Journal of Advances in Management, Engineering and Science (JAMES), 2026; 1(1): 11 – 17

Research Article

Intelligent Deep Ensemble Learning Model for Advanced Phishing Attack Detection and Cybercrime Forensics

Dr. M. Senbagavalli, Associate Professor, Alliance School of Advanced Computing, Alliance University, India
senba1983@gmail.com
Received 27th June 2025; Accepted 28th November 2025

http://doi.org/10.65470/james.11

Abstract **–** One of the most common types of cybercrime is phishing, which uses social engineering and technological deceit to obtain sensitive personal and financial data through email spoofing, malicious websites, and destructive software installations. Phishing attack detection is an important field of study in cybercrime forensics because attackers use a variety of communication methods, such as emails, URLs, messaging apps, and phone calls. In order to overcome this obstacle, this work builds a new model that combines group convolution with a symmetric structure rather than using a conventional CNN. It then uses the SMOTE to control the data's class imbalance. Incorporating snapshot ensemble improves the model's generalisability without drastically raising computational costs, while cyclic cosine annealing learning rates further boost the training process. With a classification accuracy of 99.12%, the suggested method for detecting phishing attacks outperforms four existing ensemble methods, according to the results. Using ensemble learning techniques in conjunction with group convolution greatly improves accuracy and adaptability, as seen below. Finally, the suggested approach provides a solid defence against the increasing danger of phishing attempts by providing a dependable, effective, and extensible cybercrime forensics solution.

Keywords—Phishing Attack Detection (PAD), Uniform Resource Locators (URLs), Conventional Neural Network (CNN).

I. INTRODUCTION

Modern life in the digital age would be incomplete without the internet, that has become an integral component of many aspects of today's world, from communication to online banking and shopping. This tendency has been made even faster by the widespread availability of smartphones, that allow people to easily and comfortably access the internet. Smartphones have become an essential part of people's daily lives, changing the way they interact with technology, according to studies[1].The importance of strong cybersecurity measures to safeguard consumers from different online threats is highlighted by this reliance on internet technology. Cybercrimes are becoming more complex and common as the number of devices connected to the internet keeps increasing. As a result of people's and businesses' reliance on the internet, cybercriminals are able to conduct a wide range of illegal activities. One of the most common forms of cybercrime, phishing attempts to trick victims into giving over sensitive information like passwords, bank account details, or personal identification numbers. These assaults frequently take the form of seemingly legitimate websites, emails, or messages, making it difficult for consumers to recognize them[2]. Phishing via URLs is a kind of cyberattack that uses email and URLs to trick users into thinking the message is from a legitimate source, like a bank or company, and thus more likely to download attachments or click on links[3]. Thereafter, the user's data becomes accessible to attackers. In addition, phishing websites and emails are made to appear like legitimate business ones. Phishing is one of the most well-known and long-standing forms of cyberattack.

The goal of phishing, a kind of cyberattack, is to get users to provide sensitive information by email, phone, or text message. One term for a social engineering attack is phishing. In this type of attack, the attacker sends an email containing a link that, when clicked, takes the victim to a malicious website where they are tricked into divulging sensitive information[4]. This data can then be utilized for illicit activities such as identity theft, black market sales, or other financial gains. The majority of phishing attacks occur on social media or banking websites, that the hacker can gain access to important

information and utilize it for his own gain. In order to trick even the most careful visitors, these fake sites deploy complex methods to evade standard security protocols. The difficulty of detecting and preventing phishing attacks is growing as their sophistication rises.

Modern attackers use sophisticated techniques like optical character recognition to conceal harmful material within photographs and avoid traditional detection methods[5]. In addition, phishing efforts often use legitimate-looking but infected websites to trick people into visiting dangerous ones. In order to trick customers into visiting malicious websites, spammers inject fake links into email content. In this operation, the fake URLs imitate popular websites, giving them an air of mystery. In addition, delays and network congestion are the results of sending and receiving a large volume of spam emails. At least in theory, the network wouldn't crash if spam messages were blocked. Email security and user resource protection could be improved with the ability to identify and confirm real emails. However, it may be time-consuming and expensive to filter out a large quantity of spam emails, even when human spam recognition is possible.

