Grenze International Journal of Engineering and Technology, June Issue

Fortifying Email Security: A Machine Learning Approach

Shaik Salma Begum[1], Ananta Pavani[2], Gedela Narasimha Naidu[3], Gonela Sandeep[4] and Devu Pavan[5]
[1-5]Seshadri Rao Gudlavalleru Engineering College/CSE, Gudlavalleru, India
Email: shaiksalma.gec@gmail.com, {ananthapavani4, naidugedela565, sandeepgonela2003, pa1dev.edu}@gmail.com

***Abstract*— In today's communication landscape, emails are essential for both personal and business interactions, serving as a common method to transmit sensitive information, including financial data, credit reports, and login credentials .However, the time delay between sending and receiving emails provides an opportunity for cybercriminals to exploit vulnerabilities and compromise data integrity. Phishing, a frequently used malicious technique, involves impersonating reputable entities to acquire confidential information from unsuspecting individuals. To counter the growing phishing threat, this project focuses on utilizing machine learning (ML) algorithms.**

Through dataset segmentation, model training, and validation, this project demonstrates the effectiveness of our approach. Our systematic comparison of different datasets and features reveals that incorporating more features enhances accuracy and efficiency, strengthening our efforts to combat the widespread threat of phishing attacks

***Index Terms*— Introduction, Literature Review, Existing Configuration, Proposed Configuration, Experimental Results, Conclusion**

I. INTRODUCTION

Cybercrime pertains to offenses targeting computers or networks, covering a wide spectrum of potentially unlawful activities. The most frequently employed form of social engineering attack is phishing. Through these tactics, attackers aim to illicitly acquire private information from the target, intending to exploit it fraudulently. In today's digitally driven business landscape, an increasing number of companies are capitalizing on the continually advancing opportunities in cyberspace. This trend is particularly evident due to the pervasive influence of internet technology in our daily routines, compelling individuals to depend more heavily on the internet across all sectors. Phishing draws a direct analogy to fishing in water, except that, instead of seeking to catch fish, malicious actors endeavor to pilfer the victim's personal information. Phishing websites often mimic their legitimate counterparts closely to allure a significant number of internet users. Recent strides in phishing detection have prompted the development of numerous novel approaches centered on visual similarity. Machine learning and current artificial intelligence generation are used successfully in all regions of human lifestyles. Many researchers have used machine gaining knowledge of to improve safety. Computer threats may be divided into 3 sorts: bodily attacks, synthetic attacks and semantic assaults. In this kind of fraud, attackers take advantage of customers' vulnerabilities, mainly users translating computer messages. This is especially because maximum users have a tendency to agree with unverified information, making them liable to manipulation.

Grenze ID: 01.GIJET.10.2.160_1

Phishing is a major social engineering assault that is regularly used to scouse borrow consumer information to get entry to critical accounts, that could lead to robbery and monetary loss. This happens while an attacker impersonates a trusted supply and tricks the sufferer via diverse forms of verbal exchange. Sufferers are tricked into clicking on malicious hyperlinks that may lead to the installation of malware, gadget freezes in ransomware attacks, or statistics leaks.

Phishing perpetrators frequently attempt to deceive through phishing via electronic mail, which is the most efficient method for executing phishing attacks. Instant messaging, alternatively labelled as "phishing," has become widely favoured among social engineers for conducting phishing and reverse social engineering assaults. Telephone calls and Voice over IP (VoIP), commonly referred to as "vising," constitute alternative approaches employed by social engineers to procure sensitive data from victims. These strategies are formulated to guide individuals to counterfeit websites and deceive consumers into exposing their financial information, which includes usernames and passwords. as an example, phishing can be described as a fraudulent try to illegally gain personal information, typically through e mail. however, it is worth noting that phishing assaults can take many forms; for instance, social engineering messages can trick sufferers into installing malware at the browser. The ransomware can transfer funds to the victim's bank account whenever they access the financial institution without pilfering the sufferer's private information. therefore, it is clear that the Phish Tank subject matter will now not cowl all scams. Another definition says: "A phishing internet site is a internet site that impersonates an unauthorized third party in an effort to trick viewers into trusting that manor woman .it'smiles prison for the third birthday party to act. The definition is clearer because it recognizes that attackers are not constrained to stealing the sufferer's non-public information." however, it also prohibits phishing attacks on behalf of uncommon 1/3 events, such as community phishing attacks. Crafted messages maybe used to trap victims to web sites that seem to incorporate at ease content, causing the victim to put in the man-in-the-browser (MITB) malware.

