International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.013 ISSN: 2581-4621

Advanced Phishing Protection Techniques

Mamatha.P
Assistant professor,CSE Department,AVN Institute of Engineering and Technology,Hyderabad,Telangana,India.

Abstract:
The performance of phishing prevention and detection system can be highly improved through the use of advanced machine learning models.Traditional systems often rely on simple pattern recognition,but newer approaches employ complex algorithms to interpret subtle and contextual hints around phishing activities.Such systems can identify phishing threats more accurately by combining models such as Deep Neural Networks(DNNs),Random Forests,and Support Vector Machines(SVMs).Through analysis of complex patterns,SVMs are very good at separating phishing from genuine messages.By merging multiple decision trees,Random Forests enhance detection and reduce susceptibility to a range of phishing attacks.Abnormalities in data and complex features are detected by DNNs due to their deep layers.These advanced classifiers combined work towards the development of a more advanced concept of phishing,resulting in better detection and reduced false positives.

Keywords:Phishing detection and prevention,Support Vector Machine,Random Forests,Deeep Neural Network.

I.INTRODUCTION

Phishing attacks remain a significant cybersecurity threat by illegitimately taking advantage of system and human weaknesses.Conventionally,phishing detection tools depend on simple pattern matching,and it doesn't work against advanced attacks.A potential solution is new machine learning,which learns and processes the sophisticated,subtle hints of phishing attacks through advanced algorithms.Deep Neural Networks(DNNs),Random Forests,with support vector machine models(SVMs)are among the leading ones in this approach.Through the utilization of intricate patterns of analysis for differentiating legitimate communication from phishing,SVMs can attain valid categorization.Through the compilation of several decision trees,Random Forests drive detection accuracy maximally while abiding by the broad spectrum of phishing methods.DNNs,meanwhile,utilize hierarchical structure to distinguish situational discrepancies and advanced anomalies in phishing databases.By incorporating these advanced models into phishing detection systems,accuracy might be enhanced and false positives eliminated,providing a stronger defense against dynamically changing threats[1].

II.LITERATURE SURVEY

Card fraud poses a significant threat to banks as well as consumers with increasing numbers of credit and debit card transactions becoming a normal part of life online.Fraudsters continue to find vulnerabilities despite the existence of many security features,including the need to send OTPs to consumers'phones and inboxes.Cloud-based financial databases are more vulnerable to these types of attacks,which result in huge economic losses and security issues.Preventive solutions have not been exhaustively studied yet,and available solutions center on post-entry authentication processes[1].

As the number of internet users increased,so has crime,mainly phishing.Apart from the usual ones like phishing URLs,emails,or websites,phishing attacks now aim at social media and gaming sites as well.We came up with a machine learning-based Twitter spear phishing tool to tackle this.To enhance detection precision,we tried different classifiers to identify phishing URLs,emails,as well as websites,with special focus on training time optimization.The objective of this book is to apply machine learning to phishing detection and prevention[2].

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.013 ISSN: 2581-4621

This work discusses how employees'psychological characteristics and behavioral issues affect their susceptibility to email phishing attacks,across various departmental contexts in an organization.The work evaluates the extent to which these characteristics drive susceptibility to phishing.The writer suggests a means by which companies can create anti-phishing solutions tailored to fit specific psychological and behavioral patterns associated with increased risk.This way,the solution seeks to better the efficacy of phishing defense since it addresses each employee's vulnerability[3].

In a business culture of networks,phishing poses an important threat by attempting to secure sensitive data illegally.Phishing attacks are being developed in the form of highly sophisticated and deceptive attacks that cannot be detected.In order to detect valid compared to forged URLs,we utilized a neural network as a binary classifier.Its performance was considered on the metric of binary classification accuracy,based on how accurately it can segregate legitimate versus phishing URLs[4].

Phishing endangers personal data,affecting individuals,cloud storage services,and government agencies.Software methods provide an easier solution than hardware anti-phishing tools,which are often expensive and unpopular.A heuristic approach that labels links as non-phishing phishing based on input parameters such as online traffic and URLs has been suggested since existing models cannot cope with zero-day phishing attacks[5].