Here is the outline of the paper: The relevant literature is reviewed in Section 2, and Section 3 presents a new approach to cybercrime forensics and phishing attacks. The dataset utilised in this study is described in Section 4, together with the experimental results and analysis. Section 5 presents the conclusions.

II. LITERATURE SURVEY

In order to identify phishing attempts on websites, they unveiled a hybrid ML method. A vector representation of the URL-centric dataset initially was acquired, and it was then preprocessed to eliminate any null values. Afterwards, the features chosen using the canopy technique were trained using a hybrid model that included LR, SVM, and DT classifiers. The results of the predictions were enhanced by employing the grid search optimization method. The result was an improvement in performance due to the enhanced precision and accuracy. However, the chosen SVM failed to learn the higher amount of data adequately[6]. LR is used in URL phishing detection to identify long URLs that belong to the same server. Bigrams and host-based features make this process easy. It is challenging to recognize complex URLs with LR due of its simplicity.

Fixing this is as simple as deriving more complicated characteristics from the simpler ones. The approach also breaks out in cases where the data linkages are complicated and nonlinear. Its downsides are exacerbated by missing data as well. The overall performance is limited by making static assumptions before training[7]. In an effort to quickly and accurately identify phishing attempts, they provided a model that integrates neural networks with binary visualization. As the model learns from mistakes and improves identification over time, the BV approach reveals structural variations in web pages[8]. Further work is required to improve accessibility through browser extensions and user interfaces, although XGBoost was found to be highly accurate in URL-based phishing detection.

Transformers have completely changed the game when it comes to phishing detection. They use self-attention processes to zero in on the most important parts of the input data. Because of this feature, the models can identify phishing signals that are both subtle and fine-grained, that can be missed by more traditional methods. The capacity to handle and integrate several forms of data concurrently is a key strength of transformer-based models[9]. These models can integrate visual aspects like logos and webpage layout with textual information like URLs and metadata through multimodal feature fusion. Their structural features of websites are also taken into account. This combination improves the model's detection capabilities by enabling it to examine phishing attempts from several angles[10]. Various studies have also offered different techniques from different academic viewpoints.

For instance, one of the most basic methods, known as blacklisting or whitelisting, involves compiling a list of legitimate and illegal URLs[11]. The problem with this method is that it is susceptible to viruses, such as zero-day assaults, and not all phishing websites are included in the lists. To circumvent this limitation, numerous machine learning methods have demonstrated to be highly beneficial[12]. These methods include NB, hybrid feature selection, RF, LR, SVM, and AdaBoost. These methods train the classifier using features extracted from URLs or webpage contents.

Hence, in order to enhance the model's generalisation performance while keeping training costs low, they shall investigate a snapshot ensemble strategy. Group convolution, rather than conventional convolution, is used by the fundamental classifier. The ensemble model's generalisability was enhanced by a snapshot ensemble, which reduced training expenses without sacrificing accuracy. The method's efficacy has been demonstrated in multiple experiments.

III. PROPOSED SYSTEM

As the number of people using the internet continues to skyrocket, more and more of their personal details are being made public. Consequently, fraudsters have access to a deluge of sensitive financial and personal data. Cybercriminals can fool users and obtain sensitive information using techniques like phishing. Cybercriminals, who have made a living off of the illicit exploitation of digital assets, particularly personal information, are just as quick to adapt to the ever-changing digital landscape.

From January to May 2015 and May to June 2017, a total of 5,000 phishing and 5,000 legal websites were downloaded, and 48 features were retrieved from these datasets. In contrast to the regular expression-based parsing method, the feature extraction method that makes use of the browser automation framework (namely, Selenium WebDriver) is more accurate and resilient [13].

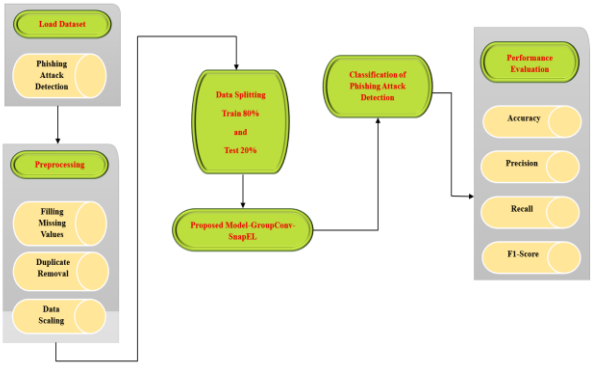

Fig. 1. Phishing Attack Proposed Model Framework

In Figure 1 they can see the proposed model together with the associated processes. The features extracted from the dataset are the initial inputs to our model. Missing data, normalization, and other tasks are part of the preprocessing stage, which has begun. Given that phishing website instances constitute merely 3.27% of total observations, addressing this disparity is essential for effective model training due to the dataset's class imbalance[14].

