A Two-Stage Hybrid Approach for Phishing Attack Detection Using URL and Content Analysis in IoT

Sahar Yousif Mohammed[1], *Mohammad* Aljanabi[2], *Maad* M. Mijwil[3], *Ali* J. Ramadhan[4*], *Mostafa* Abotaleb[5], *Hussein* Alkattan[5] and *Zainalabideen* Albadran[4]

[1]University of Anbar, Al Anbar, Iraq

[2]Al-Iraqia University, Baghdad, Iraq

[3]Baghdad College of Economic Sciences University, Baghdad, Iraq

[4]University of Alkafeel, Najaf, Iraq

[5]South Ural State University, Chelyabinsk, Russia

Abstract. The goal of phishing assaults is to trick users into giving up personal information by making them believe they need to act quickly on critical information. The creation of efficient solutions, such as phishing attack detection systems backed by AI, is essential for the safety of users. This research suggests a two-stage hybrid strategy that uses both URL and content analysis to identify phishing assaults. In the first step of the suggested method, URL analysis is used to determine the legitimacy of suspected phishing assaults. If the site is still live, the second check uses content analysis to determine how serious the attack is. Both analysis' findings are taken into account in the decision-making procedure. As can be seen from the experiments, the hybrid systemobtains an astounding 99.06% accuracy rate. This research adds to the existing body of knowledge by providing a massive dataset of over 14 million data samples that includes both legal and phishingURLs. Furthermore, when content analysis is required for phishing URL detection, the two-stage hybrid technique significantly outperforms URL analysis alone by 70.23 %. The proposed methodprovides better defense against phishing attempts and is practical enough for widespread use.

1 Introduction

The number of people actively using the internet has grown substantially along with the proliferation oftechnological devices. There were only around 3,000 computers in use by businesses in the 1950s, but by the 1970s that number had risen to 80,000 [1]. As computer hardware improved, the number of people using them forboth work and play grew.

* Corresponding author: ali.j.r@alkafeel.edu.iq

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

The number of PCs in use around the globe went from roughly 300,000 in 1975 to around 4 million by 1980 [2]. From 116 million in 1990, the figure jumped to 530 million by the year 2000, and then to about 1.5 billion by 2010 [3]. As of this year, Statista estimates that more than 1.3 billion computers were in use worldwide [4]. By the end of 2022, that figure is expected to rise to more than 2 billion. More people are now online thanks to the proliferation of mobile phones, tablets, laptops, and other gadgets connected to the Internet of Things (IoT). By 2022's close, there should be almost 5.6 billion people using the internet [5].Many facets of our life, from professional endeavors to leisure pursuits, have benefited from the widespread use of computing and the internet. Positive effects have been seen in many fields thanks to the convenience and speed with which activities and transactions may be completed, including business, healthcare, education, communication, finance, aviation, research and engineering, entertainment, and public services. As more and more of our routines are moved online, new jargon has had to be coined to describe them. Any effort to infiltrate the information systems of specific persons or organizations within the virtual environment inhabited by internetusers is known as a cyber-attack [6]. Cybersecurity refers to the practices that are used to prevent, detect, and respond to cyber threats [7].

A cyber-attack is any malicious attempt to disrupt a computer system, steal information from it, or exploit a compromised system to launch additional attacks on other networks [6]. The perpetrators of cyber assaults may be broken down into four categories: cybercriminals, hackers, benign (white hat) attackers, and hacktivists [8]. The malicious actors among them seek to obtain unauthorized access to the targeted computer in order to do directdamage to it or the data it contains. IBM estimates that $4.91 million [9] was lost due to phishing assaults in theirreport on data breaches from 2022. And according to the Anti-Phishing Working Group's (APWG) report for 2022, there were 1,097,811 phishing assaults recorded in Q2 alone [10]. According to APWG, this is the greatestquarterly total on record. An additional 312,000 phishing websites were identified annually (from the third quarterof 2021 to the end of the second quarter of 2022) in the same research, depending on the date of release. Becauseof their low barrier to entry and wide potential audience, phishing assaults may have a major impact. The averagenumber of new phishing websites each month is shown in Figure 1.1, which shows a linear growth in phishing assaults over the past few years. Figure 1: [11] as depicted in the figure1 of the most common kind of cyberattackin recent years, phishing attacks leverage victims' trust in online interactions to steal their personal information, such as passwords and bank details. Figure 1.1, taken from the data periodically released by APWG [12], revealsan alarmingly high rate of new phishing websites being developed, notably in the last two years. Humans are oftenput in the role of the target entity, which contributes to the high quantity. This is due to the fact that human beingsare the easiest target for phishing scams. This method of attack has been in use since the early 2000s, although ithas been countered using a variety of strategies and software. However, the system's vulnerability to such attacksis weakened by the inclusion of humans. Losses can be reduced by the development of a system that reduces reliance on the human element in the face of ever-evolving phishing attempts. Many papers have been done basedon this fact.

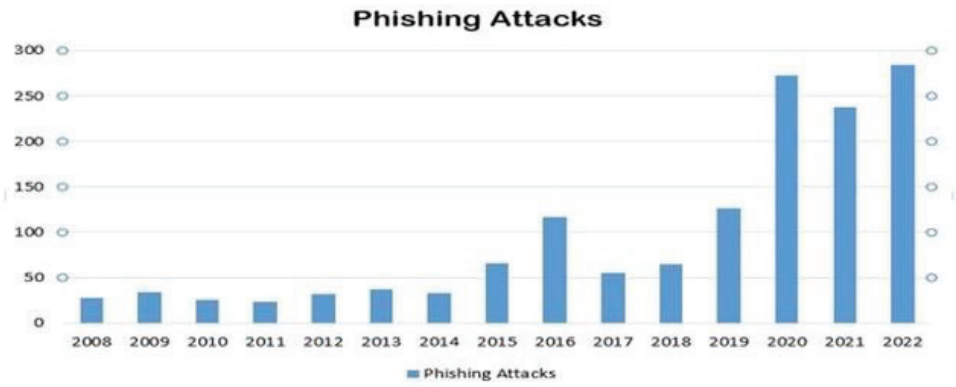

Fig. 1. Average Number of Unique Phishing Attacks Per Year [11].