III.SYSTEM ARCTITECTURE.

Obtaining the required dataset is the initial and most crucial step in our process.To counter the evolving nature driving phishing attack strategies with their rising sophistication,we have selected three publicly known datasets with diverse features.This enables us to investigate how diverse features influence the effectiveness of the model in phishing detection.We purified the data sets after acquiring them by removing duplicates,introducing missing data,and applying instance balancing to produce maximum correctness.The training set of 70%as well as the testing set of 30%were developed based on the purged data.[2]The proportion is generally used to make certain that the model employs an ample amount of testing data and high amounts of training data to optimize classification[6].

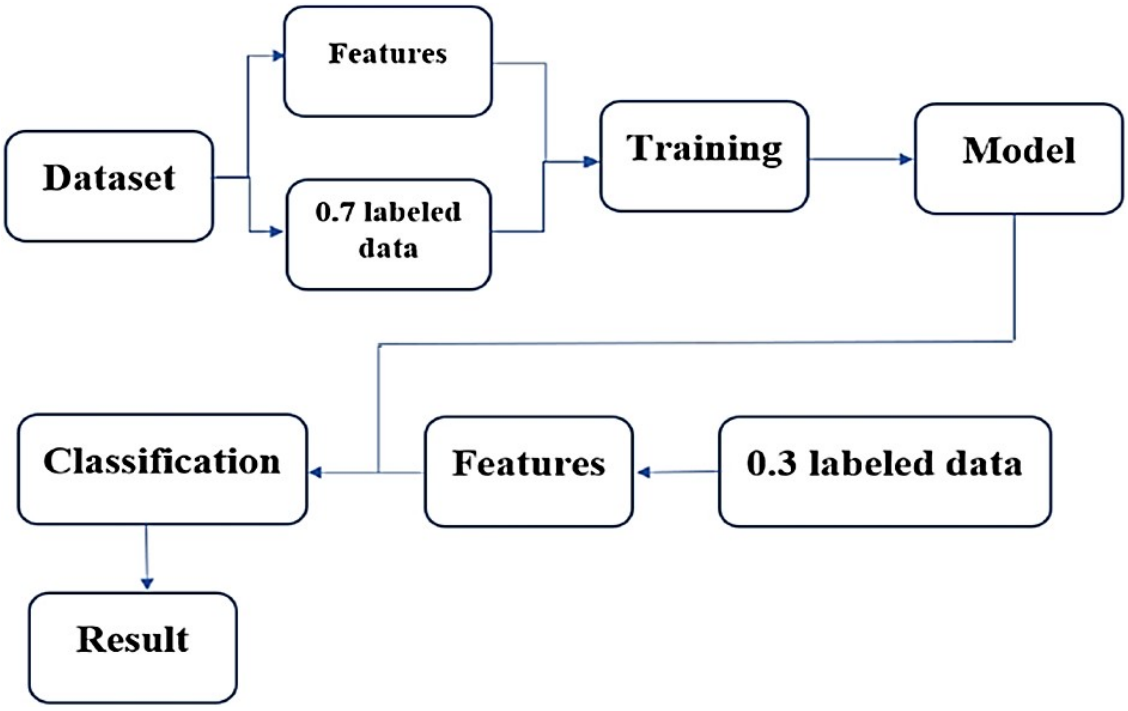

Fig 1:Proposed detection model

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.013 ISSN: 2581-4621

The second phase,the training phase,is gained by executing the machine learning algorithm to train the classifier model in accordance with 70%of the training set dataset.Under this phase,the model learns to label an email as spam or authentic based on features involved.[4]Once training has been accomplished,the model may then proceed to classify a new email into either spam or authentic classes in accord with learned rule[5].