Upon initiation of the workgroup, it has the capability to apprehend keystrokes with the purpose of purloining the victim's passwords. It's noteworthy to highlight that in this particular circumstance, the assailant refrains from assuming the identity of any external entities throughout the phishing operation. Alternatively, they dispatch messages with embedded links crafted to allure victims into accessing videos or multimedia content. To surmount the constraints of the earlier delineations, we categorize phishing attacks as semantic assaults. These utilize electronic communication channels to disseminate socially engineered messages, coercing the victim into undertaking actions advantageous to the assailant.

Email spams persist as persistent adversaries, cunningly navigating through digital landscapes. These virtual miscreants, armed with deceptive tactics, infiltrate inboxes with a singular mission – to compromise the sanctity of digital communication. Unwanted and often masked as benign messages, email spams relentlessly vie for attention, exploiting vulnerabilities in cyber defenses. As organizations fortify their cybersecurity arsenals, these stealthy invaders evolve, employing ever-shifting strategies to bypass filters. The battle against email spams is a dynamic one.Per reports on phishing attack trends from the APWG (Anti-Phishing Working Group), the volume of observed phishing attacks surged over 2020, escalating twofold throughout the year. Phishing attacks are disseminated via SMS, instant messaging, social networking, and email, with the latter remaining a prevalent vector for these assaults.

Financial losses can ensue from phishing emails, as attackers persistently employ this method to convince users they are interacting with a trustworthy entity, coaxing them into revealing personal credentials like credit card numbers, account login details, or identity information. In 2019, an astonishing 293.6 billion emails were daily sent and received, encompassing a substantial share of promotional emails from merchants. Although many view such content as spam, marketing emails are typically benign, albeit occasionally bothersome. Spam messages comprised 47.3 percent of email traffic in September 2020, resulting in considerable economic losses and societal issues. Spam email is essentially synonymous with email, and contemplating email without addressing the spam issue is challenging. Trojan horses, spyware, and ransomware are the most prevalent forms of malicious spam, and various methods, including awareness focus, blacklists, and machine learning (ML), have been developed to combat the spam dilemma. In recent years, deep learning (DL) has emerged as one of the most efficacious techniques within the machine learning domain.

II. LITERATURE REVIEW

In the ever-evolving digital landscape, phishing attacks have emerged as a formidable threat, endangering internet users, governments, and businesses alike. Exploiting human vulnerabilities through deceptive techniques like email, SMS, and voice phishing, these attacks pose risks ranging from identity theft to financial loss and

reputational damage. The escalating frequency of such incidents underscores the urgency for robust detection mechanisms.

Phishing attacks on emails pose a threat to individuals and organizations that need security solutions. Law-based and signature-based approaches often struggle to keep up with the ever-changing trends of phishing attackers. This literature review delves into the intersection of machine learning and security, with a particular focus on the use of neural networks (RNN) to improve email security. The flexibility and adaptability of RNNs holds promise for detecting subtle patterns in phishing attacks.

Conventional approaches, including rule-based and signature-based methods, are prevalent but exhibit limitations in adapting to emerging phishing tactics. Machine learning techniques, such as decision trees and ensemble methods, have gained prominence, with this review emphasizing RNNs. RNNs, designed to handle sequential data, are particularly well-suited for the dynamic nature of email content. Researchers have explored the use of Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) architectures within RNNs, showcasing their efficacy in identifying nuanced patterns associated with phishing attacks.

