INTERNATIONAL RESEARCH JOURNAL OF HUMANITIES AND INTERDISCIPLINARY STUDIES
(Peer-reviewed, Refereed, Indexed & Open Access Journal)
DOI : 03.2021-11278686 ISSN : 2582-8568 IMPACT FACTOR : 6.865 (SJIF 2023)

Machine Learning to Detect Email Attacks: A Review

Annasaheb M. Chougule,[1] Dr. Kavita S. Oza,[2] Rohit B. Diwane[3]

[1]Research Student, Department of Computer Science,
Shivaji University, Kolhapur (Maharashtra, India)
E-mail: amc.rs.csd@unishivaji.ac.in
[2]Associate Professor and Head, Department of Computer Science,
Shivaji University, Kolhapur (Maharashtra, India)
E-mail: kso_csd@unishivaji.ac.in
[3]Research Student, Department of Computer Science,
Shivaji University, Kolhapur (Maharashtra, India)
E-mail: rbd.rs.csd@unishivaji.ac.in

DOI No. 03.2021-11278686 **DOI Link ::** https://doi-ds.org/doilink/06.2023-51186971/IRJHIS2306021

Abstract:

Email attacks have become a common issue in the digital age. With the increased transmission of sensitive information via email, it has become critical to create effective tools for detecting email attacks.Machine learning, an artificial intelligence subset, has proven to be a useful method for detecting email assaults. We will explore the creation and development of machine learning models to identify email assaults in this article. In this research paper wear ere viewed recent research papers with key points and research gaps in tabular format. The quantity of published research that were carefully and critically examined adds to the importance of detecting and preventing email assaults.

Keywords: *email attacks, machine learning, Artificial Intelligence, natural language processing, phishing, spam, smishing.*

1. Introduction:

Email security is a significant concern, and several researchers have explored machine learning approaches to address the challenges of detecting and preventing email attacks, especiallyphishingattacks.The purpose of this review paper is to provide a summary of studies that use machine learning approaches to detect email phishing attacks and their effectiveness in preventing email attacks.Email attacks have become a common issue in the digital age. With the increased transmission of sensitive information via email, it has become critical to create effective

tools for detecting email attacks.It has been proved that machine learning is subset of artificial intelligence which is a useful technique for identifying email threats. In this article, we will look at how to create and build machine learning models to detect email attacks.

Email attacks are broadly divided into two types: phishing attacks and spam emails. Phishing attacks pretend to be an honest company in order to collect sensitive data including login credentials, credit card numbers, and personal details. Spam emails, Unwanted emails, on the other hand, are those that advertise a product or service to a significant number of recipients. To conduct a thorough search across a number of databases, including IEEE, ACM, and Science Direct, the terms "email security," "machine learning," and "phishing" were used. The relevant articles were chosen from the search results and included in this review. The included articles were evaluated based on their goals, methods, and outcomes. Before identifying study gaps and potential future research objectives, a systematic literature review looks for prior studies that are pertinent to the subject. It also focuses on the advantages and applications of designing and developing a machine learning model to detect email attacks. During this research, we focused on areas where email and email attacks are common and detection is critical. More than 50 papers were examined. It has been observed that while technology for detecting email attacks or preventing spam or phishing attacks has many advantages, there is a lack of awareness; this is most common in IT organizations and individuals.

2. Literature Review:

Table 1: Literature review in tabular format

Sr. No.	Key Points / Review	Research Gaps
1	Using deep learning algorithms, this study suggests a method for detecting complex phishing. While a CNN is used to extract information from websites, an LSTM network is used to determine whether a web page is real or a phishing effort.The proposed scheme achieved ahigh detection accuracy of 98.7%.[1]	Future work will examine the proposed scheme's performance on a larger and more varied dataset, compare it to other state-of-the-art phishing detection schemes, and examine whether it can be applied to cyberattacks other than phishing. [1]
2	- Developed a machine learning modelling cycle to identify phishing attacks. - Developed a system that uses a dataset of URLs to train and test the machine learning model. When analyzing the performance of the recommended solution using multiple machine learning algorithms, high	- The proposed solution is evaluated using a single dataset, which may not be representative of all types of phishing attacks. The proposed solution is evaluated using a limited number of machine learning algorithms, and there may be other algorithms that can achieve better performance [2]