A. Data Preprocessing:

Doing basic preparation operations on datasets is the first and most crucial step in getting them ready for analysis and modeling of phishing websites. Dealing with incomplete data Methods like these include standardizing data size and removing extraneous data. By finishing these procedures, you may improve the information's consistency and set the stage for accurate evaluation and effective modelling to identify potential phishing attack scenarios.

Absent Data Managing: The primary objective of missing value management is to resolve data discrepancies caused by incomplete or missing information. Mean imputation is one approach that is commonly employed for this purpose. When a value is lacking for a given characteristic, mean imputation can fill it in by utilizing the average of the known data points for that characteristic. They can see the process in a nutshell in Equation (1).

$$U_{filled} = \frac{1}{X}\sum_{q=1}^{X} U_q \qquad (1)$$

The expected values to fill the gaps are denoted by U_{filled}, the initially observed values are represented by U_q, and the total number of non-missing values is denoted by X.

Duplicate Record Removal: Eliminating duplicate entries ensures that our dataset contains only unique data points, reduces the likelihood of bias caused by duplication, and keeps our data accurate and trustworthy. To extract the unique records from all of them, it's necessary to compare and contrast them using equation (2).

$$H_{distinct} = \{h_r \in H : No\ identical\ entry\ in\ H\ matches\ h_r\} \qquad (2)$$

When all duplicate entries have been eliminated from a dataset, it is marked as $H_{distinct}$. One unique entry h_r and the original collection H, which may have contained duplicates, are the descriptors used to describe this dataset.

To ensure uniformity and consistency across all numerical parameters, data scaling is a crucial step in data preparation. Standardization and min-max scaling are the two most used methods for this. Standardization involves transforming a characteristic C to achieve a standard deviation of one and a mean of zero. Equation (3) shows that this transformation allows us to compare feature C with other features in a dataset efficiently.

$$B_{normalized} = \frac{B - \sigma}{\mu} \qquad (3)$$

If you look at the equation above, you can see that $B_{normalized}$ stands for the normalized feature, B is the original feature, σ is the mean, and μ is the standard deviation. Nevertheless, in order for a feature B to fit

within the range [0,1] stated in equation (4), it is altered using min-max scaling.

$$B_{normalized} = \frac{B - B_{min}}{B_{max} - B_{min}} \quad (4)$$

$B_{normalized}$ is now a variable that represents a feature that has been scaled or normalized according to its minimum B_{min} and maximum B_{max} values, as well as its original value B.

B. Model Training:

1) GroupConv-SnapEL:

The suggested phishing attack approach in this paper is based on GroupConv-SnapEL. Figure 2 shows the overall framework of the system. The snapshot ensemble model and the group convolutional network model are the two primary components of the approach. The group convolutional network model initially receives the preprocessed data [15]. Subsequently, various snapshot models are generated by the training of the group convolutional network. The final classification results are derived by ensemble, with these models serving as basis classifiers. Here is the procedure for putting this strategy into action:

1. Preprocessing the data is an absolute essential. Digitisation, normalisation, and numerical matrix conversion are all parts of data preprocessing. To train a group CNN, plug in the numerical matrix.
2. Instead of using regular convolution, group convolution is employed, and multi-channel fusion is used to produce the basis classifier. This article employs cosine annealing learning rate to train the model to consistently achieve several local optimal points and preserve these models.
3. Employ the averaging technique to aggregate the stored models and derive the categorisation outcomes. The parameters of each model represent the optimal local parameters obtained during training, and all exhibit a high classification accuracy rate.
4. The test data that has been preprocessed is inputted into the snapshot ensemble model, which then produces the test data's classification results.