While RNNs show promise, challenges exist in their application to phishing detection. Imbalanced datasets, where legitimate emails significantly outnumber phishing emails, present a challenge in preventing biased models. Ensuring the generalization and transferability of RNN-based models across diverse email environments and languages is crucial. Overcoming these challenges is paramount for developing robust models that can effectively identify phishing attacks in real-world scenarios.

Future research directions include exploring hybrid models that combine RNNs with other machine learning techniques for enhanced adaptability. Additionally, efforts should be directed towards improving the interpretability of RNN-based models to foster trust and understanding of their decision-making processes. Despite challenges, the application of RNNs in phishing detection offers a promising avenue for creating dynamic and adaptive security solutions. The ongoing research should address existing limitations and focus on building robust, interpretable models to fortify email security against evolving phishing threats.

A fast filter for the large-scale detection of malicious web pages" by Canali et al. introduces Prophiler, a system devised to swiftly identify malicious web pages amidst the vast expanse of online content. Recognizing the pressing need for efficient web security, the paper outlines Prophiler's innovative approach, focusing on rapid detection techniques to filter out potentially harmful web pages. Its objective lies in bolstering cyber security measures and safeguarding users against prevalent cyber threats prevalent in the digital landscape [1].

Delves into the crucial task of identifying phishing websites. The authors propose a method based on analyzing the feature distribution of URLs, aiming to distinguish between legitimate and malicious websites. By scrutinizing specific characteristics within the structure of URLs, the paper explores how these features can be leveraged to create a robust detection mechanism for identifying potential phishing threats online [2].

This system proposes a scalable and adaptable reputation-based framework designed specifically to detect and mitigate the risks posed by phishing websites. By employing reputation scores derived from various sources or features, PHISHGUARD aims to provide a robust mechanism for recognizing and flagging potential phishing threats, enhancing online security measures [3].

The study explores how various ML techniques can be utilized to differentiate between legitimate and fraudulent websites. By leveraging features and patterns extracted from website data, the paper introduces and evaluates the effectiveness of ML-based approaches in the identification and classification of phishing websites, contributing to enhancing cybersecurity measures [4].

The study delves into the analysis of the inherent characteristics and structures within emails to differentiate between legitimate and phishing attempts. By exploring these structural attributes, the paper introduces a methodology aimed at effectively identifying and categorizing phishing emails, contributing to the advancement of email security measures [5].

In conclusion, this literature review illuminates the diverse strategies employed against phishing attacks. It emphasizes the dynamic nature of the battle, requiring continuous research and innovation to counter the evolving tactics of sophisticated phishers. The need for effective and adaptive detection mechanisms remains paramount in addressing this persistent and growing cyber threat [6-15].

III. Existing Configuration

Phishing attacks in emails continue to evolve as cybercriminals adapt their strategies to exploit human vulnerabilities. Spoofed sender addresses are a common element, with attackers adept at mimic king reputable entities to gain trust. The urgency created in these emails often compels recipients to acthastily, amplifying the

effectiveness of the attack. Moreover, embedded links play a crucial role, directing users to fraudulent websites that closely resemble legitimate platforms. This tactic relies on the assumption that individuals may not scrutinize URLs before clicking, making it essential for users to exercise caution.

Attachments in phishing emails pose a significant threat, as they can contain malware that compromises the security and privacy of the recipient's device. These attachments may be disguised as seemingly harmless files or documents, making it imperative for users to refrain from opening attachments from unverified sources. Grammatical errors and typos, though not fool proof indicators, can serve as warning signs. Legitimate organizations typically maintain a high standard of communication, and the presence of such mistakes can hint at the fraudulent nature of the email.