2 Related Work

Users are frequently lured into malicious websites and emails in phishing attempts, which represent a serious risk to online security. Many research have suggested various strategies for identifying phishing attempts. The purpose of this literature review is to synthesize and assess these methods, drawing attention to their strengths, weaknesses, opportunities, and threats. According to Adebowale et al. (2019) [12].

Integrated aspects of pictures,frames, and text into an intelligent web-phishing detection and security strategy were presented. With this method,we were able to examine phishing campaigns in depth. Nonetheless, the study did not deal with potential difficulties and restrictions connected to the suggested methodology, such as identifying modern phishing methods[13].

Eman &etal (2023) this study introduces a deep learning-based phishing detection method for current URLsecurity. The study shows that a Convolutional Neural Network (CNN) model can detect phishing and suggests additional research. The results suggest that this system may greatly improve phishing detection and provide a great internet alternative. For some businesses, the proposed method may demand a lot of computer power. Finally, the study only detects URL-based phishing assaults, not email or social engineering ones. [14].

Kocyigitet al. (2021) employed machine learning methods to detect cyber threats in real time based on content. The research successfully accomplished the task of analyzing web page content and identifying many risks. The machine learning algorithms were not described in full. [15] An efficient method for detecting phishing websitesbased on URL and HTML attributes was proposed by Aljofey et al. (2022). The method offered a more complete evaluation since it took both URL and HTML features into account. Limitations and difficulties of the detection method were not discussed [16].

Mohammed M. Alani(2023).The study describes a two-stage machine learning method for smart grid cyber threat detection and categorization. The first step efficiently and accurately detects attacks, while the second stage analyzes data to determine attack class. The suggested system performed well onthe DNP3 intrusion detection dataset with an F1 score of 0.9976 at detection and 0.9883 at attack typeclassification. The DNP3 intrusion detection dataset, which may be limited, is used to evaluate the system's performance [17]. Njoku et al. (2023) introduced a combined method for phishing detection that included both URL and content analysis. This method's accuracy was boosted by integrating characteristics gleaned from URLsand page content. However, it's possible that this approach falls short because it relies too much on a small subsetof possible phishing attack patterns or attributes. [18]. A Novel Two-Stage Deep Learning Model for Network Intrusion Detection, was proposed by

Hnamte at el (2023). This study suggested a unique two-stage deep learningapproach for attack detection that combines Long-Short Term Memory (LSTM) and Auto-Encoders (AE). For thepurpose of optimizing the proposed LSTM-AE, we employ the CICIDS2017 and CSE-CICDIS2018 datasets. Theexperimental findings validate the effectiveness and viability of the proposed hybrid model in identifying assaultsin real-world settings. [19].

3 Background

3.1 Phishing Attack

Cybercriminals that engage in phishing attempts pose as legitimate businesses in order to trick users into handing over sensitive information. Attackers want to gather personal information for illicit activities, making confidence in the message and communication channel important. As the effect of phishing assaults grows, it iscrucial for people and businesses to implement preventative measures. Finance, email services, cloud platforms, payment services, and cloud-based software services are some of the most common phishing targets, per the APWG's Phishing Activity Trends Report [20].

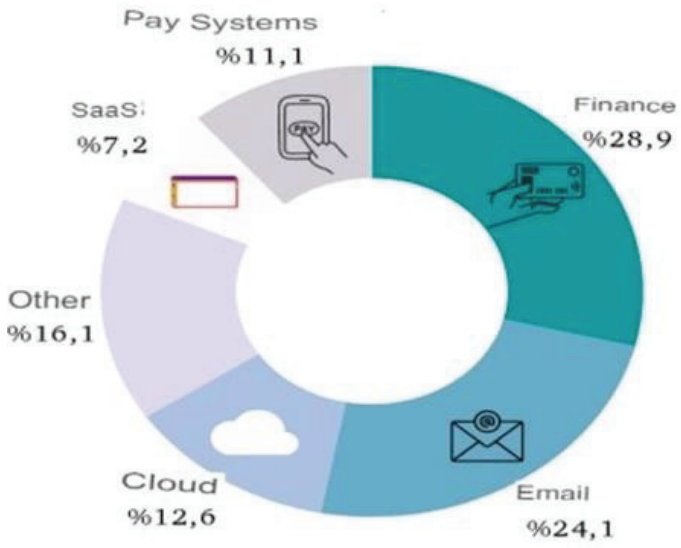

Fig.2. Phishing Attack Targeted Sectors [21].

3.2 Approaches for Phishing Attack Detection

Software like phishing detection systems can help keep private data safe by limiting access to malicious websites that try to steal it. In order to identify prospective attacks, these systems examine the URL or text content of malicious websites. They work as either standalone programs or browser add-ons,and their primary goal is to identify phishing attempts as fast and correctly as possible. There have been studies using URL-based methods, content-based methods, and combined URL and content-based methods. The target is rapid and accurate detection of phishing attempts [22].

3.3 URL-Based Approaches

Features of URL-based phishing detection systems are discussed here. Protocol, server name, and resource identifier are only a few of the elements that make up a URL. Despite their significance for building trust, server names and subdomains may be used in brand impersonation attacks. URL characteristics, such as the server name or the complete URL text, are extracted using machine learning methods. It's critical to be able to notice things quickly, and studying only the URL can help with that. While domain names may be the primary target of certain OSTS programs, subdomain assaults and self- page construction necessitate looking at the full URL [23].

