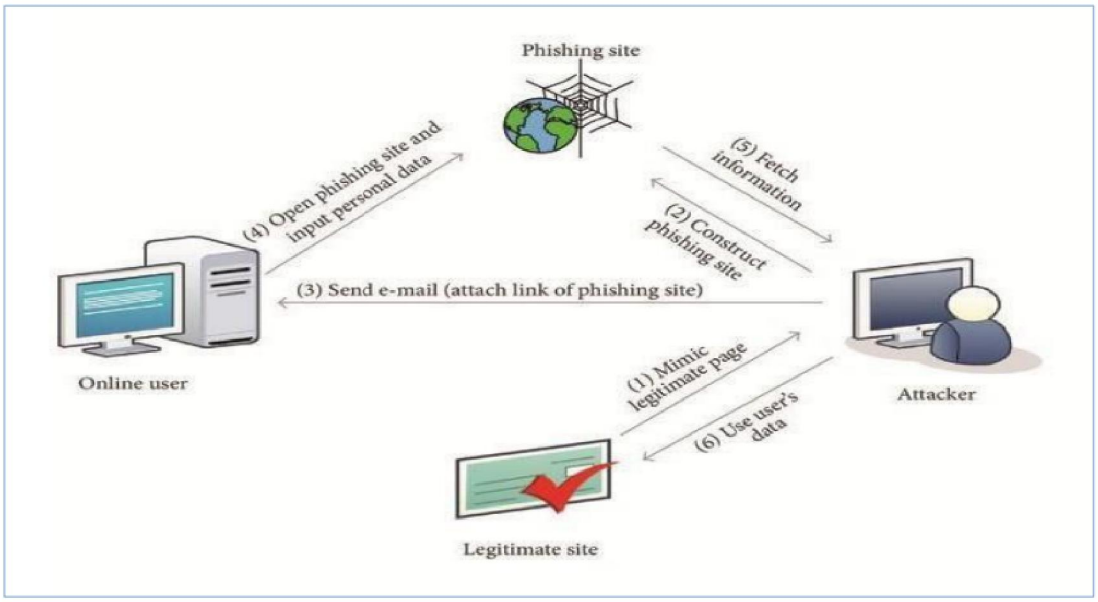

Figure 1: Architecture Diagram

V. MODELLING AND ANALYSIS

We are using waterfall model for our project.

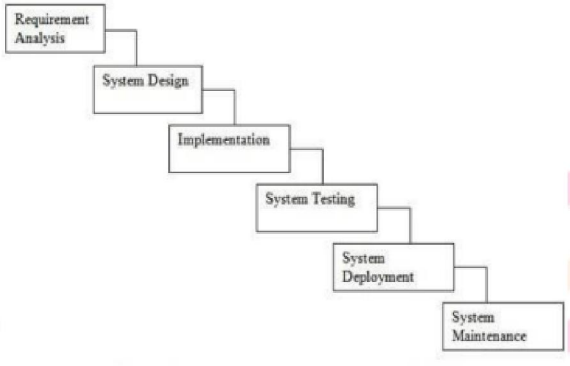

Figure 2: Waterfall Model

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

Requirement Gathering and Analysis: In this step of waterfall we identify what are various requirements are need for our project such are software and hardware required, database, and interfaces. System Design: In this system design phase we design the system which is easily understood for end user i.e. user friendly. We design some UML diagrams and data flow diagram to understand the system flow and system. module and sequence of execution.

- Testing: The different test cases are performed to test whether the project module are giving expected outcome in assumed time. All the units developed in the implementation phase are integrated into a system after testing of each unit. Post integration the entire system is tested for any faults and failures.
- Deployment of System: Once the functional and non-functional testing is done, the product is deployed in the customer environment or released into the market.
- Maintenance: There are some issues which come up in the client environment. To fix those issues patches are released. Also to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment. All these phases are cascaded to each other in which progress is seen as flowing steadily downwards like a waterfall through the phases. The next phase is started only after the defined set of goals are achieved for previous phase and it is signed off, so the name Waterfall Model. In this model phases do not overlap.

VI. CONCLUSION

An ensemble model for detecting phishing and trojan attacks using the latest machine learning techniques offers a promising approach to bolster cybersecurity defenses. Despite the challenges, the advantages in accuracy and robustness make it a valuable tool in identifying malicious activities, particularly in a continuously evolving threat landscape. Ongoing research and development are essential to harness the full potential of ensemble models for this critical task.

REFERENCES

[1]. Cabaj, K.; Domingos, D.; Kotulski, Z.; Respício, A. Cybersecurity Education: Evolution of the Discipline and Analysis of Master Programs.Comput.Secur. 2018, 75, 24–35. [CrossRef]
[2]. Iwendi, C.; Jalil, Z.; Javed, A.R.; Reddy, G.T.; Kaluri, R.; Srivastava, G.; Jo, O. KeySplitWatermark: Zero Watermarking Algorithm for Software Protection Against CyberAttacks. IEEE Access 2020, 8, 72650–72660. [CrossRef]
[3]. RehmanJaved, A.; Jalil, Z.; AtifMoqurrab, S.; Abbas, S.; Liu, X. Ensemble AdaboostClassifier for Accurate and Fast Detection of Botnet Attacks in Connected Vehicles. Trans. Emerg. Telecommun.Technol. 2020, 33, e4088. [CrossRef]
[4]. Conklin,W.A.; Cline, R.E.; Roosa, T. Re-Engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. In Proceedings of the 2014 47th Hawaii International Conference on System Sciences, IEEE,Waikoloa, HI, USA, 6–9 January 2014;pp. 2006– 2014.
[5]. Javed, A.R.; Usman, M.; Rehman, S.U.; Khan, M.U.; Haghighi, M.S. Anomaly Detection in Automated Vehicles Using Multistage Attention-Based Convolutional Neural Network. IEEE Trans. Intell. Transp. Syst. 2021, 22, 4291–4300. [CrossRef]
[6]. Mittal, M.; Iwendi, C.; Khan, S.; RehmanJaved, A. Analysis of Security and Energy Efficiency for Shortest Route Discoveryin Low-energy Adaptive Clustering Hierarchy Protocol Using Levenberg-Marquardt Neural Network and Gated Recurrent Unit forIntrusion Detection System. Trans. Emerg. Telecommun.Technol. 2020, 32, e3997. [CrossRef]
[7]. Bleau, H.; Global Fraud and Cybercrime Forecast. Retrieved RSA 2017. Available online: https://www.rsa.com/en-us/resources/ 2017-global-fraud (accessed on 19 November 2021).
[8]. Computer Fraud & Security. APWG: Phishing Activity Trends Report Q4 2018. Comput.Fraud Secur.2019, 2019, 4. [CrossRef]
[9]. Hulten, G.J.; Rehfuss, P.S.; Rounthwaite, R.; Goodman, J.T.; Seshadrinathan, G.; Penta, A.P.; Mishra, M.; Deyo, R.C.; Haber, E.J.; Snelling, D.A.W. Finding Phishing Sites; Google Patents: Microsoft Corporation, Redmond,WA, USA, 2014.