Mitigating the risk of falling victim to phishing attacks requires a multi-faceted approach. Education is crucial, as individuals need to stay informed about the evolving tactics employed by cybercriminals. Implementing security measures, such as enabling multi-factor authentication and using reputable antivirus and anti-malware software, adds layers of protection. Reporting suspicious emails to both email providers and the organizations they claim to represent contributes to collective efforts in combating phishing. Ultimately, a combination of vigilance, awareness, and technological safeguards is essential in safeguarding against the persistent threat of phishing attacks in emails.

Technics Used

A. Logistic Regression
B. Boosted Decision Tree
C. Support Vector Machine

A. Logistic Regression

Logistic regression is a statistical technique commonly used in binary functions. Its main purpose is to estimate the probability that a sample belongs to a particular class, making it a powerful tool in cases where the difference between two classes is significant. Contrary to its name, logistic regression focuses on distribution rather than regression, using the logistic function or sigmoid function to model the relationship between independent variables and the distribution of outcomes.

Commonly used in binary classification scenarios such as determining yes/no occurrence or splitting into true/false category-Logistic regression calculates the probability that a comparison boundary belongs to one of two groups based on input features.

Predictive power is based on a mathematical equation that has a weight (coefficient) assigned to each feature and the time involved. Model training involves optimizing these parameters, usually by methods such as max or min, to minimize the difference between predicted and actual class enrollments.

Logistic regression performance is often measured using metrics such as accuracy, precision, and recall, such as F1 scores or ROC curves. However, this method relies on some assumptions, including a linear relationship between independent variables and log variables, and many differences between democracies are uncorrelated.

The versatility of logistic regression can be used in many fields, from medicine (predicting disease) to finance (helping with credit scores) to business (high customer churn).While logistic regression provides simple, effective and interpretable results; it also has its limitations. His perception of the relationship between features and variables, his sensitivity to outliers, and his inability to disentangle interactions between variables can limit his actions. It was good in many distributions. But logistic regression is still an invaluable starting point for machine learning and statistical analysis, often as a way to improve search algorithms for many tasks such as sharing and distribution.

B. Boosted Decision Tree

Support decision trees represent a powerful collaborative learning method that combines the advantages of decision trees with support techniques to improve the accuracy of predictions. Unlike traditional decision trees, which can suffer from under- or over-fitting, boosted trees reproduce multiple decision trees sequentially, with each subsequent tree correcting the errors of its leaders.

In essence, decision trees support working by fitting a new tree to the remnants (errors or misclassifications) of the previous tree. These trees, often called weak learners or root learners, are generally shallow decision trees, meaning they have only a few nodes or levels. By focusing on the errors in the previous trees, the goal of each subsequent tree is to improve the prediction performance of the model, gradually reduce the bias and difference, and finally improve the truth.

A popular algorithm for boosting decision trees is gradient boosting, where the algorithm minimizes the loss function by adding new trees that predict the remainder of the previous prediction. Throughout this iterative process, the model evolves to make more accurate predictions while reducing overall error.
Boosted makes good decisions in many areas such as finance, healthcare and e-commerce, among others. Their ability to control the relationship between features and outcomes and their robustness against overfitting make them popular in predictive modeling. They can also handle different types of data, including numbers and attributes, and capture the relationship between variables.
However, the advantages of augmented decision trees come with more challenging work and higher risks if not maintained properly. Optimizing parameters such as learning rate, tree depth, and number of boosting iterations is important to prevent overfitting and ensure model performance.
Overall, leveraging decision trees is a powerful integration technique that leverages the advantages of a decision tree while minimizing its disadvantages. By iteratively improving predictions and focusing on error correction, they provide a strong foundation for accurate and flexible predictive modeling in diverse and complex data.