IV.METHODOLOGY

SVMs are employed to discriminate URLs or messages by creating a decision boundary that separates phishing attempts from real ones.SVMs analyze the feature space by finding the hyperplane with maximum margin among different classes(non-phishing and phishing).This is achieved by utilizing complex pattern recognition technique to identify subtle variations in features,such as URL structure and the metadata[6].By mapping data onto a higher-dimensional space,SVMs can discriminate between authentic and phishing messages that contain sophisticated patterns[7].SVMs are good classifiers,hence are effective in phishing attempt detection based on thorough pattern and feature inspection,thus improving the accuracy of the overall phishing detection system.

Random Forests are used to improve detection performance via aggregation of the results from a set of decision trees.Random Forests construct an ensemble of decision trees,with each tree being trained on different subsets of data and feature set.[8]Each decision tree gives a classification,and the final decision is obtained by the majority vote of all decision trees.This ensemble makes it easy to treat many different phishing techniques with effective detection of different patterns and features.Random Forests enhance the robustness and accuracy of the phishing detection system through reducing the probability of overfitting and consolidating multiple views of decision-making,which facilitates dealing with diverse phishing strategies[9].

DNNs are employed to uncover detailed anomalies and context-specific nuances in phishing data through their hierarchical design.DNNs utilize a number of neuron layers to capture high-level complex abstractions from data.[10]Every layer captures different features or patterns,progressively building an entire picture of the input data.In phishing detection,this means that DNNs can recognize deep and intricate patterns and contextual cues that other simpler models cannot identify,including hidden phishing tactics or unusual combinations of traits.[11]DNNs allow detailed phishing data analysis and allow the detection system to capture deep and subtle phishing attacks that may be lost with traditional approaches.This results in more effective detection and fewer false alarms[12].

Combining SVMs,Random Forests,and DNNs in one system for phishing detection.Through uniting all these cutting-edge algorithms,the system integrates the advantages of each method.SVMs handle intricate pattern processing,Random Forests improve resistance and precision through ensemble learning,and DNNs provide deep insights in intricate data patterns.This merging gives a holistic method of identifying phishing.[12]The merger of these models gives a more sophisticated defense against the evolving phishing attacks,improving the general accuracy and dependability of the system for detecting phishing with fewer false positives.From this trio of algorithms DNNS offers beset accuracy[13].

V.CONCLUSION.

To summarize,since the phishing attacks become increasingly more subtle,traditional methods of detection fail to cope with the intelligence of modern-day attacks.Blending the state-of-the-art machine learning models with Support Vector Machines(SVMs),Random Forests,and Deep Neural Networks(DNNs)has turned out to be substantially effective against the detection of phishing.These include Deep Neural Networks,which stand out for their excellent performance as a result of their

DOI:10.46647/ijetms.2025.v09si01.013 ISSN: 2581-4621

ability to learn subtle patterns and contextual nuances from their stacked model.DNNs possess the ability to discover slight abnormalities and complex features that other models might miss,resulting in the highest accuracy in the detection of phishing attempts.By leveraging the deep learning capability of DNNs,phishing detection systems can be made more accurate and reduce false positives,and hence a more effective defense against evolving cyber attacks.

VI.FUTURE WORK

Future research needs to concentrate on enhancing Deep Neural Networks(DNNs)using more diverse and dynamic datasets that will help capture and respond appropriately to emerging phishing techniques.Through the supply of divergent and up-to-date data,DNNs can be made to learn new phishing methodologies that will not be evident in static datasets.Further,exploring hybrid models that combine the use of DNNs with other machine learning algorithms,such as Support Vector Machines or Random Forests,would be useful to enhance detection by leveraging strengths of more than one method.Exploration of real-time detection systems would also be necessary to enable timely detection and disruption of phishing attacks[14].The integration of these systems with existing security infrastructures can enable successful deployment and overall security posture.Secondly,the combination of user behavior analysis and contextual data within the detection process can enhance accuracy further by taking into account individual patterns and contexts.Model updating is necessary on a continuous basis to stay current with evolving phishing techniques.Infrequent updating with real-world attack and detection feedback will guarantee that the detection system remains timely and effective.Continuous adaptation maintains the effectiveness of phishing defenses against fresh and sophisticated threats[15].