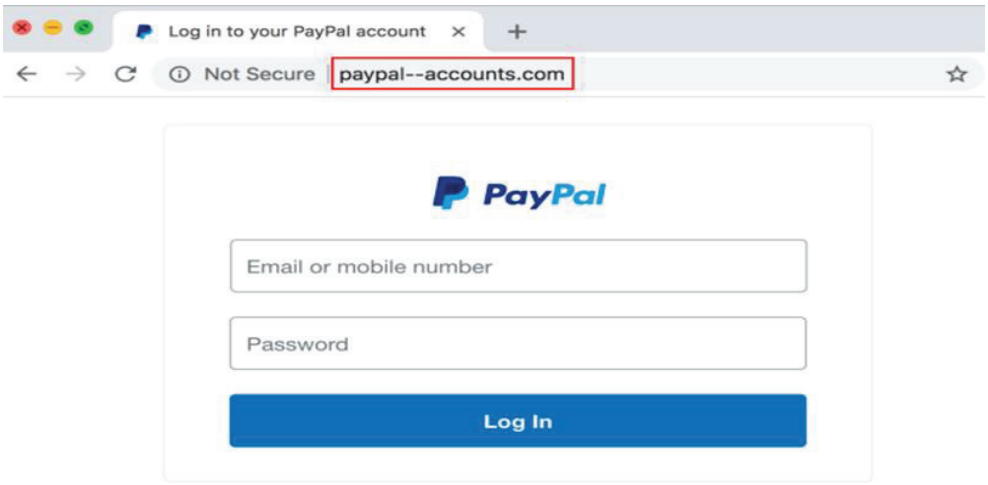

Fig. 3. Advantages of Example of Character Substitution in Domain Name [24].

Features taken from URLs and features generated from third-party services are both included in previous studies as being employed in machine learning based OSTS. For the purposes of deep learning, URLs are interpreted as sentences, and features are then automatically determined. This section emphasizes the value of prompt detection and investigates the many characteristics and approaches used by anti-phishing systems that are URL-based [25].

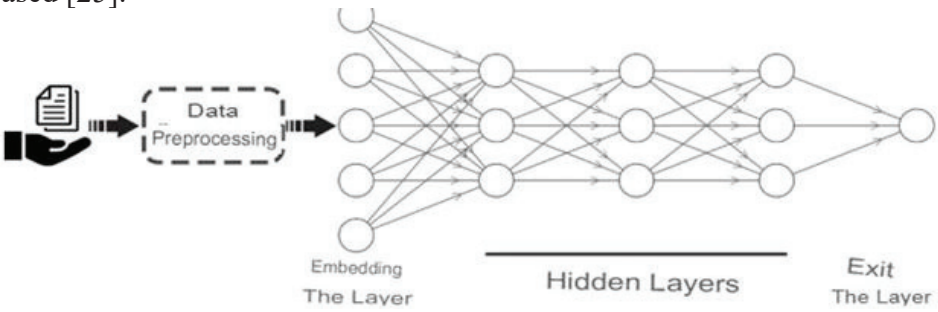

Fig. 4. Advantages of Basic Deep Learning Architecture for Text Processing [25].

3.4 Content-Based Approaches

Phishing detection systems are content based. The study covers email and online content. Because email contains substantial phrases, word-based algorithms are used to evaluate it. Phishing URLs are phishing detection systems are content based. The study covers email and online content. Because email contains substantial phrases, word-based algorithms are used to evaluate it. Phishing URLs are analyzed using Bag of Words, TF-IDF, and word vectors. Website content is evaluated using HTML, CSS, computer languages, graphics, and text. HTML governs a website's look, whereas CSS controls its layout [26]. Programming languages like JavaScript promote user interaction. The designs of phishing websites often resemble real ones. Document Object Model (DOM) background codes can identify fraudulent

redirection. Deep learning and machine learning evaluate text and pictures. Deep learning automates feature extractionwith word-based analysis. Effective phishing detection systems use content analysis. HTML, CSS, and programming language codes can identify qualities [27].

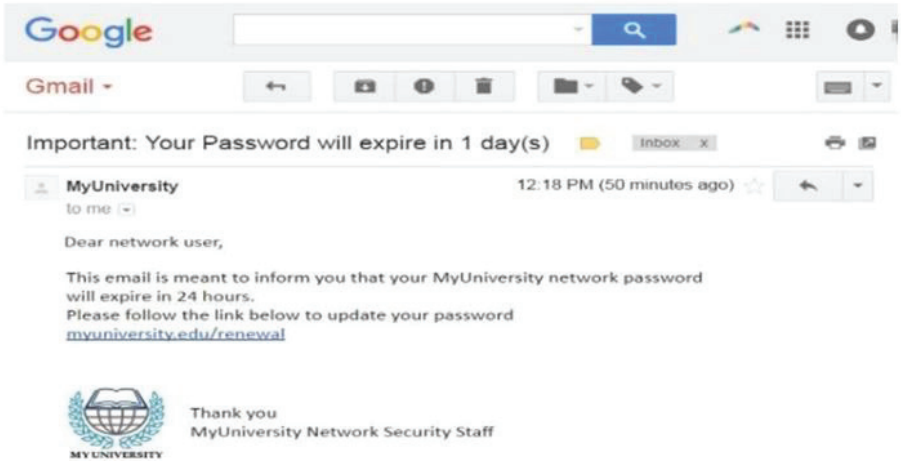

Fig. 5. Phishing Attack Email Text [29].

Statistics are needed for these materials. Like URL content, tag diversity, quantity, and size matter.The framework may also examine the DOM-derived site. Manually Extracted features were found in a prior exam. Phishing attempts can be detected using this method; however, data collection and analysis require time. The detection findings are delayed [28].