C. Support Vector Machine

Support vector machine (SVM) is a powerful learning algorithm frequently used for task classification. SVMs are unique in their ability to handle distribution and heterogeneity by finding the optimal hyperplane that best separates classes in a given domain. The goal is to maximize the distance between the global plane and the closest data for each class, making SVM powerful and efficient in many cases.
The principle behind SVM is to map input data into high dimensional space; here it is easier to find hyperplanes that clearly separate different groups. If the original data is not linearly separated, SVM can effectively create nonlinear decision boundaries by transforming it into a high dimensional one using so-called kernel input.
SVM has the ability to maximize margins while reducing classification error. SVM selects a hyperplane that not only separates classes but also preserves the maximum distance from the data closest to each class. This concept, known as the maximum marginal hyperplane, improves the power of the model and its ability to generalize to unobserved data.
Due to its features, SVM is widely used in many fields such as image classification, text classification, bioinformatics and finance, versatility and ability to handle high data. In addition, their ability to manage large areas and high performance (especially in cases where data is limited) make them the choice of many applications.
Beyond their acclaimed features like versatility and adept handling of extensive datasets, SVMs shine as beacons in realms as varied as anomaly detection in cybersecurity and predicting stock market trends. Their robust nature extends to ecological studies, aiding in the classification of species based on complex biological data, further solidifying SVMs as indispensable tools across scientific and technological landscapes.
However, SVM also has some limitations. They can have many features, especially when working with large files. In addition, their performance often depends on the choice of the kernel function and the tuning of hyperparameters, which affects the accuracy and performance of the model. Overall, support vector machines are powerful and versatile tools in machine learning; It provides ood solutions to divide tasks and find the best decision at the top to achieve the best results, thus intelligently understanding the importance of skills. in various applications.

IV. PROPOSED CONFIGURATION

Recurrent Neural Networks (RNNs) offer several distinct advantages over traditional machine learning models like Logistic Regression, Boosted Decision Trees, and Support Vector Machines (SVMs), especially in handling sequential or time-series data. One key advantage lies in RNNs' ability to capture temporal dependencies and sequential patterns within data. Unlike Logistic Regression, which assumes independence between input features, RNNs can retain information from previous time steps, making them adept at tasks like time series forecasting, natural language processing, and speech recognition.
Moreover, RNNs excel in handling variable-length sequences, which can be challenging for models like Boosted Decision Trees and SVMs that typically require fixed-length input vectors. This flexibility enables RNNs to process and generate sequences of different lengths, making them suitable for tasks involving text of varying lengths, audio data, or even stock market predictions where sequence lengths may vary.
Another advantage of RNNs is their ability to handle long term dependencies, which can be challenging for traditional models. While models like Boosted Decision Trees or SVMs might struggle to capture relationships between distant events in a sequence, RNNs with specialized architectures like Long Short-Term Memory (LSTM)

or Gated Recurrent Unit (GRU) can better preserve information over longer time spans, mitigating the vanishing or exploding gradient problems typically encountered in deep networks.
Furthermore, RNNs possess the capacity to learn complex non-linear relationships in data, which might be difficult to capture using linear models like Logistic Regression or SVMs. This characteristic makes RNNs more suitable for tasks involving intricate patterns or contexts, such as sentiment analysis in text or understanding the context in dialogue systems.
However, RNNs also come with their own set of challenges. Training RNNs can be computationally intensive and suffer from issues such as missing or distorted gradients, which can hinder learning over long distances.
Additionally, tuning the RNN architecture and hyperparameters requires expertise and can be more disruptive than simple models such as logistic regression or SVM, especially when displaying training data is prohibited.
In summary, RNNs have great advantages in storing sequential data, processing variable-length processes, and learning complex patterns, making them better suited to tasks involving time or relational data, as well as logistic regression, decision support, etc. It has advantages. This is good, as traditional models such as trees or support vector machines can be difficult to perform tasks.