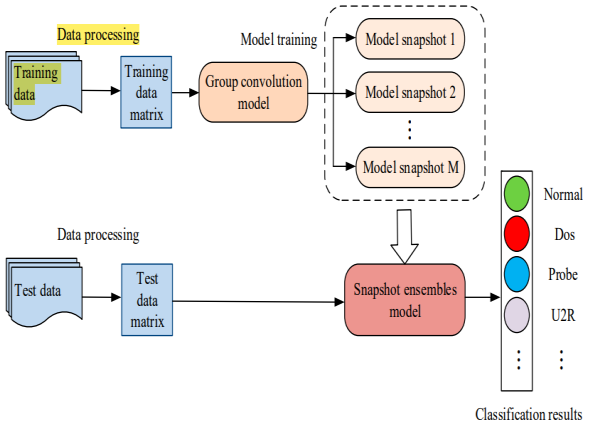

Fig. 2. The Overall Framework for GroupConv-SnapEL

a) Group Convolution

In most cases, adding more feature maps can boost the model's performance. However, keep in mind that overfitting can occur with bigger parameter scales, and certain convolution kernel components will be unnecessary. With the introduction of Group Convolution in AlexNet, the goal was to partition the network such that it could be executed concurrently on two GPUs; this would address the issue of inadequate video memory and allow for further optimisation in the ResNeXt network. Group convolution, which is identical to the original convolution technique. Although it performs the same convolution function as ordinary convolution, group convolution is easier to avoid overfitting and uses fewer parameters.

Prior to convolving each subset of input data independently, group convolution must group the data into appropriate categories shown in equation (5).

$$U(c) = \sum_{r=1}^{T} S_r(c) \quad (5)$$

where $[c_1, c_2, \ldots, c_T]$ is the input feature map divided into T groups.

b) Group Convolution Multi-Channel Fusion

Grouped convolution runs convolution operations independently on each group, which means that the input feature map is incomplete and that the output feature map is incomplete as a result. As a result, there may be no way for the results from each group to contribute to the other. In this article, group convolution is employed to eliminate unnecessary parameters, and multi-channel fusion is employed to enhance feature information by strengthening the information sharing of feature maps between channels. This article uses the multi-channel fusion method to improve the information interchange

between the network's output feature maps from different layers and to enhance the feature information at each level. It is possible for the network's convolution blocks to take input only after all the features in front of them have been merged because each block is combined in pairs. The feature channel's connecting function allows for the fusion of each module's features. A fully connected layer, three group convolutional blocks, a global pooling layer, and softmax are all components of the group convolutional network model. The model's final classification result is then obtained. Hence, non-linear processing is carried out using the ReLU activation function, and BN processing follows each convolution operation.

c) Shapshot Ensemble

EL improves a model's classification performance by producing a model with better generalisability than a single model could. A snapshot ensemble can modify the learning rate using cosine annealing without raising training costs, in contrast to traditional ensemble approaches which produce substantial training costs. In this part, examine the model's testing and training principles, the snapshot ensemble principle, and the evolution of the cosine annealing learning rate.

d) Principle of Snapshot Ensemble

Through its training process, Snapshot Ensemble is able to produce a collection of different and realistic models. At its heart, snapshot ensemble is an optimisation procedure that, before finally converging, visits numerous local minima. Capturing an image of the model at each local minimum and preserving the corresponding parameters equates to obtaining a comprehensive snapshot of the entire model.

Using the computational processes outlined in Formulas (6) and (7) , the snapshot ensemble optimises using stochastic gradient descent (SGD):

$$t_g = \nabla_{\theta_{g-1}} U\left(\theta_{g-1}\right) \quad (6)$$

$$\Delta\theta_g = -\xi * t_g \quad (7)$$

where t_g stands for the gradient and ξ for the learning rate. Generalisability is frequently better at the relatively flat local minimum, even though the trained network model may fail to converge to the global minimum on occasion. An excessively high learning rate hinders the convergence speed while optimising with SGD, causing it to swing near the extreme point. Although convergence will be slower with a low learning rate, it will frequently reach the optimum local minimum. Various optimisation phases can take use of SGD's drastically diverse behaviour. Enter a somewhat flat local minimum while keeping the learning rate high at the beginning of the optimisation. The learning rate will fall, reach a lower level, and converge to a local minimum once the gradient is not updated anymore.