3.5 URL and Content Based Approaches

The research highlights the inherent trade-off that exists between the speed and comprehensivenessof phishing detection. Systems that rely on URL analysis demonstrate fast processing capabilities, although their predictive accuracy may be compromised in the absence of website examination. Content analysis- based systems offer a comprehensive approach to examining websites; however they tend to have slower processing speeds. Furthermore, it is worth noting that there may be instances where viewing the content of a website is not feasible. In order to address these issues, scholars have put up the suggestion of integrating URL and content analysis [30]. In general, the aforementioned research provides evidence of the efficacy of integrating URL and content-based methodologies in the detection of phishing attacks. Thisintegration results in the attainment of elevated levels of accuracy, while simultaneously mitigating the constraints associated with each individual technique. This study will adopt a distinct strategy in analyzingthe hybrid structure. A novel approach will be suggested wherein the integration of URL and content attributes is replaced by a distinct framework that handles these two analytical processes as distinct phases.The objective of this study is to provide a novel contribution to the existing body of literature via the implementation of a distinctive strategy.

4 Methodology

In this research, a solution was presented to improve phishing detection systems and safeguard users from one of the most common forms of cyberattack. Attackers use phony websites to "phish" for sensitive information from unsuspecting users.

4.1 Dataset

The approach employs a larger and higher-risk dataset for building a more secure detection system,which improves the efficacy of protective systems. The suggested model makes use of data from a large- scale collection of both genuine and phishing URLs spanning the years 2006-2021. 51,316 genuine URLsand contents are included in the dataset, along with 36,173 phishing URLs and contents. The dataset was compiled by having a script scan PhishTank every 10 minutes for potentially malicious URLs. Any matched URLs had their contents and corresponding IDs appended to the collection. CSV files included the dataset, with a value of 0 for valid entries and a value of 1 for phishing ones. According to the data distribution, the majority of the phishing data in the sample was collected in 2021, suggesting the presence of zero-day assaults.

4.1.1. Dataset Preprocessing and Preparation

The dataset was pre-processed to guarantee its quality and compatibility for the suggested method before analysis. The dataset does not include URLs that have a size of "0 KB." In addition, each URL wasexamined separately, and the data set was cleaned out if any of them returned a "Error 403" message. In addition, during preprocessing, we looked at some basic statistics about the URLs, such how long they were on average and whether or not they followed any regular patterns. These procedures helped provide a clean and trustworthy dataset for further study.

4.1.2. URL-Based Phishing Detection System

In order to facilitate expedited identification, the suggested method places emphasis on the detectionof phishing attacks based on URLs. URLs are subjected to analysis by considering their constituent elements, which encompass the protocol, subdomain, main domain, top-level domain, directory, file name,and parameters. The system utilizes two distinct methodologies for training the detecting system. Initially,a procedure of feature extraction is employed to identify a total of 73 distinct characteristics from the textual content of the URL. Deep learning models, such as Generative Adversarial Networks (GANs) andConvolutional Neural Networks (CNNs), are employed for the purpose of analyzing these aforementioned properties. Figure 6 depicts the utilization of a deep learning model, namely a Generative Adversarial Network (GAN), for the purpose of identifying URL-Phishing. Secondly, the URLs are subjected to analysis.

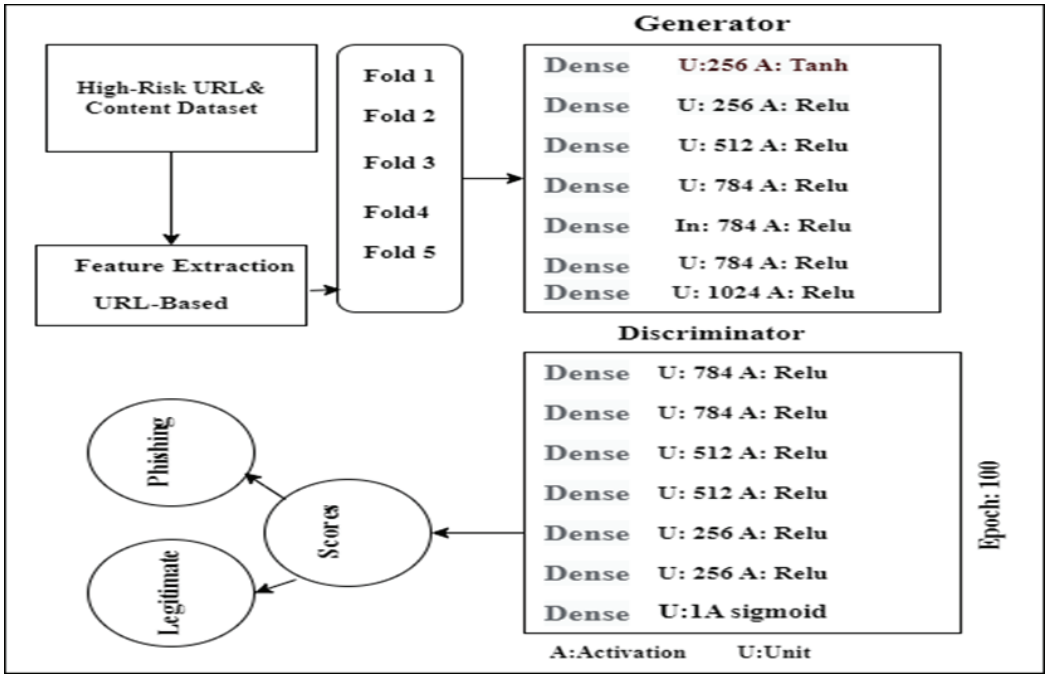

Fig. 6. The workflow of generating URL handcrafted features using a GAN model.

