Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 5): pp. 5970-5977
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.05.671

ENHANCED RECURRENT CONVOLUTIONAL NEURAL NETWORKS BASED EMAIL PHISHING DETECTION

SADULA SAIPRASANNA, MTech student, Dept. of CSE, Anurag Group of Institutions, Ghatkesar(M), Ranga Reddy(Dist) Hyderabad. TS,saiprasannasadula@gmail.com
N. SWAPNA GOUD, Assistant Professor, Dept. of CSE, Anurag Group of Institutions, Ghatkesar(M), Ranga Reddy (Dist) Hyderabad. TS,swapnagoudcse@cvsr.ac.in
Dr.G.VISHNU MURTHY, Professor, Dept. of CSE, Anurag Group of Institutions, Ghatkesar(M), Ranga Reddy(Dist) Hyderabad. TS,hodcse@cvsr.ac.in

Abstract: Email communication has now become a necessary conversation medium in our daily life. Particularly for the finance sector, communication by email represents a primary role in their businesses. So, it is necessary to classify emails based on their performance. Email phishing is one of the most serious Internet phenomena that make various difficulties to business class essentially to the finance sector. Furthermore, phishing emails are increasing at a dangerous rate in recent days. Hence, more environmentally friendly technology for phishing detection is required to manage the risk of phishing emails. This paper proposes an intelligent system for identifying phishing emails using enhanced recurrent convolutional neural networks (ERCNN). The system performs as new ability to have a web browser as an extension that notifies the user mechanically during detection of phishing emails. The whole system is based on a deep learning approach, in particular supervisory mastery. We chose the Convolutional Neural Network (CNN) due to its excellent overall performance in this category. Our conscience is looking for a higher overall performance classifier by analyzing phishing emails' potential and selecting aenhancedmixture of them to train the classifier. The results shows that proposed work get98.8% accuracy and a total of 26 features.

Keywords:, **phishing email detection, classification, recurrent convolutional neural networks, convolutional neural networks (CNN).**

I. INTRODUCTION

With the fast improvement of the internet in the currentyears, few of attackers launched phishing sites on the Internet to mimic the real enterprise sites for ordinary customers to reveal particular statistics, for example, due bank money, postal bills, and passwords. The type of phishing attacks now is prevalent and is overgrowing. In a report released these days using the Anti-Phishing Task Force (APWG) [1], it is reported that APWG members discovered more than 250,000 phishing attacks using 195,475 exceptional ranges from 2015 to 2016. These both numbers are the best file given the fact that APWG started reporting about phishing events in 2007.
Detecting phishing has garnered a variety of investigations in recent years. In particular, current phishing detection methods fall into three unique categories: technologies that rely entirely on blacklists and whitespace, processes that rely primarily on visual similarities to web pages, and technologies that depend entirely on website and URL content. The long-term list, mostly black and white, comes close to clashing if a particular URL represents phishing compared to a list of recognized phishing sites identified during the 1/3 birthday party. These techniques are commonly used in industrial engineering to intercept URLs [2, 3] in a specific file. The compromise of this generation is, on the one hand, that it mainly relies on detection results provided by using 0 .33 times, in conjunction with Google's Safe Browsing API, which has a significant effect and cannot protect against phishing attacks. For 0 days. Miles indexed on the whitelist is illegally classified as suspicious, which is arbitrary for high-security sites.

Recently, there have been several investigations attempting to deal with the issue of phishing. Some researchers used the URL. Compared to the victorious blacklists of malicious website listings they developed, others used the URL in the opposite direction, primarily evaluating the URL against the website's legitimate whitelist. Websites use the latest in heuristics technology, which uses a signature database for any diagnosed attack that forms a focused signature form to determine if you are miles away from a phishing website. Also, to appreciate website visitors, Alexa is any other era that researchers use to discover phishing sites[4].

Also, many researchers have used subject system strategies. Machine skill is one of the branches of creating computers, and it is also the department of artificial intelligence (AI) that plays functions and may reasonably be seen or shown. It has specific types of expertise: supervised know-how and unsupervised knowledge. The know-how that is monitored for its acquisition becomes based on problem education. It gives fast and challenging operation of target tag data related to this data. Once the version is highlighted, you can create a new goal tag with more data. On the other hand, completely unsupervised stats have become changes that depend entirely on new knowledge production without intention sign in the training paradigm.

