Selection Technique based Gated Recurrent Unit for Phishing attack detection using several URL

ThangaTamilSelvi S[1], Astangini Selvaraj[2],Kavitha Devi M K[3]

CSE, Bannari Amman Institute of Technology

CSE, Thiagarajar College of Engineering

CSE, Thiagarajar College of Engineering

Abstract-Phishing attacks remain a considerable risk for user data on internet, highlighting the need for sophisticated detection systems. Phishing attacks typically involve cybercrimes with user driven disclosing profound information, such as user login or financial transactions, via emails or specific websites. Phishing sites are widely used as social tools that enable fraudulent actions in day to day activities. This research focuses on the efficacy of a selection based Gated Recurrent Unit (S-GRU) model for predicting phishing attack from thousands of URL and internet protocol addresses attaining an accuracy rate of 98.14%. This paper affords an intense view of Deep Learning algorithm for effective detection handling numerous websites. We performed experiments on an extensive dataset consisting of 95,000 URLs. Our main goals are to enhance cyber security measures against phishing attacks, to innovate by incorporating various attention mechanisms based on GRU, and to certify the effectiveness of our model through certain metrics. The cyber security faces increasing trails; our study enables significant acumens and also outlines a a scope for future cyber security role play.

Keywords: selection based Gated Recurrent, Deep Learning, Phishing sites and cyber crimes

I. INTRODUCTION

The recent challenge on internet is the cyber security that encompasses the protection of data used in several application on internet suffer from various cyber threats. As digital attacks become more sophisticated, they pose some challenges in the information management associated with data handling risks. A common form of these attacks is phishing,[1] where predators create counterfeit websites that closely resemble legitimate ones, for hacking or misuse of personal information such as login with passwords, bank details, etc. Many workgroups handling these phishing attacks provides a survey for the past three years handling more than 50 lakhs websites under these types of attacks. Several detection techniques are incorporated for the analysis and avoidance of URL based phishing detection. This paper examines AI based strategies aimed at mitigating phishing attacks with a focus on secure readability, fraudulent website visits and submission of secure data online.

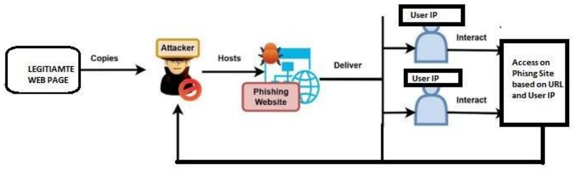

Figure 1 Phishing attach on a legitimate web page

The availability of data in the proposed solution is crucial for its successful implementation; any issues regarding data availability could adversely affect the project's accuracy. [2] The data utilized for model testing must be both reliable and suitable to effectively identify all websites that the user intends to examine. Additionally, model consistency is a significant factor that could lead to project failure, necessitating that the model accurately determines the true identity of URLs. This method utilizes features inherent to standardized resource locators (URLs). The defined features include URLs associated with phishing sites. The proposed approach leverages specific characteristics to detect phishing attempts. The strategy was evaluated using a dataset comprising 3,000 URLs from phishing sites and 3,000 URLs from legitimate sites. Phishing is recognized as a form of cybercrime characterized by the imitation of a legitimate enterprise's website with the intent of obtaining confidential details shared on the web including pin numbers [3][4]. Distinctive traits differentiate phishing websites from authentic ones, including elongated URLs, the presence of an IP address within the URL, and the addition of prefixes and suffixes to the domain and request URL. This paper focuses on abstract structures that are routinely mined from websites using a novel device, rather than depending upon qualified professionals for handling data online and estimates the reputation of these features for determining webpage accessibility [5]. This research aims to achieve a set of proven models that could be steadfast and nominal in foreseeing improper websites based on URL and IP address-based detection. If an IP address is utilized as a substitute for the domain name in the URL, such as “http://x.x.x.x/fake1.html,” users should be wary, as this indicates a potential attempt to compromise their personal information.

II. Literature Review

Modelling Hybrid feature Based [3] Phishing website detection aim to analyse website to steal private data, including card details, security codes and passwords. Several anti-phishing technologies are unable to identify zero-hour phishing attacks. Furthermore, as they rely on outside sources like search engines, older methods are complicated and inappropriate for real-time settings. For the goal of conducting tests utilizing well-known some of the classification approaches, this study concludes a presents a novel dataset used in many experiments.