	accuracy was achieved.[2]	
3	- Developed an algorithm utilizing deep learning and machine learning to detect email phishing. - The system detected phishing emails with a 98.8% accuracy rate. [3]	-The proposed system needs to be evaluated on a larger and more diverse dataset to assess itsgeneralizability. -The proposed system needs to be evaluated against more sophisticated phishing attacks.[3]
4	- Machine learning techniques for phishing detection are compared. -Feature selection for improving accuracy. -Evaluation of various classifiers.[4]	The study did not cover advanced phishing techniques such as spear phishing and clone phishing. The performance of the techniques may vary with different datasets.[4]
5	- Email phishing attacks are easy to identify with the help of machine learning cognitive techniques and its architecture. The proposed solution uses ensembleclassifiers techniques to improve phishing email detection for more accuracy for result.[5]	- Need for further evaluation of proposed system on larger and more diversedatasets. Need for investigation of the impact of various features on the performance of the system.[5]
6	- Deep learning techniques are applied with the aid of convolutional neural networks, or CNNs, and long short-term memories, or LSTMs. - Proposed system uses hybrid CNN-LSTM architecture for better detection performance.[6]	- Need for further evaluation of proposed system on larger and more diversedatasets. The requirement for comparison with other cutting-edge phishing detection methods. [6]
7	- Detection of phishing emails and its machine learning based methods are mentioned. - used a variety of criteria for detection, including features based on the URL, domain, and content. [7]	- Need for evaluation of proposed system on larger and more diverse datasets. - The requirement for research into how various characteristics effect system performance.[7]
8	- Machine learning with natural language processing (NLP) methods are most usable as well as most effective methods for phishing detection. Used various features such as email header, sender information and message body for detection.[8]	- Need for evaluation of proposed system on larger and more diverse datasets. There is a need for comparison with other cutting-edge methods of phishing detection. [8]
9	- To identify email phishing assaults, deep learning and machine learning are utilised.	-Further improvement in the accuracy of detection models. -The impact of various email attributes

	-Analysis of various email features for detecting phishing attacks. -Performance evaluation of different machine learning and deep learning models.[9]	on the effectiveness of detection model performance is being investigated.[9]
10	- Machine learning methods and its importance to useful for prevention and detection of malicious emails. -Proposed system achieved high detection accuracy on experimental dataset. - It is very helpful to detection and identification of email phishing.	- The proposed system needs to be tested on a larger dataset to evaluate its effectiveness. The study focused on detecting phishing emails and did not address the prevention of suchattacks.[10]
11	- A review of different machine learning methods for spotting phishing websites -An analysis of the benefits and drawbacks of each strategy. [11]	-- The requirement for additional analysis and comparison of machine learning methods for website phishing detection - Need for the development of more accurate and robust algorithms.[11]
12	-Use of random forest technique for classification of phishing email. - The algorithm's performance is evaluated using various metrics. [12]	-Improvement of feature selection methods for better classification accuracy. -Incorporation of additional techniques for better phishing email detection.[12]
13	- suggested using URL analysis to detect phishing websites using machine learning. The proposed method is computationally efficient and can be used in phishing detection systems that operate in realtime.[13]	- No information provided on the dataset used for thestudy. There was no comparison with existing phishing detectionmethods.[13]
14	- Total 114 papers on deep learning and phishing detection based were reviewed by the author. - Identified the main techniques, datasets, and evaluation metrics used in thesestudies. Analyzed the performance of the reviewed studies and identified their strengths andlimitations.[14]	- Lack of standardization in datasets and evaluation metrics for phishing detection. Need for further research on interpretability and explain ability of deep learning-based phishing detectionmodels.[14]
15	- compared intelligent machine learning methodologies for detections ofPhishing. Analysis of models based on their	- Potential limitations of the comparison methods. Future research can focus on exploring newer and more advanced machine

	content andfeatures.[15]	learning techniques for phishingdetection.[15]
16	- Using the JavaScript PL function to create addons for the Google Chrome web browser that address phishing issues. - Blacklisting and semantic analysis are used to detect and prevent phishingattacks. Text, links, images, and other data are used to perform pattern recognition.[16]	The paper does not discuss the effectiveness of the recommended strategy in real-world situations.[16]
17	- Using random forest technology, we are developing a method for detecting phishing websites. -programmer serves as an add-on for web browsers, alerting users whenever phishing is found. -Examining phishing website characteristics to select the best set of features for classifier training. [17]	The paper does not discuss the potential limitations of using random forest technology in phishing detection or the effectiveness of the proposed system in real-world scenarios.[17]
18	In order to obtain critical information, attackers deceive visitors by making a masked website appear real or credible. Website phishing attack solutions come in a variety of shapes and sizes. [18]	No mention of the effectiveness of the proposed solutions.[18]
19	EMD is recommended as an extremely effective method for detecting phishing webpages. Extensive testing on 10,281 suspect web pages reveals high classification specificity, phishing recall, and relevance. [19]	No mention of the limitations of using EMD or alternative methods for phishing web page detection.[19]
20	Comprehensive feature on phishing and the 'Phish Bench' benchmarking framework presented. Retraining is useless against new attacks, and attackers must use unique features and strategies to trick detection systems. [20]	No mention of the specific new features and tactics needed or how to effectively prevent attackers from deceiving detection systems.[20]
21	The use of four classification methods to identify phishing assaults is covered in the study along with the development of anti-phishing measures. The study's results demonstrated a high degree of accuracy in identifying assaults using a	Some deep learning models that have proven to be useful can be used to the proposed model in future efforts.[21]