The characteristics of interest were represented using character-based embedding, as seen in Figure 7, which depicts the use of the CNN Model. The present study centers on the detection of URL-based phishingthrough the utilization of several deep learning models in order to construct an ideal architecture. During the pre-processing step, a standardization technique is applied to transform all letters to lowercase, so assuring consistency in the data. Furthermore, Uniform Resource Locators (URLs) are included into text using a pre-established word count. In order to determine the most optimal architecture, the system conducts thorough experimentation on several deep learning models. It is worth mentioning that models such as Generative Adversarial Networks (GANs) and Convolutional Neural Networks (CNNs) demonstrate remarkable performance. To get optimal precision, a synergistic amalgamation of these exemplary models is employed. The system architecture adheres to a two-step methodology. At the outset,distinct detection techniques are employed for each model. This facilitates a thorough assessment of theirstrengths and limitations. In order to improve the efficiency and accuracy of the system, a hybrid model is developed by integrating the Generative Adversarial Network (GAN) model, which leverages 73 features, with the Convolutional Neural Network (CNN) model, which utilizes a single character embedding. By amalgamating the functionalities of these two models, the suggested system optimizes its ability to identifyphishing in the URL-based method. The suggested architecture for URL-based phishing detection is visually depicted in Figure 7, illustrating the collaborative integration of GAN and CNN models.

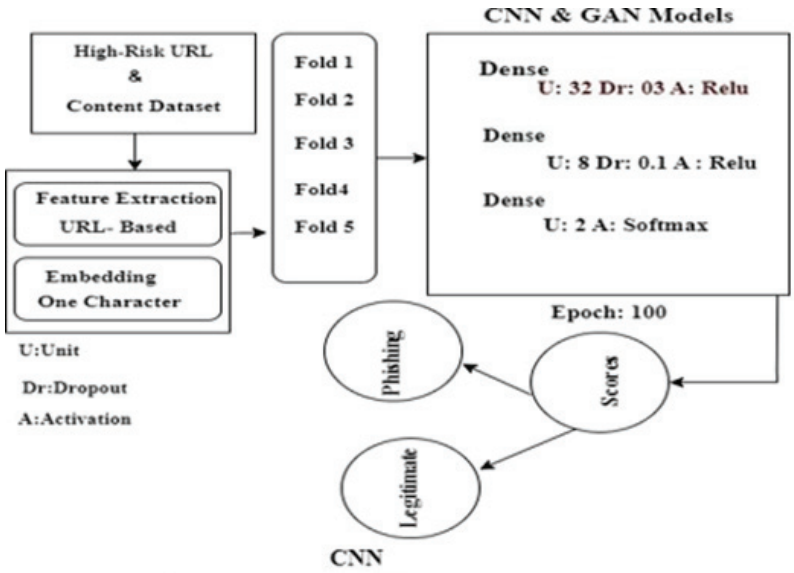

Fig. 7. Workflow of the character-based CNN model on URL.

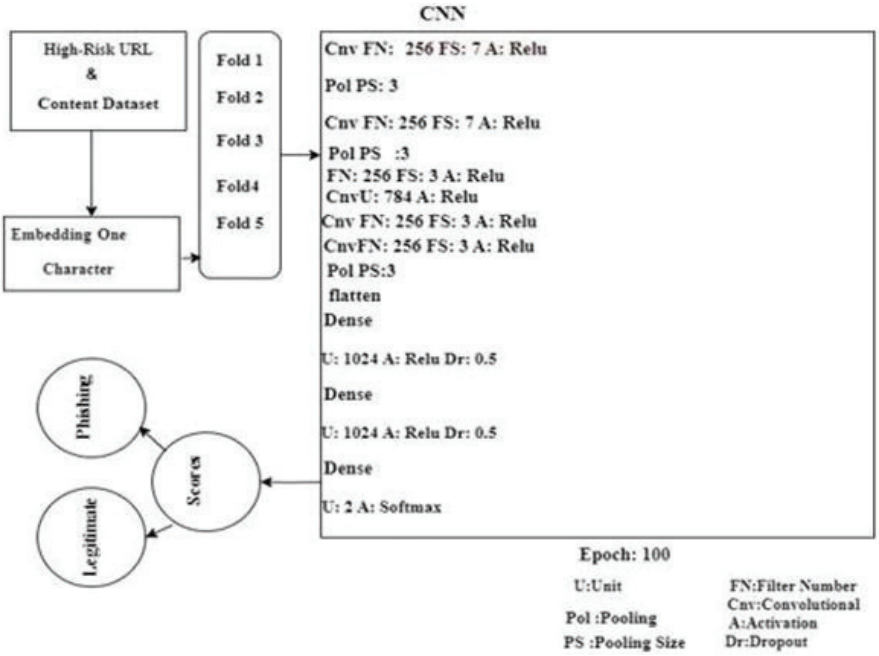

Fig. 8. The process flow of the URL-based model incorporating handcrafted features and single-character embedding.

4.2 Content-Based Phishing Detection System

The suggested system encompasses a content-based phishing detection mechanism that does an analysis of website content, primarily focusing on HTML, CSS, and JavaScript components. A comprehensive set of 57 content-based characteristics are retrieved, encompassing various indications suchas the existence of submit inputs, email inputs, hidden tags, pop-ups, and other relevant elements. Each feature is assigned a binary value of either 1 or 0 to indicate its existence or absence in the material, or thefrequency count of the feature, respectively. The retrieval and pre-processing of the content of each webpage in the dataset are conducted. Subsequently, the designated function for each exemplar isperformed in order to get numerical values. The aforementioned values are employed inside the content- based model, which makes use of machine learning algorithms to identify phishing websites by analyzingtheir content properties.