This literature evaluate analyses the cutting-edge panorama of AI-pushed phishing detection technology. This aid to inspect research with a different credible reasserts from beyond ten years of data. Phishing, which commenced as smartphone-phreaking and has advanced into internet are totally based on scams, stays an essential chance to customers worldwide to be addressed. Early detection techniques presented low accuracy, with conventional structures frequently failing to apprehend phishing attempts. Advanced [17] AI-pushed approaches—spanning gadget learning (ML), deep learning (DL), and hybrid models—have proven promising effects in improving detection capabilities. Nevertheless, those AI techniques introduce new challenges, which include extended computational needs and a hazard of fake positives, which may be steeply-priced to manipulate in real-time environments.

Many current methodologies rely on manually designed lexical and statistical features derived from the textual content of websites to develop some methods of classification on finding fake web pages [19].However, many phishing detection techniques h ave drawbacks, including (1) the excessive man power and time consuming procedure for extracting manually crafted features, which necessitates specialized knowledge to identify which features are relevant for a specific platform; and (2) the challenges faced by models based on these manually crafted features in effectively recognizing the semantic patterns present in the words and characters found in URLs and HTML content.

NLP methodologies for classification and training purposes are examined in several studies with various alternatives. The aim of this research is to review that synthesizes existing application in identifying attacked emails. The several research in recent years have detected many phishing sites. This study focuses on key many domains in email detection with attacks, through learning algorithms involved in content based features present in emails, and utilized resources, where the evaluation metrics applied [28][29] The results indicate the every primary focus extraction of attacked emails, followed by classification and prediction of phishing content online. Among the various algorithms used for classification, support vector machines (SVMs) are predominantly used for email detection. The commonly employed techniques include TF-IDF and word embeddings.

III. Methodologies

Generally, two Methodologies are utilized to identify phishing websites. The first is the blacklist approach, which involves comparing the request requested URL against here predefined list of unknown phishing sites. A significant limitation of this method is that theblacklists often fail to encompass all phishing websites, as new fraudulent sites can be emerged within few moment. The second methodology is heuristic based, which gathers multiple features from a website to determine its legitimacy. Unlike the blacklist approach, heuristic methods can detect newly established phishing sites. This effectiveness on exploratory approach relies on the careful selection of distinctive features that can differentiate phishing sites from original. Feature extraction performed on various applications, for the users to identify fake or original website. However this method requires users to invest considerable time in understanding the latest phishing tactics, which can be challenging for most internet users. Alternatively, automatic extraction is employed. This involves analysing the webpage to identify patterns commonly used by phishers.[6][7] This analysis includes examining the web page properties derived from HTML tags or by the corresponding logical address of the web page.

This study explores the revealing of phishing URLs through the usage of Gated Recurrent Unit (GRU) models enhanced with better mechanisms. We aim to improve the efficacy of differentiating between legal and phishing sites by utilizing the features that inherited to the website URLs and implementing an advanced GRU models. Our contribution to this fields includes the introduction of a deep learning methodology that employs GRU with valid mechanisms specifically for phishing attack monitoring. The presentation of impressive outcomes, such as elevated accuracy, precision, recall, and F1 score,[8] derived from an extensive dataset comprising 1 lakh URLs. - The fortification of cyber security measures against phishing threats by incorporating multiple attention mechanisms within the GRU framework and conducting thorough performance assessments. In contrast to traditional blacklisting techniques, our proposed method demonstrates the ability to adapt to the dynamic level of pressure, enabling the autonomous detection of new websites based on insights gained at the sampling phase. The embedding of various mechanisms into the GRU significantly uplifts its capability on identify relationships and concentrate on essential parts of input data that were analysed. The research extends its support to the applications of cybersecurity methods on investigating GRU-based approach with attention for precise phishing identification.