	dataset of phishing email websites. [21]	
22	This paper proposes a feature extraction strategy and semi-automatic phishing classifier (SAFEPC) to identify phishing attempts that avoid detection using current phishing email detection methods. [22]	Rank the features in order of importance and consider whether a subset of them can provide lower but acceptable precision and accuracy. [22]
23	The paper investigates the challenge of estimating remote state using a sensor with a restricted power budget. The paper looks at dynamic attack power allocation and how it may be turned into a Markov process to find the optimal solution in the context of denial-of-service (DoS) assaults. [23]	Only a few numerical simulations were presented to show how well our findings worked. [23]
24	- Traditional phishing attacks continue to cause data breaches. - Web-based phishing attacks deceive users by using deceptive websites. - Page resemblance is a key sign for identifying phishing websites because the appearance of the website is meant to trick consumers. - Phishing Alarm is a novel solution proposed to detect phishing attacks.[24]	-the need to explore further the detection techniques for phishing attacks that go beyond CSS-based features of web pages. -Future study could look into combining several detection techniques, such as machine learning, natural language processing, and behavioral analysis, to improve the accuracy and efficacy of phishing detection. -Additionally, there is a need to investigate the effectiveness of the proposed approach, Phishing-Alarm can detect spear phishing and whaling assaults, among other types of phishing attempts.[24]
25	- Phishing websites have emerged as a new cyber securitythreat. - Phishing websites can cause various security issues, such as spam, malware, ransomware, andmore. - Newly generated phishing websites are notdetected. - Machine learning methods can detect phishing websites. When multiple approaches were compared, the URL classification achieved an accuracy rate of 98%. - The naive classifier had a 1.5% accuracy.	-Firstly, the feature extraction approach used in this study is based on simple regular expressions, which may not capture all the important characteristics of phishing URLs. Therefore, future research can experiment with additional features that may lead to better accuracy. -Secondly, the dataset used in this study is a bit old, which may not represent the current trends of phishing attacks. Therefore, regular continuous training along with new datasets can improve the accuracy and performance of the

	- Recall performance was 0.95, and F1 Score was 0.97.[25]	system significantly.[25]
26	- Phishing websites are designed to steal sensitive information by disguising legitimate websites. -Blacklists, whitelists, and heuristic functions are used as anti-phishing strategies. -Methods based on visual similarity are suggested to lessen the likelihood of people falling victim to phishers.[26]	The paper focuses on phishing website identification using machine learning approaches, but it does not provide phishing assault mitigation or prevention. Future research can explore how to integrate the proposed approach with other security measures to provide a more comprehensive defense against phishing attacks.[26]
27	-Phishing is a widespread problem that costs consumers a lot of money each year. The following three techniques are used to resolve vulnerabilities: reading the URL's various functionalities, verifying the validity of the website by learning where it is hosted and who is in charge of it, and visual appearance-based analysis.[27]	-The effectiveness of the three proposed techniques is not compared to each other or to other techniques for detecting phishing websites.[27]
28	-Developed a machine learning-based ensemble to prevent deep phish. -The 100% accurate lexical function is the foundation of the Phish detection system. -tested the approach using 100,000 benchmark datasets for phishing and ordinary URLs. [28]	-further investigation could focus on comparing their ensemble approach with other existing approaches for preventing deep phish attacks to determine which method is more effective.[28]
29	- It was possible to identify "zero-day" phishing attempts using anomaly detection based on machine learning. -Phishing attacks were attempted by creating fake websites that imitate popular banks, social media, e-commerce, etc. -Focused on dynamic structures because of their vulnerability.[29]	They focused on dynamic structures in their anomaly detection approach, but it is unclear whether they considered other factors that could affect phishing attacks, such as user behavior or network traffic. Further research could explore these factors and their impact on phishing attacks.[29]
30	-Implemented a system to notify users by email and pop-up notifications when accessing a phishing site. -The system detects blacklisted URLs and can be used as an identification, authentication, and legalization tool.	It is unclear whether they evaluated the effectiveness of their system in preventing users from falling for phishing attacks. Further research could concentrate on assessing the efficacy of such systems