IV. Result and Discussion

The term "phishing" refers to the practice of sending fraudulent emails that pose as legitimate businesses in an effort to trick recipients into divulging sensitive information. Phishing emails frequently masquerade as communications from well-known websites, such as social media, auction houses, online payment processors, or IT administrators, in an effort to trick the naive. Malicious links to websites might be included in phishing emails.

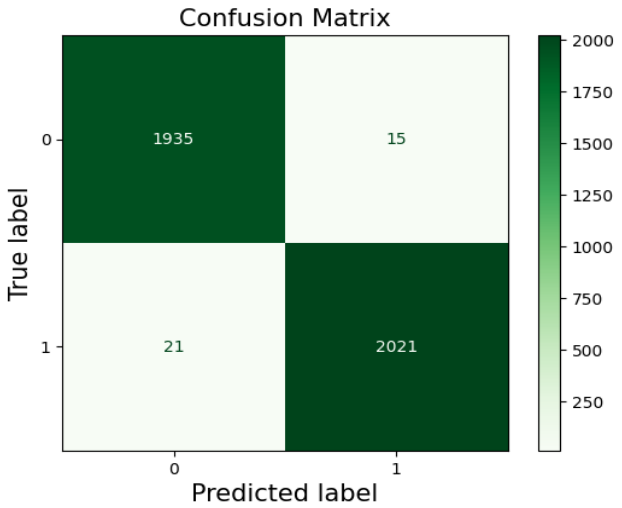

Fig. 3. Confusion Matrix

The confusion matrix graph in Figure 3 shows that a well-tuned model should have excellent accuracy. One way to see how well a classification model did is to look at its confusion matrix, which is a table that shows the percentage of right and wrong predictions for each class.

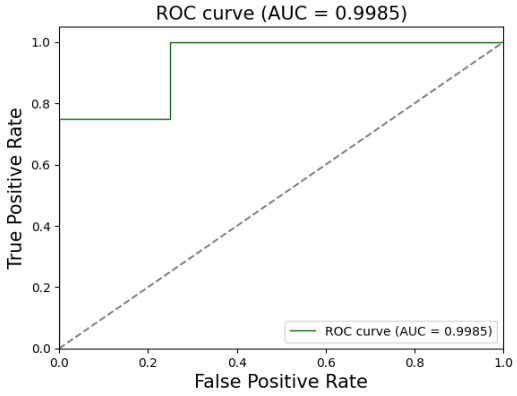

Fig. 4. ROC Curve

As a graphical representation, ROC shows the relationship between specificity and sensitivity. The receiver operating characteristic (ROC) plots the ratio of true positives (TP) to false positives (FP). The AUC is a measure of accuracy that lies under the ROC curve. As demonstrated in Figure 4, our experiment yielded an AUC of 0.9985.

TABLE I. PERFORMANCE COMPARISON(%)

Models	Accuracy	Recall	Precision	F1-Score
CNN-LSTM	92.18	90.30	88.71	92.88
BiLSTM	96.43	94.76	92.83	96.74
GroupConv-SnapEL	**99.12**	**97.61**	**95.52**	**99.92**
DNN	90.67	88.40	86.37	90.64

By comparing how well four machine learning algorithms—CNN-LSTM, BiLSTM, GroupConv-ShanpEL, and DNN—detect phishing websites, they can see how accurate they are. The outcomes are primarily evaluated using four metrics: accuracy, precision, recall, and F1 score shown in Table 1.

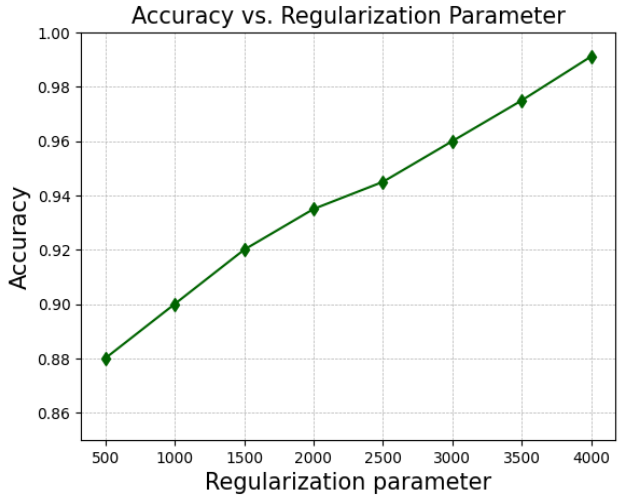

Fig. 5. Accuracy Curve for Proposed model

Figure 5 shows the relationship between the regularisation parameter and the accuracy. If the regularisation parameter is greater than 500, accuracy remains constant, but it improves when it's less than 500. The greatest value is 99.12% at a regularisation parameter of 4000.