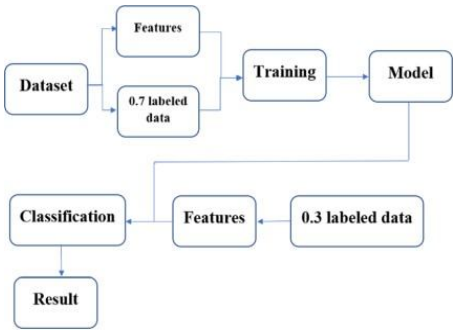

Figure 1. Proposed Model flow chart

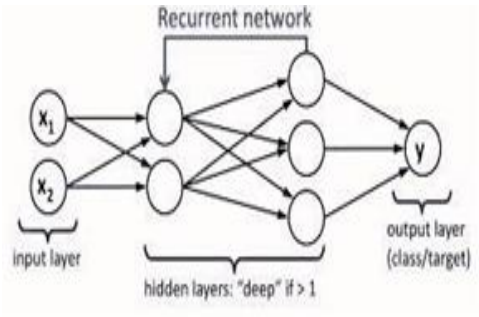

Figure 2. Proposed Model

A Recurrent Neural Network (RNN) represents a specialized neural network uniquely tailored to handle sequential data. What distinguishes RNNs is their inherent ability to retain information from prior states, enabling them to comprehend and operate on continuous processes. This memory attribute empowers RNNs to thrive in tasks revolving around contextual understanding, such as natural language processing and real-time analysis. Unlike traditional neural networks, RNNs are structured to facilitate the persistence and transfer of information from one step to the next, making them particularly suited for processing variable-length content, such as articles or dynamic documents.
However, many RNN models encounter challenges when it comes to long-term learning, often facing issues like the degradation of information over time, especially in early stages of online learning. To address this, various advancements in RNN architectures have emerged, including Long Short-Term Memory networks (LSTMs)and Gated Recurrent Units (GRUs).These evolved architectures integrate specific mechanisms to enhanced at a retention over extended periods. Notably, LSTM implementations utilize gating mechanisms to regulate data flow, significantly alleviating issues related to information loss during learning processes.
RNNs find widespread utility across diverse domains, particularly in language processing tasks like language modeling, sentiment analysis, and machine translation. Their applications extend to speech recognition, time-series forecasting, and robotics. Despite their potency, RNNs with certain limitations, such as computational demands during training and struggles in retaining long-term dependencies. Their effectiveness relies heavily on thoughtful selection of structure, organization, and a comprehensive understanding of underlying principles.

V. Experimental Results

The data set here consists of 2 features and it consist of 5573 instances, 87% of the tags are ham (not spam) and 13% are spam i.e., 724 phishing and 4848 legitimate instances. The size of the file is 213 KB and we allocated it 80% for the training process and 20% for the testing process. Most of the data is hams for disparity in class, we validated this using an 80-20 split for training and testing. High accuracy indicates pattern. Good performance distinguishing amateur emails from non-document spam.
The selected ML algorithm and the existing algorithms are employed on the processed dataset. The results are represented in the following table:

TABLE I: COMPARISON OF VARIOUS ALGORITHMS

Algorithm	Accuracy	Precision	Recall	F1-score
Recurrent Neural Network	0.98	0.96	0.87	0.92
Support Vector Machine	0.96	0.85	0.97	0.90
Logistic Regression	0.95	0.86	0.91	0.88
Boosted Decision tree	0.95	0.86	0.91	0.88

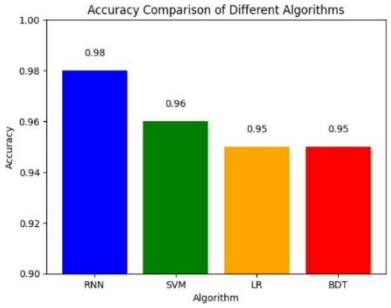

Figure 3: Accuracy Comparison

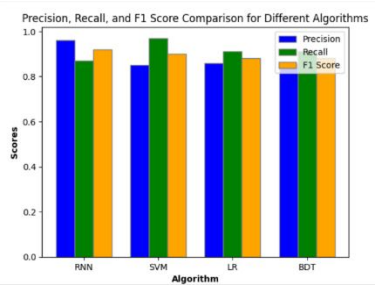

Fig 4: Precision , Recall and F1-Score

VI. CONCLUSION

The study delved into the realm of phishing email detection leveraging Recurrent Neural Networks (RNNs). The utilization of RNNs in identifying phishing emails showcased promising outcomes, emphasizing their efficacy in capturing inherent textual characteristics and other pertinent features within email content.