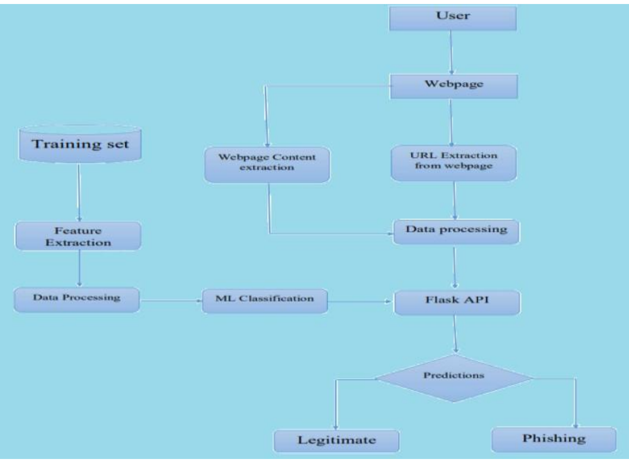

Figure2. Workflow of Selection based for GRU for phishing detection

All data obtained in this study include a total of one missing collected at Fish Storm, denoting not valid and valid sites. [9] To warranty a full assessment, the datasets were categorized into trained and tested sets. The education set consisting of 5,6730 samples served as the basis for teaching the GRU model, while the test consisting of 12,150 samples was reserved to assess the performance of the model. The proposed model for this study was created to distinguish between phishing and legitimate URLs. The selected method incorporates a closed recurrence unit for phishing detection. This combination is chosen to effectively capture sequential URLs, allowing the model to focus on a particular part of the input sequence. The input layer acts as an input point for input data and represents the input form. In this case, the input layer takes the entire sequence representing the tokenized URL The input layer determines the input form for the model that corresponds to the length of the URL sequence[10][11].

3.1 Gated Recurrent Unit (GRU)

A selection based Gated Recurrent Unit (GRU) refers to a different model with GRU structure, the mechanism to randomly choose data from past state of record for present state, enabling selection to rank related information based on the recent data, thus improving the working ability to aim on sequential data segregation.[12] This model works for identifying anomalies by selectively comparing current data to past information with relevancy.

3.1.1 Computational Formula:

Gate value: □□= (□□ [h□ −1,□□]);
Gate reset: $r_t = \sigma(W_r[h_t - 1, x_t])$
Candidate hidden state: $h_t' = \tanh(W_h[r_t \odot ht - 1, x_t])$;
state hidden: $h_t = (1z_t)h_t - 1 + z.\ h_t'$

Where tanh is the hyperbolic tangent and Wr is the weighted average of reset gate Wz is the weighted average of update gate. The gate rested determines which parts of state hidden should be elapsed. The gate to update findss the balance of novel and past information. The state that is hidden is calculated based on the updated hidden state. If the value of r_t =1 then it means the entire information from the previous hidden state H_t-1 is considered. If the value of r_t is 0 then the information from the previous hidden state is completely ignored.
The efficiency of S-GRU is much efficient than LSTM as they are faster in handling the information and needs only minimal storage capacity.

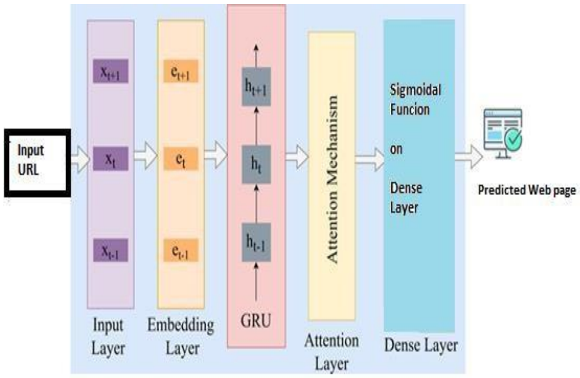

Figure 3: Working of Selection based GRU as layered approach

Phishing emails and URLs undergo a transformation into a format that is compatible with the model, typically involving the extraction of pertinent characteristics such as domain names, IP addresses, suspicious terminology, or the structure of the URLs.[13] Methods such as correlation analysis and feature importance scoring are employed to determine the most critical data to be extracted . These inputs are fed into the GRU network, designed to recognize patterns and relationships within the sequence that signal a phishing attempt. By concentrating on the most relevant features, the model is able to attain greater accuracy in detecting phishing attacks than if it were to utilize all available features.

Data set	cumulative size	Actual	Phishing
Trained set	67890	36471	39689
Tested set	18683	8563	9289
Tested set	90118	51009	45982

Table:1 shows the dataset with total size of training and testing dataset.

An inter-connected layer utilizing a function of activation function serves as the layer outcome for the GRU, facilitating the transmission of its output.[14][15] This transforms the data acquired from the sequential input into a score ranging from 0.0 to 1.0. A score closer to 1.0 signifies an increased probability that the input sequence is associated with the illegal class. The outcome is expressed as follows:

$$\text{Output} = \sigma\,(W_o \cdot C + b_o)$$

Where the variables W_o and b_o are the weighted matrix and bias vector connected layer representation, and σ is the sigmoid function[16].This study applies GRU with attention methods, and this performs well predict intricate URL based on IP address in website which dynamically concentrates on the most related details w.r.t website. This system is designed to improve the working performance in phishing site detection.