II. LITERATURE SURVEY

Phishing is one of the significant security issues in the registry. It can appear in the methods, either through receiving suspicious e-mail messages leading to a fraudulent website or through a person's access to hyperlinks that are crossed simultaneously as a phishing website. However, both strategies are considered benchmarks for an element; Meaning, the attacker points to human weaknesses rather than shortcomings of this system. Phishing can be described as a scam that aims to control people by providing non-public information, along with a section on customer contact, passwords, and credit cards. These scams create Forex crises for clients.

Recently, several studies have been conducted to address phishing. It can be categorized into four categories: blacklists, heuristics, classification of content materials, and devices that obtain technical records. The URL Blacklist compares the current database that includes the list of phishing URLs. With the rapid rise of phishing sites, the blacklist has proven to be of no use in determining whether every URL is a phishing webpage on the Internet. This kind of procrastination can lead to one-day attacks from phishing sites.

(Nguyenet al.2018) The main aim of is to find phishing content/documents in aA collection of text records. It is an internet protection nuisance that can help protect customers from fraudulent information. Natural Language Processing (NLP) gives a natural technology to this defect as it can read smart, popular text content. They were evaluated new NLP text classification techniques to deal with the hassle of preventing phishing in emails (that is, predicting whether or not the email is phishing). Those technologies mainly rely on a wide range of services that have made network attention these days. Specifically, it provided a framework with Hierarchical Long Short Term Memory (H-LSTM) and attention mechanisms for emails that simultaneously send phrase levels and sentences. They counted on providing a useful anti-phishing model and demonstrated the effectiveness of deep domain cyber protection issues.

Zhang et al.(2017) With the rapid improvement of the Internet, phishing and other scams are increasing dangerously. Criminals pretend to be banks, powerful suppliers, and social media sites to send fraudulent data to make users log in and steal consumer records. So, a large number of customers and financial institutions suffer from losses and economic assets. How to accurately and successfully detect the dangers of phishing on the Internet was a big problem on the Internet. The authors were examined the history of phishing prevention and detection development introduced artificial minority technology of DBN (Deep Belief Network) to detect phishing. The generation uses a deep phishing detection method that is completely based on network log content materials and other capabilities to improve recognition accuracy by 1%. In addition, the Borderline-Smote Report is used to address the unbalanced facts issue in teaching phishing detection, supplementing with an F-fee with the help of 2% and considering the value.

Abadiet al.(2016) TensorFlow is a system of study of devices that works widely and in heterogeneous environments. TensorFlow uses data flow charts to symbolize computing, common country, and operations that change this country. It maps nodes to flow data across multiple devices in a group, and within a system in various computing devices, including multi-core CPUs, the preferred cause of GPUs, and specially designed ASICs called Tensor Processing Units (TPU). This structure gives developer flexibility: While in previous "parameter server" designs, shared nation control is integrated into the device, TensorFlow allows developers to test using new improvements and educational algorithms. TensorFlow supports packet broadcasting, focusing on education and inference in deep neural networks. TensorFlow is used in manufacturing by various Google offerings; we have launched it as an open-source task and have been widely used in machine learning studies. In this document, we describe TensorFlow's data flow model and reveal the compelling overall performance that TensorFlow accomplishes for many real-world programs.

Nguyen et al.(2015) So far, relationship extraction systems have widely used the capabilities generated by language assessment units. Errors in these properties lead to relationship and row detection errors. In this paper, we build on those traditional procedures with engineering complex functions by introducing a convolutional neural network to extract relationships that routinely learn the properties of sentences and reduce dependence on external tools and resources. Our model receives more than one window for filters and vaccinations for pre-flagged phrases as a principle in an unstable structure to improve overall performance. We highlight the relationship of problem extraction with an unbalanced group. Experimental effects show that our machine significantly outperforms the best reference retrieval system for relationships, but also the latest relationship category system.