Through the evaluation across three supervised datasets, this research highlighted the performance of various RNN-based classifiers. The comparison among these classifiers delineated distinctive accuracy levels. Notably, the use of a multi-feature RNN model, incorporating 50 features, yielded the highest accuracy. Conversely, employing a reduced feature set of 20 exhibited a reasonably high accuracy rate but was deemed insufficient for robust phishing email detection.

However, despite the improvements achieved with RNN- based models, a significant limitation surfaced during this study—the challenge of acquiring predefined datasets specifically tailored for phishing email detection in the research domain. This limitation posed obstacles to further refining the accuracy and efficacy of RNN models for phishing email detection."

REFERENCES

Absolutely, here's a list of 15 references on phishing detection in emails:

[1] Canali, Claudia, et al. "Prophiler: A fast filter for the large-scale detection of malicious web pages." Proceedings of the 20th international conference on World wide web. 2011.

[2] Zhang, Zhiwei, and Sencun Zhu. "Detecting phishing websites by analyzing the feature distribution of URLs." Proceedings of the 2013 IEEE International Conference on Communications (ICC). IEEE, 2013.

[3] Ramachandran,Varun,etal."PHISHGUARD: A scalable and adaptive reputation system to detectphishingwebsites."2011IEEE/IPSJ International Symposiumon Applications and the Internet. IEEE, 2011.

[4] Das, Shubhadip, et al. "Phishing website detection using ML algorithms." 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT). IEEE, 2018.

[5] Wang, Tao, et al. "Phishing email detection based on structural properties." IEEE Transactions on Information Forensics and Security 11.9 (2016): 2071-2084.

[6] Almomani, Omar, et al. "Machine learning approach for phishing detection based on URL features." 2018 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2018.

[7] Verma, Deepika, and Mohit Sewak. "Phishing DetectionUsingMachineLearningTechniques." ProcediaComputerScience132(2018):1139-1146.

[8] Dhilip, S., and N. K. Sakthivel. "Phishing Email Detection using Ensemble of Machine Learning Classifiers." 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2020.

[9] Ghorbani,Amineh,etal."A survey of machine learning algorithms for phishing detection."ACM Computing Surveys (CSUR) 53.6 (2020): 1-38.

[10] Alzahrani, Saleh, et al. "An evaluation of machine learning techniques for detecting phishing websites." 2017 2nd International Conference on Knowledge Engineering and Applications (ICKEA). IEEE, 2017.
[11] Hussain,Rasool, and Mohd Fadzli Marhusin. "Phishing Detection Techniques: A Comprehensive Review." 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). IEEE, 2018.
[12] Shaik Salma Begum & Dr. D. Rajya Lakshmi, "GLCM of Fuzzy Clustering Means for Textural Future Extraction of Brain Tumor in Probabilistic Neural Networks," International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, Volume-9, Issue-1, and November 2019.
[13] Shaik Salma Begum & Dr. D. Rajya Lakshmi, " Combining optimal wavelet statistical texture and Recurrent Neural Network for Tumor detection and Classification over MRI," Multimedia Tools and Applications, ISSN 1380-7501, January 2020, Springer.
[14] Shaik Salma Begum et al. "Protecting Girls from Harassment and Fraudulent Calls: A Voice-to-Text Approach", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, Volume: 11, Issue:8, July 2023, DOI: https://doi.org/10.17762/ijritcc.v11i8s.7250.
[15] Shaik Salma Begum et al. "RDNN for Classification and Prediction of Rock or Mine in Underwater Acoustics", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, Volume: 11,Issue: 3,March 2023, DOI: https://doi.org/10.17762/ijritcc.v11i3.6326.