3.1.2 Training procedure

The procedure of the model includes neutralizing the parameters to reduce the loss generated on functional computation. This outlines the essential components such as precision value, recall value and F1 value based on the trained data sets.[18]

3.1.3 Evaluation metrics

In the metrics of evaluation the chosen parameters with its performance can be measures to analyse the efficacy of our process. The chosen set for analysis includes basic units as accuracy (Acc), precision (P), recall (R), and F1 score (F1). Accuracy is the unit measure of proportionately categorised URLs (phishing or legitimate) from huge data set containing websites based on the samples tested. With reference to data set. [20][21]

ACC=CL+CPCL+CP+InCL+InCP

where, CL is predicted legitimate URL count and CP is predicted anomaly URL count. The InCL denotes the incorrect predictions, where as InCP is the count of incorrectly predicted URLs as phishing sites.

IV. Results and summary

This study along with selection based GRU model gives improved accuracy with number of iterations carried out with minimal of 30 iterations [22]. The web site is analysed based on URL or with an IP address which can be predicted as legitimate or phishing site based on precision, F1 score, recall based on which accuracy can be achieved with maximum efficiency. The table 3 shows the class average of legitimate and phishing site based on the weighted average and level of accuracy.

4.1 Contributions:

The results of our research hold considerable significance for the domain of cyber security. By utilizing attention mechanisms with selection based GRU models, we improve the model's capacity to identify pertinent information and more effectively differentiate between legitimate and phishing URLs. This advancement has practical consequences for bolstering online security protocols,[23] particularly as phishing continues to be a widespread threat in the digital environment. In this experiment, we used different types of attention with GRU. The goal was to determine which mechanism gave the most accurate results. With this approach, we adapt the work mechanism of work at the time of time with HT weights, calculated from the GU output. Request, key and value of Q, K and V is obtained from the inputs according to the URL with HT using Wing, W_K and W_V weight matrices, respectively.

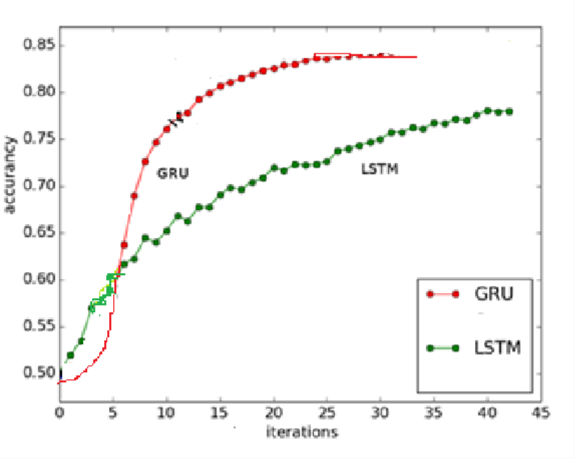

Figure 4: Graph with comparative analysis S-GRU vs LSTM

The performance of GRU is better than LSTM[24] as per the study, The GRU model is effective with less time for analysing as it has good performance review compared to the LSTM model. The estimated average time for both models are 11,836 and 6863s. This is given with accuracy level in the below table2.

Attention mechanism	Accuracy	F1 score	Precision	Recall	FPR	FNR
Multiplicative	0.9552	0.9887	0.9539	0.9839	0.0475	0.0160
Scaled Dot-product	0.9547	0.9516	0.9311	0.9836	0.0163	0.0715
Self-attention	0.9727	0.9682	0.9759	0.9489	0.0234	0.0510

Table 2: Performance based measure of selection based GRU and LSTM

Class Average	Precision	Recall	F1 Score
Phishing (Class 0)	0.981	0.990	0.981
Legitimate (Class 1)	0.992	0.982	0.982
Accuracy	0.980	0.981	0.980
Macro avg	0.981	0.980	0.981
Weight	0.982	0.982	0.982

Table 3 Shows the precision, Recall and F1 Score with accuracy

4.2 Sample Output

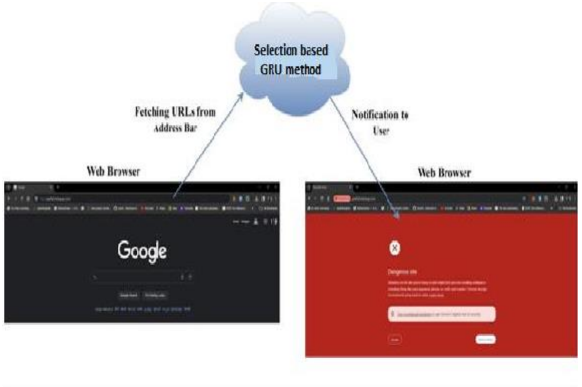

Figure 5: the sample webpage with phishing or legal website based on URLs/IP

As the result of this study, a comparative study has been made to find phishing website. The results shown gives a proposed selection based GRU with Long Short-Term Memory (LSTM) model. The GRU consistently surpassed this basic model (LSTM), underscoring its efficacy in identifying phishing URLs[25].