VII.REFERENCES

[1] Parvesh,Indervati.Secure Credit or Debit Card Transaction Using Alert messages and OTP to prevent phishing attacks.in:2023 3rd International Conference on Innovative Practices in Technology and Management(ICIPTM).
[2] Phishlabs,“2019 Phishing Trends and Intelligence Report:The Growing Social Engineering Threat”https://www.phishlabs.com/
[3] P.Prakash,M.Kumar,R.Rao Kompella,and M.Gupta,“Phishnet:predictive blacklisting to setect phishing attacks,”in Proceedings of 29th IEEE Conference on Computer Communications(Infocom),pp.1–5,Citeseer,San Diego,CA,USA,March 2010.
[4] R.M.Mohammad,L.McCluskey,and F.Thabtah,“Intelligent rule based phishing websites classification,”IET Information Security,vol.8,no.3,pp.153–160,2014.
[5] S.C.Jeeva and E.B.Rajsingh,“Intelligent hishing URL detection using association rule minning”Human-centric Computing and Information Sciences(2016)6:10 DOI 10.1186/s13673-016-0064-3.
[6] R.M.Mohammad,F.Thabtah,and L.McCluskey,“Predicting phishing websites based on self-structuring neural network,”Neural Computing and Applications,vol.25,no.2,pp.443–458,Aug 2014.[Online].Available:https://doi.org/10.1007/s00521-013-1490-z.
[7] W.Wang,F.Zhang,X.Luo,S.Zhang:PDRCNN:Precise Phishing Detection with Recurrent Convolutional Neural Networks,Security and Coomunication Networks,https://doi.org/10.1155/2019/2595794 0.88 0.9 F1 Score 0.92 Figure 4:F1-score 0.94 0.96 0.98 Volume 2019.
[8] H.Yuan,X.Chen,Y.Li,Z.Yang,and W.Liu,‘Detecting Phishing Websites and Targets Based on URLs and Webpage Links’,in 2018 24th International Conference on Pattern Recognition(ICPR),2018,pp.3669–3674,doi:10.1109/ICPR.2018.8546262.
[9] UCI Machine Learning Repository,“Phishing Websites Dataset”[online]:https://archive.ics.uci.edu/ml/datasets/phishing+websites.
[10] Y.LeCun,Y.Bengio,and G.Hinton,Deep learning,Nature 521(2015),no.7553,436-444.

DOI:10.46647/ijetms.2025.v09si01.013 ISSN: 2581-4621

[11] N.Srivastava,G.Hinton,A.Krizhevsky,I.Stuskever,and R.Salakhutdinov.“Dropout:A simple way to prevent neural networks from overfitting”.The Journal of Machine Learning Research,15(1):1929-1958,2014.
[12] X.Glorot,A.Bordes,and Y.Bengio,‘‘Deep sparse rectifier neural networks,’’in Proc.14th Int.Conf.Artif.Intell.Statist.,2011,pp.315 323.0.9 0.92 Accuracy 2019,0.94[online]0.96 Avialable 0.98.
[13] R.M.Mohammad,F.Thabtah,L.McCluskey“Phishing Websites Features”(2015)[Online]availableat:http://eprints.hud.ac.uk/id/eprint/24330/6/MohammadPhishing14July201 5.pdf
[14] Bahnsen,D.D.Camacho,A.Villegas,C.A.Ledezma,and R.F.Casanova,“Classifying phishing URLs using recurrent neural networks,”2017 APWG Symposium on Electronic Crime Research(eCrime),Scottsdale,AZ,USA,2017,pp.1-8.
[15] M.T.I.Khan,S.S.S.R.Depuru,and P.Devendran,“Phishing website detection:A machine learning approach,”2020 International Conference on Artificial Intelligence and Signal Processing(AISP),Amaravati,India,2020,pp.1-5.