Stollenga et al.(2014) Convolutional neural networks (CNN) are fixed and fed in the future. They do not change their criteria at any stage of the evaluation and do not use the best comments to reduce the layers. Real brains, however, do. The same is true for the selective deep care network (dasNet) architecture. The structure of DasNet comments can dynamically change the sensitivity of the bypass filter across a category. It takes advantage of chain processing power to improve species performance by allowing society to recognize its internal interest frequently in some bypass filters. By looking for direct coverage in a vast milestone area of one million dimensions, experts receive SNES feedback. In the CIFAR-10 and CIFAR-100 data sets, dasNet outperforms the previous modern model in unprocessed data sets.

Verma et al.(2013) In a phishing attack, a suspicious patient, usually by email, is attracted to a website designed to steal sensitive information along with account numbers from financial institutions/credit cards, credit card information, debit login, and so on. Every 12 months, internet customers lose billions of dollars because of this scourge. They have presented a method for choosing a standard indicator attribute for text problems that relies entirely on statistical analysis and WordNet and demonstrates its effectiveness in detecting fraudulent email by designing classifiers containing semantics and facts when studied. Their feature selection technology was not unusual and useful for various analytics packages that mainly rely on textual content. The primary email text classifier achieves over 95% accuracy in detecting phishing emails with a hyperbolic rate of 2.24%. Because they use semantics, their feature selection method was robust against adaptive attacks and avoided joint retraining required to stop the classifier.

Shashidharet al.(2012) Phishing affectsbillions of dollars every year and is a significant threat to the Internet's economic system. Email is still the most used method for phishing attacks. This article introduces a complete and all-natural attacking phishing email format about the use of competencies, which can be static and mean phishing. Their diagram used all email records, specifically the header, hyperlinks, and textual content in the body text. Although that was abundantly clear that phishing emails were designed to spark victim movement, none of today's modern detection systems uses this fact to identify phishing emails. Their detection protocol generally aims to distinguish between "executable" and "informational" email messages. To do so, it used herbal language strategies to detect phishing. They also used contextual data when identifying a phishing website: They tested phishing detection harassment within the contextual hurdles of a person's email domain and showed that context plays a vital role in detection. Understandably, a key information image that uses natural language strategies and contextual facts to locate a phishing site. They explained that the scheme goes beyond existing phishing detection schemes. Finally, the protocol detected phishing at the email level instead of trying to find disguised websites. It was necessary to prevent the victim from clicking on malicious links in the email. Known as PhishNet-NLP, this app works between a User's Mail Transfer Agent (MTA) and Personal Mail Agent (MUA) and handles every phishing email before it reaches your inbox.

Hamid et al.(2011) Phishing emails are more active than ever before and makes the average user of laptops and companies vulnerable to a great deal of information, brands, and financial loss. This document focused on the attacker's necessary behavior that can be extracted from the email address by analyzing the accumulated amount of phishing and emails. Additionally, it recommends using a mixed job selection approach that relies primarily on a combination of content and behavior. The technology must completely undermine the attacker's behavior based on the email header. In a body overview, our `Hybrid feature selection can bring in an accurate price of 96%. Moreover, we passed the high-quality check of our proposed behavior-based job using the records feature.

Table.1 Comparison between various techniques in phishing email detection

Author	Technique used	Advantages	Disadvantages
Nguyen et al.[2018]	Hierarchical Long Short-Term Memory (H-LSTM)	Proposed anti-phishing technique can detect phishing web pages efficiently, and it is better than the baseline model.	These systems can be avoided by deceptive web pages that do not contain legitimate hyperlinks.
Zhang et al.[2017**]**	Deep Belief Network (DBN)	Improve recognition accuracy	Existing methods are only used to prevent customers from accessing recognized phishing sites and not discovering new phishing sites.
Abadiet al. [2016]	TensorFlow	This structure gives developer flexibility, TensorFlow supports packet broadcasting	Phishers can evade their method by altering the position and layout of the visual elements
Nguyen et al.[2015]	Convolutional neural network(CNN)	It significantly outperforms the best reference retrieval system for relationships, High level of accuracy	It Consuming memory, Huge number of features
Verma et al.(2013)	WordNet Text classifier	It achieved over 95% accuracy in detecting phishing emails at a fake high price of 2.24%.	Attackers may be able to design their attacks to avoid heuristic detection.
Shashidhar et al.[2012]	PhishNet-NLP	Threat detection through active scanning of URLs is good. It avoids the false positives.	Time consuming,
Hamid et al.(2011)	Hybrid feature selection (HFS)	Must completely undermine the attacker's behavior based on the email header	These techniques are difficult and usually computationally expensive

III. PROPOSED METHDOLOGY

Emails are categorized into two parts in this paper are phishing emails and valid emails. Recognizing phishing emails is a paired problem. We estimate the issue and split the email into tools, header and text. We represent a binary variable y to indicate email attributes. That is, method $y\ D\ 1$ for this email is phishing and $y\ D\ 0$for that email are legitimate.