	-Phishing attacks are on the rise, and personal information is being obtained through fraudulent means.[30]	and identifying ways to improve them. [30]

According to the findings of the reviewed articles, machine learning algorithms are helpful in detecting email phishing attacks. To identify emails as phishing or non-phishing, the models proposed in the reviewed publications use a variety of factors such as email content, sender information, and URL links. Furthermore, the research papers evaluated the effectiveness of several machine learning approaches for email phishing detection, such as SVM, Random Forest, Naive Bayes, and Decision Trees.

Furthermore, the reviewed papers highlight the challenges of email security, such as the need for real-time processing and the high volume of emails to be processed. A promising strategy for solving these difficulties is to use hybrid models, which combine statistical and machine learning methods for email phishing detection.

However, there viewed papers also suggest that further research is needed to investigate the potential of using deep learning techniques and ensemble methods for email phishing detection. Additionally, exploring the impact of different feature engineering and preprocessing techniques on model performance could provide further insights into improving email phishing detection.

This review included thirty research articles. The articles proposed machine learning- based models for detecting email phishing attacks and evaluated the performance of these models based on accuracy, precision, and recall metrics. Some articles explored the impact of different feature extraction and selection techniques on model performance, Others looked into the prospect of employing deep learning and ensemble approaches to detect email phishing. The research papers also proposed hybrid models that combine machine learning and statistical methods for email phishing detection.

3. Conclusion:

In conclusion, Email attack detection has been demonstrated to benefit from the use of machine learning. The development of a machine learning model to detect email threats involve collecting a large dataset of emails, preprocessing the data, feature extraction, training the model, and evaluating its performance. With the increasing amount of sensitive information being shared through emails, the development of efficient techniques to detect email attacksis.

Crucial in ensuring the security of our digital world. The design and development of ML models to detect email attacks is an active research area, and several approaches have been proposed. These approaches include unsupervised and supervised ML algorithms, hybrid approaches, DL models, and clustering-based approaches. While each approach has its strengths and weaknesses, the results show that ML models have the potential to be effective in detecting email attacks and

improving email security. Further research is needed to explore the potential of using deep learning techniques and ensemble methods for email phishing detection and to investigate the impact of different feature engineering and preprocessing techniques on model performance.

4. References:

1. Moruf Akin Adebowale, Khin T. Lwin, M. A. Hossain , “Intelligent Phishing Detection Scheme Using Deep Learning Algorithms” in Journal of Enterprise Information Management 2021
2. Bryan Espinoza; Jéssica Simba; Walter Fuertes; Eduardo Benavides; Roberto Andrade, “Phishing Attack Detection: A Solution Based on the Typical Machine Learning Modeling Cycle” in IEEE 2019
3. Umer Ahmed Butt, Rashid Amin, Hamza Aldabbas, Senthilkumar Mohan, Bader Alouffi& Ali Ahmadian , “Cloud-based email phishing attack using machine and deep learning algorithm” in IEEE Access 2022
4. A. K. Jain and B. B. Gupta, “Comparative analysis of features based machine learning approaches for phishing detection” in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIA Com), New Delhi, India 2016
5. I. Ortiz Garcés, M. F. Cazares and R. O. Andrade, “Phishing Email Detection using Machine Learning: A Comparative Study” in 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA2019
6. M. A. Adebowale, K. T. Lwin and M. A. Hossain, “Deep Learning with Convolutional Neural Network and Long Short-Term Memory for Phishing Detection” in IEEE 2019
7. C. -Y. Wu, C. -C. Kuo and C. -S. Yang, “A Phishing Detection System based on Machine Learning” in IEEE 2019
8. T. Peng, I. Harris and Y. Sawa, “Detecting Phishing Attacks Using Natural Language Processing and Machine Learning” in IEEE 2018
9. Rathee, D., & Mann, S., “Detection of E-mail phishing attacks–using machine learning and deep learning” in International Journal of Computer Applications 2022
10. D. Oña, L. Zapata, W. Fuertes, G. Rodríguez, E. Benavides and T. Toulkeridis, "Phishing Attacks: Detecting and Preventing Infected E-mails Using Machine Learning Methods," 2019 3rd Cyber Security in Networking Conference (CS Net), Quito, Ecuador, 2019, pp. 161-163, doi:10.1109/CSNet47905.2019.9108961.
11. A. Odeh, I. Keshta and E. Abdelfattah, "Machine Learning Techniques for Detection of Website Phishing: A Review for Promises and Challenges," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), NV, USA, 2021, pp. 0813-0818, doi: 10.1109/CCWC51732.2021.9375997.