B. References

1. Kumar, A., Soni, R., &amp; Gupta, B. B. (2023).;A Hybrid Deep Learning Framework for Phishing Website Detection; IEEE Access, DOI: 10.1109/ACCESS.2023.3200038.

2. Shah, A., Ahmed, M., &amp; Lee, C. (2022).; Uncovering of Phishing Websites Using Multilayer Perceptrons and Random Forest, IEEE Transactions on Network and ServiceManagement, DOI: 10.1109/TNSM.2022.3167089.

3. Gupta, S., Kumar, D., &amp; Soni, P. (2023).;Phishing Detection and Prevention Using aHybrid Machine Learning Approach,; IEEE Security &amp; Privacy, DOI: 10.1109/MSP.2023.1234567.

4. Li, H., Chen, Z., &amp; Zhang, W. (2023).;AI-based Phishing Email Detection Using Natural Language Processing Journal of Information Security and Applications, DOI: 10.1016/j.jisa.2023.102301.

5. Zhang, J., Li, X., &amp; Liu, Y. (2022).;A Comparative Study of Phishing Detection Models Using Machine Learning; Computational Intelligence, DOI: 10.1007/s00542-022-07047-2.

6. Patel, K., &amp; Agarwal, A. (2024). finding Phishing Attacks Using Ensemble Learning and Feature Selection, Springer Advances in Science, Technology &amp; Innovation, DOI: 10.1007/978-3-030-23467-1

7. Xu, F., &amp; Yu, Z. (2022).;Deep Learning Approaches to Detect Phishing Websites Using URL and HTML Features, Expert Systems with Applications, DOI:10.1016/j.eswa.2022.115367.

8. Kumar, P., &amp; Patel, R. (2023).Phishing Website Detection Using Convolutional Neural Networks Information Sciences, DOI: 10.1016/j.ins.2023.02.056.

9. Singh, R., &amp; Khan, S. (2023).A Review on Phishing Detection Systems: Approaches and Trends, International Journal of Cyber Security and Digital Forensics, DOI:10.1080/19393555.2023.1836795.

10. Zhou, Q., &amp; Lee, K. (2022).Phishing Detection and Prevention Using a Hybrid Deep Learning Model, Journal of Cybersecurity and Privacy, DOI:10.1080/26938721.2022.2004974.

11. Kumar, R., &amp; Sharma, V. (2023). Phishing Attack Detection Using Machine Learning Algorithms, in Handbook of Research on Cybersecurity and Digital Forensics, IGIGlobal, DOI: 10.4018/978-1-7998-8594-1.ch011.

12. R. Zieni, L. Massari and M. C. Calzarossa,;Phishing or Not Phishing? A Survey on the Detection of Phishing Websitesin IEEE Access, vol. 11, pp. 18499-18519, 2023, doi:10.1109/ACCESS.2023.3247135.

13. M. Almousa and M. Anwar,;A URL-Based Social Semantic Attacks Detection WithCharacter-Aware Language Model; in IEEE Access, vol. 11, pp. 10654-10663, 2023,doi: 10.1109/ACCESS.2023.3241121.

14. H. Shirazi, S. R. Muramudalige, I. Ray, A. P. Jayasumana and H. Wang,;AdversarialAutoencoder Data Synthesis for Enhancing Machine Learning Based Phishing DetectionAlgorithms; in IEEE Transactions on Services Computing, vol. 16, no. 4, pp. 2411-2422, 1 July-Aug. 2023, doi: 10.1109/TSC.2023.3234806.

15. D. He, X. Lv, X. Xu, S. Chan and K. -K. R. Choo,;Double-Layer Detection of InternalThreat in Enterprise Systems Based on Deep Learning,&quot; in IEEE Transactions onInformation Forensics and

Security, vol. 19, pp. 4741-4751, 2024, doi:10.1109/TIFS.2024.3372771.