In various terms, y is email etiquette. Look at the drawer below to determine whether or not an email is phishing. To provoke this, we calculated the possibility that the email would convert a phishing email, i.e., $P(y\ D\ 1)$.The opportunity chance is then compared to the minimum semester. If it can be more than the qualification threshold, it is considered a phishing email. Our object is to determine if the victim's email is valid or the phishing is fast and accurate. In this component, we will present features of our proposed version

Also, we recommend a modern generation of phishing email detection, ERCNN (Enhanced Recurrent Convolutional Neural Networks), which better utilizes URLs for phishing detection and does not now require delivery of a third party other than the search engine or DNS. The ERCNN mines architectural and denotative abilities within phishing emails and URLs through a deep domain model to stumble upon email phishing. Our approach does not consider external databases and is very fast with a detection time of less than 0.4ms in URL parsing. In our opinion, ERCNN is a crucial thing to discover the highest and most accurate phishing with URL popularity. Our significant contributions are summarized below:

1. We first proposed a deep learning model based phishing detection which can quickly and correctly locate phishing sites, without counting 1/3 results of search engine.
2. We incorporate the uses of RNN and CNN in handling textual content information. Initially, we used the deep learning based RNN to mining global capabilities from the URL, and then we applied classifier as a CNN to mining local features.
3. We've designed 4 basic models, and experimental effects mean that PDRCNN can discover more URLs from phishing sites on the Internet than there are devices that gain knowledge of the entire method-based methods and the known n-gram methods.