4.3. Two-Stage URL- And Content-Based Hybrid Phishing Detection System

In order to optimize the effectiveness of the phishing detection system, a two-stage hybrid model has been devised. The initial phase is doing URL-based analysis, wherein an assessment is made on a given URL. If it is identified as a phishing attempt, no further study is pursued. Once the URL has been recognized as authentic, it then progresses to the second step of examination, which is content-based. Whenthe content of a URL is not accessible, the result derived from the URL is regarded as conclusive. However,in the presence of available content, the analysis conducted is dependent on the content itself. The hybrid model integrates the outcomes from both phases through the utilization of an ensemble technique known as UCDeM (URL and Content Detection Model). The classification judgment on the authenticity or phishing nature of a URL is made by UCDeM by the integration of data obtained from both URL-based and content-based analyses. The University of Cyber Defense and Monitoring (UCDeM) employs a methodology that involves the calculation of expected outcomes for each stage, expressed as percentages.These percentages serve as indicators of the probability of a given entity being either legitimate or a phishing attempt. The aforementioned percentages are thereafter allocated in accordance with a threshold value established through the utilization of an ensemble technique. Through the use of this ensemble approach, the University of California, Department of Engineering and Mathematics (UCDeM) is able to provide novel categorization values that yield a heightened level of precision and dependability in evaluating the URL.The UCDeM ensemble technique is of significant importance in the two-stage URL- and content-based hybrid phishing detection system. It facilitates the integration of both studies, resultingin improved detection capabilities and reduced occurrences of false negatives and positives. The classification values obtained from the URL-based and content-based models are combined using a weighted approach, where the weights are determined based on a threshold value. This strategy enhances accuracy by capitalizing on the advantages of both URL-based and content-based detection methods, therefore mitigating false positives and establishing a resilient phishing detection system. The suggested methodology is not restricted just to the identification of phishing attempts, but rather has the potential to be applied to several other areas within the realm of security, including but not limited to virus detection, spam filtering, and fraud detection. By using this complete technique, companies have the ability to strengthen their defenses against phishing attempts and protect the sensitive information of their end-users.

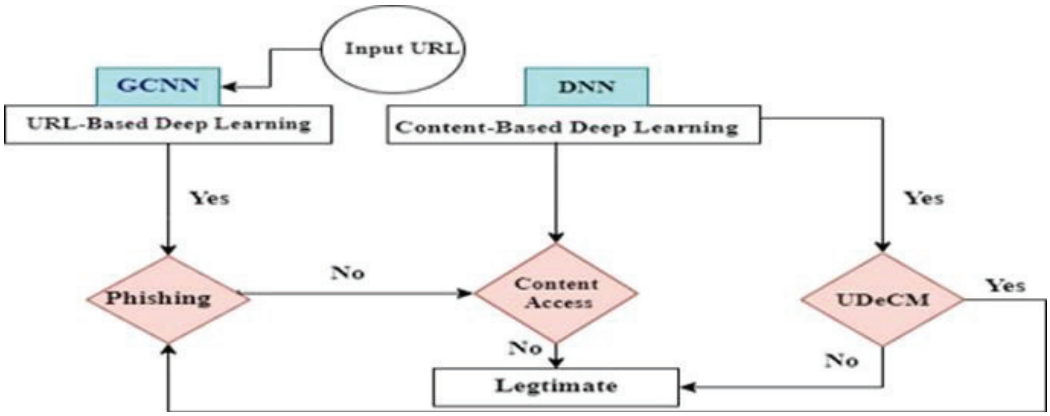

Fig. 9. Design of a Two-Stage Hybrid Phishing Detection System Combining URL and Content Analysis.

5. Experimental Results

In order to assess the efficacy of the presented models, a set of experiments were undertaken. The findings gained are reported in this part, offering valuable insights into the performance and efficiency ofthe models.

5.1 Experimental Outcomes for the URL-Based Phishing Detection System

Both manually-created features and deep learning features were used to test the URL-based phishingdetection model. Five-fold Cross-validation was used to evaluate several machine learning classifiers, suchas Decision Tree, Random Forest, ANN, LSTM, and DNN. Table 1 summarizes the findings. Table 1 displays the results of several machine learning methods, with Random Forest coming out on top with an accuracy of 91.80% and the DNN model coming in at a close second with an accuracy of 94.20%.

Table 1. Handcrafted Feature Machine Learning Classifier Evaluation Results.

Machine Learning Algorithm	Accuracy
Decision Tree	9.50
Random Forest	91.80
ANN	90.75
LSTM	84.31
DNN	94.20
GAN	94.99

In addition, the maximum accuracy (97.18 percentage points) was attained by deep learning models that included single-character embedding and CNN layers (Table 2).

Table 2. Evaluation Results of Deep Learning Models with Single Character Embedding.

Deep Learning Models	Accuracy
GRU	95.01
LSTM	95.80
BiLSTM	95.75
CNN	97.18

The results show that the URL-based approach can successfully identify phishing attempts. Table 3 displays experimental findings for combined models derived from URL analysis.

Table 3. Results of Testing for Merged URL-Based Models

Deep Learning Models	Accuracy
GAN+GRU	94.9
GAN+LSTM	96.13
GAN+BiLSTM	96.52
GAN+CNN	97.70

The results of four combined models (GAN + GRU, GAN + LSTM, GAN + BiLSTM, and GAN + CNN)are summarized in the table below. When compared to the individual models, all combined models, with the exception of the GAN + GRU model, perform somewhat better. Notably, the GAN + CNN model scored a 97.70% accuracy, which is the greatest of all of the models tested. These findings inform the proposal of a hybrid method for first phishing assault detection. The GCNN model, which is used in this method, has an impressive accuracy of 97.70%.

5.2 Experimental Outcomes for the Content-Based Phishing Detection System

Several deep learning models were used in the content-based phishing detection algorithm. Based on experimental results (Table 4), the DNN model showed an accuracy of 93.40 percent. The content-based model's performance was lower than that of the URL-based model, but it was nevertheless able to identifyseveral phishing websites that the latter had missed. When it came to identifying phishing attempts, both the content-based model and the URL-based one were useful.