Figure 6 graphic displays the capabilities of CNN-LSTM, BiLSTM, GroupConv-SnapEL, and DNN. CNN-LSTM achieves 92.18 percent accuracy, GroupConv-SnapEL reaches 99.12% accuracy after

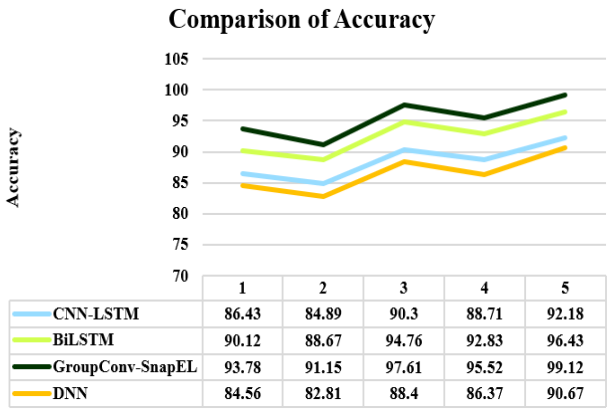

Fig. 6. Accuracy Comparison

classification, BiLSTM reaches 96.43 percent, and DNN reaches 90.67 percent. In Figure 6, they can see the results of the accuracy of these chosen machines and deep learning approaches.

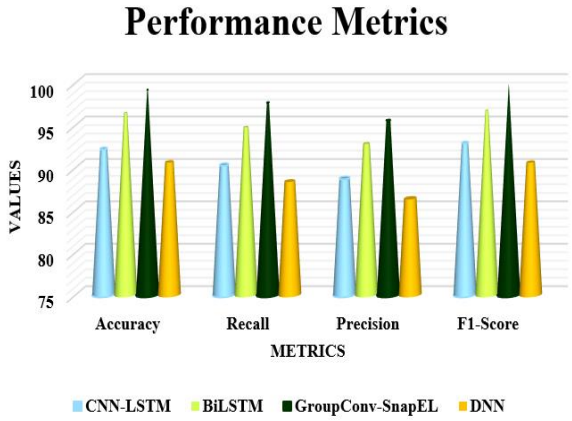

Fig. 7. Performance Metrics

Figure 7 displays the comparison of performance for F1-Score, recall, accuracy, and precision. With an accuracy rate of 99.12%, our suggested GroupConv-SnapEL Model outperforms the competition.

V. CONCLUSION

The fraudulent practice of phishing, in which the imposter poses as a legitimate business or organization in an effort to get access to sensitive information through email or other forms of electronic communication, has rapidly progressed from its humble beginnings as "a wide net." Using advanced methods, spear phishing assaults zero in on a specific high-value individual. In phishing, a type of automated social engineering, cybercriminals pose as trustworthy websites in order to trick users into divulging critical information. It employs SMOTE to manage data imbalance during initial data processing as part of our methodical effort to tackle the growing threat of phishing attacks and cybercrime forensics. In place of traditional convolution, this study presents

ensemble learning and builds a base classifier using a model of a group convolution network. Several snapshot models are produced by training the base classifier with the cyclic cosine annealing learning rate. The ensemble method produces a model with good generalisability. In comparison to four other ensemble approaches, this one achieves a classification accuracy of 99.12% on datasets, proving its usefulness.