The proposed classification algorithm has shown below,

SYSTEM ARCHITECTURE

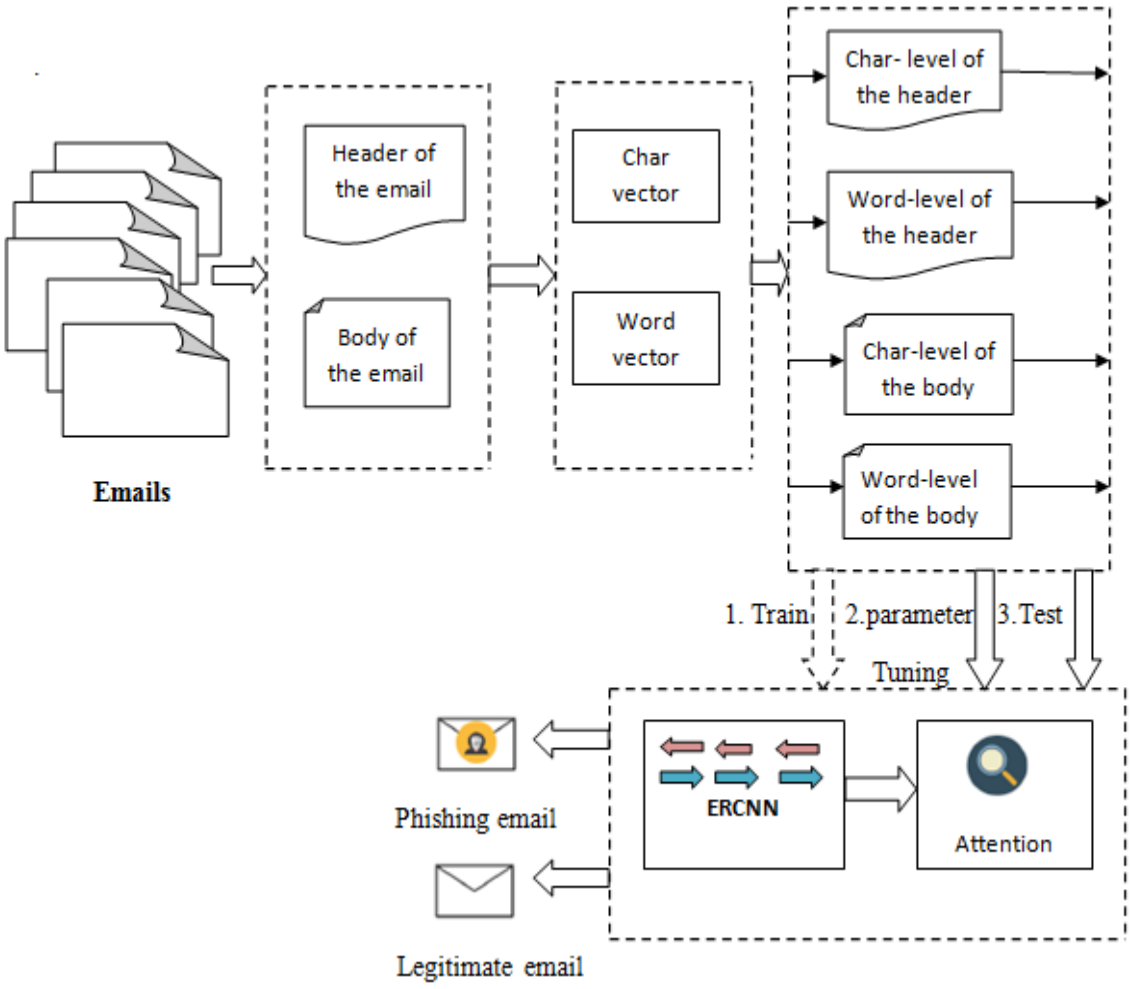


Fig.1 Framework for classifying phishing or legitimate emails

Figure 1 illustrates our model; as shown in the figure, emails are categorized into two ways phishing emails and valid emails. First of all, since email content material can be so unnatural, we want the technology to refresh the email recordset and remove more digital nonsense and immersive textual content. Email is divided into several domains: document grade and word diploma for the email header and document stage and word level in the email body. Then The Word2Vec technique is applied to define

and manage vector sequences. Then we separate the records into two segments, one as a group to check out the school and the opportunity as a test set. We are inserting part of the test kit into our form and show you how to obtain the classifier. The next level of the heuristic the set of validation is employed to perform an excellent parameter selection analysis on the classifier to get the minimal threshold. Lastly, the test set is utilized to verify the form of the classifier that decides to test the properties.

$$\boldsymbol{Algorithm}: Enhanced\ Recurrent\ Convolutional\ neural\ network$$
$$\boldsymbol{Input}: Training\ Dataset\ D = \{(x_1, y_1), (x_2, y_2), \ldots . (x_n, y_n)\}$$
$$//x_n\ is\ the\ feature\ vectors, y_n\ \ is\ the\ output(phishing\ \ or\ legitimate)$$
$$\boldsymbol{Output}: Trained\ neural\ network$$
$$initialize\ all\ weights\ and\ biases\ in\ network;$$
$$while(termination\ condition\ is\ not\ satisfied)$$
$$\{$$
$$for\ (each\ training\ parameter\ X\ in\ D)$$
$$\{$$
$$for(each\ input\ layer\ node\ j)$$
$$\{$$
$$O_j = I_j //output\ of\ an\ input\ layer$$
$$for(each\ hidden\ or\ output\ layer\ node\ j)$$
$$H_j = \frac{1}{1 + e^{-j}};$$
$$O_j = f(\sum_{i=1}^{n} w_{ij}\, x_i + b_j)$$
$$for\ (each\ node\ j\ in\ output\ layer)$$
$$E_j = \frac{1}{2}(t_j^p - o_j^p)^2$$
$$//\ t_j^p is\ the\ desired\ target\ output\ for\ the\ p-th\ observation$$
$$and\ o_j^p\ \ is\ the\ actual\ output\ for\ the\ p-th\ observation$$
$$Update\ the\ weight\ and\ bias\ value\ based\ on\ the\ E_j\ \ (error\ value)$$
$$\}$$
$$\}$$
$$\}$$
$$if\ O_j < 0.5$$
$$\{$$
$$return\ -1//it\ is\ corresponding\ to\ legitiate\ URL$$
$$else$$
$$return\ 1//it\ is\ corresponding\ to\ phishing\ URL$$
$$\}$$

The algorithm above explains how to recognize phishing URLs within websites. Initially, CNN is loaded with obtained feature vectors, and then compares to the output pattern as the first layer. Then, in every consideration series, the result will use the matrix multiplication to multiply the weight matrix, which will then load the bias*b*.