16. A. Raza, K. Munir, M. S. Almutairi and R. Sehar, Novel Class Probability Features forOptimizing Network Attack Detection With Machine Learning in IEEE Access, vol.11, pp. 98685-98694, 2023, doi: 10.1109/ACCESS.2023.3313596.

17. F. Castaño, E. F. Fernañdez, R. Alaiz-Rodríguez and E. Alegre, PhiKitA: Phishing KitAttacks Dataset for Phishing Websites Identification; in IEEE Access, vol. 11, pp.40779-40789, 2023, doi: 10.1109/ACCESS.2023.3268027.

18. M. Shafi, R. K. Jha and S. Jain, &quot;Behavioral Model for Live Detection of Apps BasedAttack; in IEEE Transactions on Computational Social Systems, vol. 10, no. 3, pp. 934-946, June 2023, doi: 10.1109/TCSS.2022.3166145.

19. S. Chen, L. Fan, C. Chen, M. Xue, Y. Liu and L. Xu, GUI-SquattingAttack:Automated Generation of Android Phishing Apps in IEEE TransactionsonDependable and Secure Computing, vol. 18, no. 6, pp. 2551-2568, 1 Nov.- Dec. 2021,doi: 10.1109/TDSC.2019.2956035.

20. G. Apruzzese and V. S. Subrahmanian, Mitigating Adversarial Gray-Box AttacksAgainst Phishing Detectorsin IEEE Transactions on Dependable and SecureComputing, vol. 20, no. 5, pp. 3753-3769, 1 Sept.-Oct. 2023, doi:10.1109/TDSC.2022.3210029.

21. S. Asiri, Y. Xiao, S. Alzahrani, S. Li and T. Li; A Survey of Intelligent DetectionDesigns of HTML URL Phishing Attacks; in IEEE Access, vol. 11, pp. 6421-6443,2023, doi: 10.1109/ACCESS.2023.3237798.

22. S. Al-Ahmadi, A. Alotaibi and O. Alsaleh, PDGAN: Phishing Detection WithGenerative Adversarial Networksin IEEE Access, vol. 10, pp. 42459- 42468, 2022,doi: 10.1109/ACCESS.2022.3168235.

23. F. S. Alsubaei, A. A. Almazroi and N. Ayub, Enhancing Phishing Detection: A NovelHybrid Deep Learning Framework for Cybercrime24. Forensics; in IEEE Access, vol. 12, pp. 8373-8389, 2024, doi:10.1109/ACCESS.2024.3351946.

24. Z. Azam, M. M. Islam and M. N. Huda, Comparative Analysis of Intrusion DetectionSystems and Machine Learning-Based Model Analysis Through Decision Tree; in IEEEAccess, vol. 11, pp. 80348-80391, 2023, doi: 10.1109/ACCESS.2023.3296444.

25. A. Karim, S. Azam, B. Shanmugam, K. Kannoorpatti and M. Alazab, A Comprehensive Survey for Intelligent Spam Email Detection in IEEE Access, vol. 7,pp. 168261-168295, 2019, doi: 10.1109/ACCESS.2019.2954791.

26. S. Remya, M. J. Pillai, K. K. Nair, S. Rama Subbareddy and Y. Y. Cho, An EffectiveDetection Approach for Phishing URL Using ResMLP in IEEE Access, vol. 12, pp.79367-79382, 2024, doi: 10.1109/ACCESS.2024.3409049.

27. Silva, J. D., Gupta, A., &amp; Alvarado, R. G. (2024). Phishing detection using deeplearning: A review of recent approaches and future directions. Journal of Cybersecurityand Privacy, 2024. Vol:8 pp:52-168

28. Patel, M. S., Mehra, R., &amp; Gupta, P. K. (2024). A survey on phishing websites detectiontechniques using artificial intelligence. International Journal of Computer Applications, 2024.

29 Williams, A. F., &amp; Kumar, L. P. (2024). Phishing and social engineering attack mitigation using behaviour analytics and AI. IEEE Transactions on Information Forensics and Security, 2024.

30. Lee, D. M., Cho, K. S., &amp; Park, Y. B. (2024). Evolving phishing attack detection with reinforcement learning. Computers &amp; Security, 2024.

31. Elhassan, F. A., Ali, M. Z., &amp; Lee, D. S. (2024). Real-time phishing detection: Challenges and solutions using block chain technology. Security and Privacy in DigitalWorld, 2024.