REFERENCES

[1] S. R. Selamat, R. Rizal, C. Nursihab, and N. Amien, "Advanced Phishing Attack Detection Through Network Forensic Methods and Incident Response Planning Based on Machine Learning," *Int. J. Informatics Comput.*, vol. 1, no. 1, p. 19, 2024, [Online]. Available: https://iaico.org/index.php/JICO/article/view/1/3

[2] R. S. Andavar and S. Rathna, "Advanced Phishing Website Identification using Transformer-Based Models that Incorporate Attention Mechanisms and Multimodal Feature Fusion," *Adv. Phishing Website Identif. using Transform. Model. that Inc. Atten. Mech. Multimodal Featur. Fusion*, vol. 12, no. September 2024, pp. 36–49, 2024, [Online]. Available: https://www.researchgate.net/publication/392760201

[3] Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, Q. E. U. Haq, K. Saleem, and M. H. Faheem, "A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN," *Electron.*, vol. 12, no. 1, pp. 1–18, 2023, doi: 10.3390/electronics12010232.

[4] G. S. and N. B. P.K., "Analysis of Phishing Detection Using Logistic Regression and Random Forest," *J. Appl. Inf. Sci.*, vol. 8, no. 1&2, pp. 7–13, 2020, [Online]. Available: http://www.publishingindia.com

[5] L. Shammi and C. Emilin Shyni, "A Novel Approach for Effective Detection and Prediction of Sophisticated Cyber Attacks Using the Stacked Attention GRU and BiLSTM," *1st Int. Conf. Electron. Comput. Commun. Control Technol. ICECCC 2024*, pp. 1–6, 2024, doi: 10.1109/ICECCC61767.2024.10593866.

[6] M. Murhej and G. Nallasivan, "Multimodal framework for phishing attack detection and mitigation through behavior analysis using EM-BERT and SPCA-BASED EAI-SC-LSTM," *Front. Commun. Networks*, vol. 6, no. July, pp. 1–22, 2025, doi: 10.3389/frcmn.2025.1587654.

[7] N. N. Naik, "Modelling enhanced phishing detection using XGBoost," *Diss. Dublin, Natl. Coll. Irel.*, 2022, [Online]. Available: https://norma.ncirl.ie/5512/

[8] A. Khan, D. M. Ahmed, and A. Fathima, "Enhanced Phishing Detection Using Machine Learning Algorithms: A Comparative Study of Random Forest, SVM, and Logistic Regression Models," *SSRN Electron. J.*, 2025, doi: 10.2139/ssrn.5191566.

[9] S. J. Yatish, V. Vinod, S. Subodh Pande, V. Lakshmi Narayana, N. Nishant, and P. T. Sivagurunathan, "Deep Learning for Attack Detection in Industrial IoT Edge Devices," *Proc. 8th Int. Conf. Commun. Electron. Syst. ICCES 2023*, no. Icces, pp. 539–544, 2023, doi: 10.1109/ICCES57224.2023.10192890.

[10] S. Sachdeva and A. Ali, "Machine learning with digital forensics for attack classification in cloud network environment," *Int. J. Syst. Assur. Eng. Manag.*, vol. 13, no. January, pp. 156–165, 2022, doi: 10.1007/s13198-021-01323-4.

[11] A. H. Alsadig and M. O. Ahmad, "Phishing URL Detection Using Deep Learning with CNN Models," *2nd Int. Conf. Intell. Cyber Phys. Syst. Internet Things, ICoICI 2024 - Proc.*, no. October, pp. 768–775, 2024, doi: 10.1109/ICoICI62503.2024.10696243.

[12] K. Veena, K. Meena, Y. Teekaraman, R. Kuppusamy, and A. Radhakrishnan, "C SVM Classification and KNN Techniques for Cyber Crime Detection," *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/3640017.

[13] "Phishing Dataset for Machine Learning." Accessed: Sep. 26, 2025. [Online]. Available: https://www.kaggle.com/datasets/shashwatwork/phishing-dataset-for-machine-learning

[14] F. S. Alsubaei, A. A. Almazroi, and N. Ayub, "Enhancing Phishing Detection: A Novel Hybrid Deep Learning Framework for Cybercrime Forensics," *IEEE Access*, vol. 12, no. January, pp. 8373–8389, 2024, doi: 10.1109/ACCESS.2024.3351946.

[15] A. Wang, W. Wang, H. Zhou, and J. Zhang, "Network intrusion detection algorithm combined with group convolution network and snapshot ensemble," *Symmetry (Basel).*, vol. 13, no. 10, 2021, doi: 10.3390/sym13101814.