IV. RESULTS AND DISCUSSIONS

We will go into the batch of checks on the form that we have previously collected and given a group of signs, these scores are applied to investigate the overall model performance accurately.. True Negative (TN)is the domain of valid emails divided as legitimate, False positive (FP) is the broad range of valid emails categorized as phishing. False Negative (FN)is the range of phishing emails divided as incorrectly as True positive (TP) is an extension of phishing emails categorized as phishing emails.

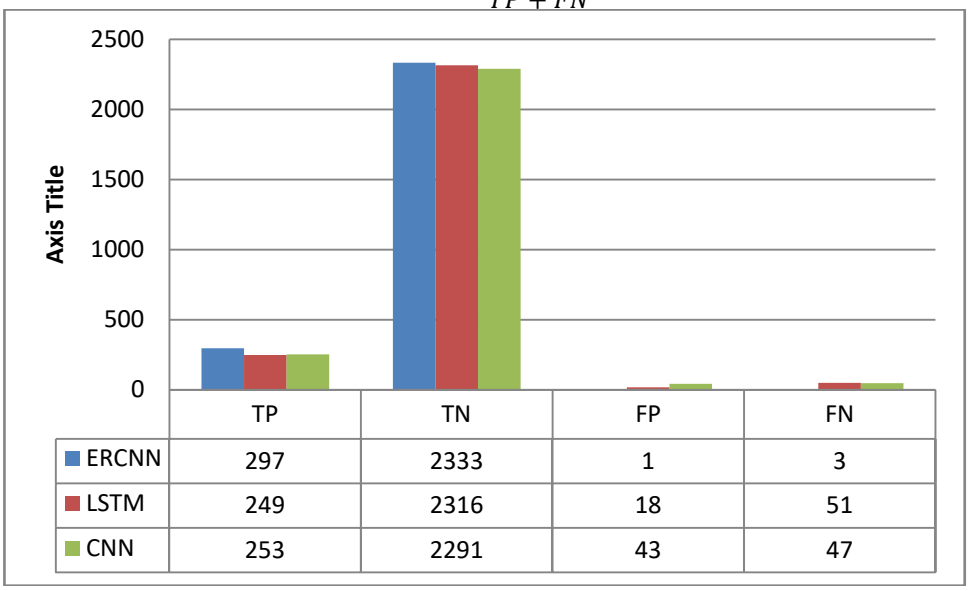
Table.1 The classification of confusion matrix

Predict / Actual	0 (legitimate	1(phishing)
0 (legitimate)	TN	FP
1 (phishing)	FN	TP

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FP}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$



	TP	TN	FP	FN
ERCNN	297	2333	1	3
LSTM	249	2316	18	51
CNN	253	2291	43	47

Fig. 2 The confusion matrix of test results

As a result of the confusion matrix, the amount of TP and TN is supposed to be significant, even if the FP and FN are rated low. As evidenced by the outcome of the confusion matrix in Figure 2, our version has more better TP and TN, FP and fewer FN than the two alternative methods. Confusion matrix results are restricted to the domain. When faced with a big data, like this test, the simplest version's advantages and disadvantages are difficult to quantify. Therefore, we utilize the result of a mixed matrix to determine and achieve similar evaluation notices.

Table.2 experimental results comparison between proposed methods with previous methods

	Accuracy	**Precision**	**Recall**
LSTM	0.974	0.934	0.841
CNN	0.966	0.855	0.848
ERCNN	0.998	0.996	0.99