Table 4. Results of deep learning models were used in the content-based phishing detection algorithm

Deep Learning Models	Accuracy
LSTM	87.9
GAN	92.80
DNN	94.40

5.3 Experimental Outcomes for Two-Stage URL- And Content-Based Hybrid Phishing Detection System

An accuracy of 98.50% (Table 5) was attained by the proposed TshPhish model, which uses the UCDeM ensemble model to integrate URL-based and content-based techniques in a two-stage hybrid phishing detection system. Table 5 shows that the URL-based model outperforms the content-based modelby around 0.69 percentage points and the TshPhish model by about 4.98 percentage points in terms of accuracy. When a valid URL is incorrectly detected as a phishing assault (False Positive), it is the worst case scenario for phishing attack detection systems. Therefore, the FPR in the confusion matrix is a significant statistic to think about. By decreasing the FPR from 0.0164 to 0.0112, the TshPhish model has demonstrated a considerable increase in the system's capacity to accurately detect genuine URLs by 30%.Furthermore, the error rate is reduced by almost 49% in the suggested model, indicating increased accuracy and dependability. Our study also reviews the work of other researchers who have used content-and URL-based methods to detect phishing attacks. In Table 6 of our study, we contrast the findings of these investigations with our method. Our research is distinctive in a number of respects, including datasetsize, quantity of phishing data, data source, and the use of deep learning algorithms. Notably, our dataset includes potentially dangerous URLs, as even trustworthy URLs have been flagged as suspicious by PhishTank users. So, this research helps by producing a real-world dataset and getting a 98.50% detection rate.

Table 5. Results of Testing for Proposed Model, and TshPhish

Content-Based Models	**URL-Based Models**			
	GAN + GRU	GAN + LSTM	GAN+BiLSTM	GAN+CNN
DNN	96.74	97.60	97.14	98.50
GAN	96.62	97.47	97.70	98.10

6. Conclusions

This work presents a novel hybrid phishing detection system that integrates both URL-based and content-based methodologies. The algorithm demonstrates a notable level of accuracy, reaching 98.37%, when applied to a dataset of websites that are deemed questionable. The efficacy of deep learning-based URL analysis models, suchas Long Short-Term Memory (LSTM), Generative Adversarial Networks (GAN), and Deep Neural Networks (DNN), in the detection of phishing URLs is notable. Content-based models, such as Generative Adversarial Networks (GAN) and Deep Neural Networks (DNN), function as an additional

detection mechanism, hence enhancing the overall accuracy. The solution under consideration aims to mitigate the problem of phishing assaults, which specifically exploit end-users in order to get sensitive information. The utilization of bigger and high-risk datasets contributes to the enhancement of the system's security. The results indicate possible applicability in several other sectors related to security. The paper makes a valuable contribution to the field of cybersecurity by presenting a sophisticated approach to the identification of phishing attacks.

References

1. M. Korkmaz, E. Kocyigit, O. K. Sahingoz, and B. Diri, "A Hybrid Phishing Detection System Using Deep Learning-based URL and Content Analysis," Elektronika Ir Elektrotechnika, vol.**28**, no.5, pp.80-89, Oct 2022. doi:10.5755/j02.eie.31197
2. A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," Telecommunication Systems, vol. **76**, pp.139–154, Oct 2020. doi:10.1007/s11235-020-00733-2
3. A. Zamir, H. U. Khan, T. Iqbal, N. Yousaf, F. Aslam, A. Anjum, and M. Hamdani, "Phishing web site detection using diverse machine learning algorithms, " The Electronic Library, vol. 38, no. **1**, pp. 65-80, Jan 2020. doi:10.1108/EL-05-2019-0118
4. Kocyigit E., M. Korkmaz, O. K. Sahingoz, and B. Diri, "Real-Time Content-Based Cyber Threat Detection with Machine Learning," In Intelligent Systems Design and Applications, vol.**1351**, pp.1394–1403, Jun 2021. doi:10.1007/978-3-030-71187-0_129
5. K. S. Ray and R. Kusshwaha, "Detection of Malicious URLs Using Deep Learning Approach," In The "Essence" of Network Security: An End-to-End Panorama, vol.**163**, pp.189–212, Nov 2020. doi:10.1007/978-981-15-9317-8_8
6. S. Sountharrajan, M. Nivashini, S. K. Shandilya, E. Suganya, A. B. Banu, and M. Karthiga, "Dynamic Recognition of Phishing URLs Using Deep Learning Techniques," In Advances in Cyber Security Analytics and Decision Systems, pp.27–56, Jan 2020. doi:10.1007/978-3-030-19353-9_3
7. S. Selvaganapathy, M. Nivaashini, and H. Natarajan, "Deep belief network based detection and categorization of malicious URLs," Information Security Journal: A Global Perspective, vol.**27**, no.3, pp.145-161, Apr 2018. doi:10.1080/19393555.2018.1456577
8. W. Yang, W. Zuo, and B. Cui, "Detecting Malicious URLs via a Keyword-Based Convolutional Gated-Recurrent-Unit Neural Network," IEEE Access, vol.**7**, pp.29891 - 29900, Jan 2019. doi:10.1109/ACCESS.2019.2895751
9. T. Rasymas and L. Dovydaitis, "Detection of Phishing URLs by Using Deep Learning Approach and Multiple Features Combinations," Baltic Journal of Modern Computing, vol.**8**, no.3, pp.471-483, 2020. doi:10.22364/bjmc.2020.8.3.06
10. B. Wei, R. A. Hamad, L. Yang, X. He, H. Wang, B. Gao, and W. L. Woo, "A Deep-Learning-Driven Light-Weight Phishing Detection Sensor," Sensors, vol.**19**, no.19, pp.4258, Sep 2019. doi:10.3390/s19194258
11. A. Aljofey, Q. Jiang, Q. Qu, M. Huang, and J. Niyigena, "An Effective Phishing Detection Model Based on Character Level Convolutional Neural Network from URL," Electronics, vol.9, no.9, pp.1514, Sep 2020. doi:10.3390/electronics9091514
12. M. A. Adebowale, K. T. Lwin, E. Sánchez, and M. A. Hossain, "Intelligent web-phishing detection and protection scheme using integrated features of Images, frames and text," Expert Systems with Applications, vol.115, pp.300-313, Jan 2019. doi:10.1016/j.eswa.2018.07.067
13. M. S. Kumar and B. Indrani, "Frequent rule reduction for phishing URL classification using fuzzy deep neural network model," Iran Journal of Computer Science, vol.4, pp.85–93, Jul 2020. doi:10.1007/s42044-020-00067-x