12. Akinyelu, A. A., & Adewumi, A. O. (2014). Classification of phishing email using random forest machine learning technique. Journal of Applied Mathematics, 2014.
13. M. Korkmaz, O. K. Sahingoz and B. Diri, "Detection of Phishing Websites by Using Machine Learning-Based URL Analysis," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-7, doi: 10.1109/ICCCNT49239.2020.9225561.
14. Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., & Shukla, S. (2022). Applications of deep learning for phishing detection: a systematic literature review. Knowledge and Information Systems, 64(6), 1457-1500.
15. N. Abdelhamid, F. Thabtah and H. Abdel-jaber, "Phishing detection: A recent intelligent machine learning comparison based on models content and features,"2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 2017, pp. 72-77, doi:10.1109/ISI.2017.8004877.
16. Abdul Razaque, Mohamed Ben Haj Frej, Dauren Sabyrov, Aidana Shaikhyn, Faith Amsaadand Ahmed Oun, "Detection of Phishing Websites using Machine Learning (Semantic Analysis Methods)" in IEEE2020
17. Amani Alswailem, Bashayr Alabdullah, Norah Alrumayh and Dr. Aram Alsedrani, "Detecting Phishing Websites using Machine Learning" in IEEE 2019.
18. Ammar Odeh, Ismail Keshta and Eman Abdelfattah, "Machine Learning Techniques for Detection of Website Phishing: A Review for Promises and Challenges" in IEEE 2021.
19. Anthony Y. Fu, Liu Wenyin and Xiaotie Deng, "Detecting Phishing Web Pages with Visual Similarity Assessment Basedon Earth Mover's Distance(EMD)"in IEEE Transactions on Dependable and Secure Computing 2006.
20. Ayman El Aassal, Sharyar Baki, Avisha Das and Rakesh M. Verma, "An In-Depth Benchmarking and Evaluation of Phishing Detection Research for Security Needs" in IEEE Access Special Section on Emerging Approaches to Cyber Security 2020.
21. Buket Geyik, Kubra Erensoy and Emre Kocyigit, "Detection of Phishing Websites from URLs by using Classification Techniques on WEKA" in Sixth International Conference on Inventive Computation Technologies 2021
22. Christopher N. Gutierrez, Taegyu Kim, Raffaele Della Corte, Jeffrey Avery, Dan Goldwasser, Marcello Cinque and Saurabh Bagchi, "Learning from the Ones that Got Away : Detecting New Forms of Phishing Attacks" in IEEE Transactions on Dependable and Secure Computing 2018.
23. Heng Zhang, Yifei Qi, Junfeng Wu, Lingkun Fu and Lidong He, "DoS Attack Energy Management Against Remote State Estimation" in IEEE Transactions on Control of

Network Systems 2016.

24. Jian Mao, Wenqian Tian, Pei Li, Tao Wei and Zhenkai Liang, "Phishing Alarm: Robust and Efficient Phishing Detection via Page Component Similarity" in IEEE Access 2017.
25. Jitendra Kumar, A. Santhanavijayan, B. Janet, Balaji RajendranandBindhumadhavaBS, "Phishing Website Classification and Detection using Machine Learning" in International Conference on Computer Communication and Informatics 2020.
26. M Somesha, Alwyn Roshan Pais, Routhu Srinivasa Rao and Vikram Singh Rathour, "Efficient Deep Learning Techniques for the Detection of Phishing Websites" in Indian Academy of Sciences 2020.
27. Malaika Rastogi, Anmol Chhetri, Divyanshu Kumar Singh, Gokul Rajan V, "Survey on Detection and Prevention of Phishing Websites using Machine Learning" in International Conference on Advance Computing and Innovative Technologies in Engineering 2021.
28. Maria Sameen, Kyunghyun Han and SeongOun Hwang, "PhishHaven – An Efficient Real-Time AI Phishing URLs Detection System" in IEEE Access 2020.
29. Mehmet Korkmaz, Ozgur Koray Sahingoz and Banu Diri, "Detection of Phishing Websites by using Machine Learning based URL Analysis" in ICCCNT 2020.
30. Mohammed Hazim Alkawaz, Stephanie Joanne Steven and Asif Iqbal Hajamydeen, "Detecting Phishing Website using Machine Learning (Agile Unified Process (AUP))" in IEEE International Colloquium on Signal Processing and its Applications 2020.