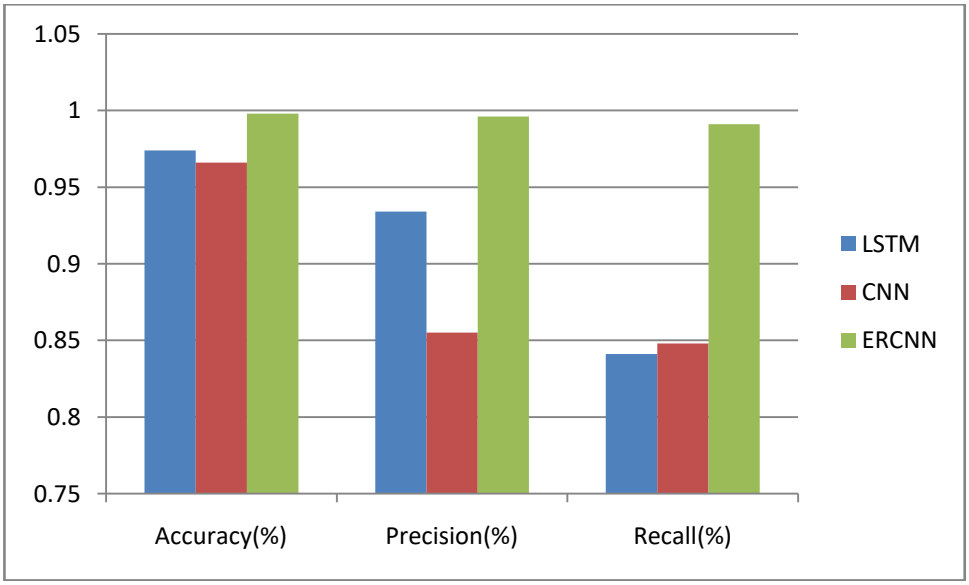


Fig.3 The summary of test results

To perform an accurate evaluation, we performed the methods as the recommended baseline ERCNN, which used CNN and RNN algorithms.
As shown in Figure 3, the ERCNN version accuracy is 99.8%, precision is 99.6%, and recall is 99.0%. All offers are superior to CNN and LSTM strategies
Although deep mastery is nearly inexplicable, we strive to analyze experimental results through misclassified emails. We tried to split emails from these four components (TP, TN, FP, and FN) from the CNN confusion matrix into the email header and email frame. Then we used the CNN template to discover the email address and email body, respectively. We compare the effects of the results received using each email.

V. CONCLUSION

We are using a modern version of deep learning known as ERCNN to identify phishing emails in this paper. The performance uses the enhanced RCNN community to model email address and textual email content in every male or female grade and sentence score. Therefore, the noise in the model is reduced. In the proposed model, used the eye mechanism inside the head and body, making the breed more interested in the most valuable information. We use an unbalanced set of records closest to the world of global behavioral experiences and calculated the representation. The ERCNN got a promising result. Many experiments have been conducted to express the advantages of the proposed version of ERCNN. We can also stay up-to-date on how we can improve our phishing email detection model without the email header and maximum practical email framework.

REFERENCES:

[1] APWG, “Anti phishing work group,” 2019, https://www. antiphishing.org/.
[2] “Google safe browsing API,” 2019, https://developers. google.com/safe-browsing/v4/.
[3] Y. Le , Y. Cao, W. Han, 2008, “Anti-phishing based on automated individual white-list”, pp. 51–60.
[4] BlasiM ,”Techniques for detecting zero day phishing websites”,2009.
[5] L. A. T. Nguyen, K H. Nguyen, 2013, ”Detectingphishing web sites: A heuristic URL-based approach,”, pp. 597-602.
[6] Nguyen M, Nguyen T. H, T. Nguyen, “A deep learning modelwith hierarchical LSTMs and supervised attention for anti-phishing'',2018.
[7] X. Li and J. Zhang, 2017, ``Phishing detection method based on borderlinesmotedeep belief network,'',pp. 45_53.
[8] M. Abadi*et al.*, 2016, ``TensorFlow: A system for large-scale machine learning,''in *Proc. OSDI*, vol. 16, 2016, pp. 265_283.
[9] T. H. Nguyen and R. Grishman, 2015, ``Relation extraction: Perspective fromconvolutional neural networks,'' pp. 39_48.
[10] J. Schmidhuberand M. F. Stollenga,``Deep networkswith internal selective attention through feedback connections,'', pp. 3545_3553, 2014.
[11] R. Verma and N. Hossain, 2013, ``Semantic feature selection for text with applicationto phishing email detection,'', pp. 455_468.
[12] N. Hossain and N. Shashidhar, 2012, ``Detecting phishing emails thenatural language way'', pp. 824_841.
[13] J. Abawajy andI. R. A. Hamid, 2011, ``Hybrid feature selection for phishingemail detection,'', pp. 266_275.