14. E. A. Aldakheel, M. Zakariah, G. A. Gashgari, F. A. Almarshad, and A. I. A. Alzahrani, “A Deep Learning-Based Innovative Technique for Phishing Detection in Modern Security with Uniform Resource Locators, ” Sensors, vol.23, no.9, pp. 1-17, Apr 2023. doi:10.3390/s23094403
15. A. Aljofey, Q. Jiang, A. Rasool, H. Chen, W. Liu, Q. Qu, and Y. Wang, “An effective detection approach for phishing websites using URL and HTML features,” Scientific Reports, vol.12, no.8842, pp.1-19, May 2022. doi:10.1038/s41598-022-10841-5
16. H. Kansagara, V. Raval, F. Shaikh, and S. Kudoo, “A Hybrid Approach For Phishing Website Detection Using Machine Learning,” VIVA-Tech International Journal for Research and Innovation, vol.1, no.4, pp.1-6, 2021.
17. M. M. Alani, L. Mauri, and E. Damiani, “A two-stage cyber attack detection and classification system for smart grids,” Internet of Things (Netherlands), vol. 24, 2023, doi: 10.1016/j.iot.2023.100926.
18. T. Makarovskikh, A. Salah, A. Badr, A. Kadi, H. Alkattan and M. Abotaleb, "Automatic classification Infectious disease X-ray images based on Deep learning Algorithms," 2022 VIII International Conference on Information Technology and Nanotechnology (ITNT), Samara, Russian Federation, 2022, pp. 1-6, doi: 10.1109/ITNT55410.2022.9848538.
19. Al-Nuaimi, B. T., Al-Mahdawi, H. K., Albadran, Z., Alkattan, H., Abotaleb, M., & El-kenawy, E. S. M. (2023). Solving of the inverse boundary value problem for the heat conduction equation in two intervals of time. Algorithms, 16(1), 33.
20. E. Mushtaq, A. Zameer, M. Umer, and A. A. Abbasi, “A two-stage intrusion detection system with auto-encoder and LSTMs,” Applied Soft Computing, vol.121, pp.108768, May 2022. doi:10.1016/j.asoc.2022.108768
21.
22. M. Abotaleb, T. Makarovskikh, A. Ali Subhi, H. Alkattan and A. O. Adebayo, "Forecasting and modeling on average rainwater and vapor pressure in Chelyabinsk Russia using deep learning models," 6th Smart Cities Symposium (SCS 2022), Hybrid Conference, Bahrain, 2022, pp. 362-367, doi: 10.1049/icp.2023.0582.
23. M. Mahmoud, M. Kasem, A. Abdallah, and H. S. Kang, “AE-LSTM: Autoencoder with LSTM-Based Intrusion Detection in IoT,” In Proceedings of the International Telecommunication Conference, pp.1-6, Jul 2022. doi:10.1109/ITCEgypt55520.2022.9855688
24. H. C. Altunay and Z. Albayrak, “A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks,” Engineering Science and Technology, an International Journal, vol.38, pp.101322, Feb 2023. doi:10.1016/j.jestch.2022.101322
25. Al-Mahdawi, H. K., Albadran, Z., Alkattan, H., Abotaleb, M., Alakkari, K., & Ramadhan, A. J. (2023, December). Using the inverse Cauchy problem of the Laplace equation for wave propagation to implement a numerical regularization homotopy method. AIP Conference Proceedings (Vol. 2977, No. 1). AIP Publishing.
26. V. Ravi, R. Chaganti, and M. Alazab, “Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system,” Computers and Electrical Engineering, vol.102, pp.108156, Sep 2022. doi:10.1016/j.compeleceng.2022.108156
27. Akbari, E., Mollajafari, M., Al-Khafaji, H. M. R., Alkattan, H., Abotaleb, M., Eslami, M., & Palani, S. (2022). Improved salp swarm optimization algorithm for damping controller design for multimachine power system. IEEE Access, 10, 82910-82922.
28. H. Alkattan, M. Abotaleb, A. Ali Subhi, O. A. Adelaja, A. Kadi and H. K. Ibrahim Al-Mahdawi, "The prediction of students' academic performances with a classification model built using data mining techniques," 6th Smart Cities Symposium (SCS 2022), Hybrid Conference, Bahrain, 2022, pp. 353-356, doi: 10.1049/icp.2023.0577.

29. A. Kim, M. Park, and D. H. Lee, "AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection," IEEE Access, vol.8, pp.70245 - 70261, Apr 2020. doi:10.1109/ACCESS.2020.2986882
30. Ehsan khodadadi, S. K. Towfek, Hussein Alkattan. (2023). Brain Tumor Classification Using Convolutional Neural Network and Feature Extraction. Fusion: Practice and Applications, 13(2), 34-41.
31. T. A. S. Srinivas, and S. S. Manivannan, "Prevention of Hello Flood Attack in IoT using combination of Deep Learning with Improved Rider Optimization Algorithm," Computer Communications, vol.163, pp.162-175, Nov 2020. doi:10.1016/j.comcom.2020.03.03