

Phishing Attack Mitigation: A Review and Multiclass Framework Utilizing Deep Learning Techniques

Abdullahi Raji Egigogo¹, Idris Ismaila², Morufu Olalere³ Abisoye Opeyemi Aderiike⁴ Ojeniyi Joseph Adebayo⁵, Idowu Afe⁶
{abdullahirajiegigogo@gmail.com¹, ismi.idris@futmina.edu.ng²,
lerejide@futmina.edu.ng³, abisoye@futmina.edu.ng, ojeniyija@futmina.edu.ng⁴
and Afeidowu@gmail.com⁶}

Federal University of Technology Minna¹²³⁴⁵⁶

Abstract

Recently, phishing attacks have become one of the significant cybersecurity threats, exploiting deception and human vulnerabilities to access sensitive information. This study evaluates existing phishing detection frameworks, emphasizing traditional machine learning and advanced deep learning approaches while identifying significant shortcomings in multiclass categorization and adaptation to evolving threats. To overcome these, we offer a new framework that fuses CNN and BiGRU. This hybrid approach combines local pattern recognition with long-range dependency analysis to boost detection accuracy across several attack types, including email phishing, smishing, and URL-based attacks. By incorporating robust preprocessing, feature engineering, and scalable architecture, the framework advances phishing detection capabilities, offering a comprehensive solution to counter sophisticated cyberattacks and serving as a foundation for future research in adaptive cybersecurity strategies.

Keywords: Deep Learning, Phishing Attack, CNN, BiGRU

I. Introduction

Online transactions have risks and benefits, with phishing attacks representing a significant threat by exploiting human vulnerabilities such as trust and urgency. These assaults, frequently disguised as authentic correspondence from credible entities, may lead to severe repercussions such as financial loss, identity theft, and data breaches. Phishing leverages human weaknesses, including trust and urgency, to entice victims into performing hazardous acts. These assaults are typically camouflaged as trustworthy messages from trusted sources, such as banks, government organizations, or well-known corporations, which makes them difficult for consumers to detect as fake. The repercussions of falling victim to phishing may be severe, ranging from financial loss and identity theft to large-scale data breaches compromising essential corporate and personal information (Yeung et al., (2023; Damaševičius et al., 2020).

The rising popularity and sophistication of phishing efforts have underscored the demand for effective and adaptive detection mechanisms. Customarily, phishing detection systems generally employ rule-based approaches based on heuristic analysis. These resolutions frequently utilized well-known patterns or signatures to detect recognized phishing attempts. For instance, rule-based systems could ascertain emails or web pages with specific keywords or questionable URLs. Heuristic analysis gave protection by examining elements such as the URL's structure, the sender's email address, and the message's tone. These systems were capable of identifying suspicious signals but struggled to respond to new and developing phishing attempts. The static nature of these classic detection approaches meant they often failed to identify sophisticated phishing attempts that evaded well-known restrictions. As phishing strategies have gotten more complex,

the requirement for dynamic, context-aware detection systems has become even more critical. This difficulty has prompted the investigation of more advanced approaches, notably those based on machine learning and deep learning.

As phishing attacks continue to grow, there is a compelling need for systems that can detect known phishing efforts and adapt to new attack techniques. Machine learning (ML) and deep learning (DL) models have emerged as viable tools for phishing detection. These algorithms may learn from enormous databases of phishing and actual incidents, detecting subtle trends and connections that older systems might ignore. This study attempts to analyze phishing detection strategies, showing the progression of detection methods from rule-based systems to more advanced machine learning and deep learning approaches. Additionally, this study offers a deep learning-based multiclass framework for phishing detection, which will increase detection accuracy, flexibility, and scalability.

II. Review of Related Works

The existing literature on phishing detection reveals diverse machine learning and deep learning frameworks, each offering unique methodologies to address this pervasive threat. Current approaches, ranging from cognitive frameworks and feature-based models to multi-layered detection systems and real-time browser extensions, have significantly enhanced phishing detection as (Alsharaiah et al., 2023) proposed a novel framework integrating random forest classifiers with k-means clustering (RM-KmC) to improve feature correlation detection. Tested on a 5,000-sample dataset, the model achieved an accuracy of 98.64% with solid precision and recall metrics.

Subba (2023) developed a security framework utilizing a diverse stacking ensemble approach, incorporating three base classifiers and a meta-classifier. The model processes 44 extracted features from URLs and web pages, combining the results for the final prediction. The framework demonstrated high accuracy (99% for binary, 98% for multi-class) on benchmark datasets. Tenis & Santhosh (2023) presented a real-time phishing detection system using a deep learning approach, including white listing and black listing mechanisms. The adaptive RNN (a-RNN) model showed a superior accuracy of 99.18% across different datasets.

Tang & Mahmoud (2022) developed a deep learning-based framework that combines white list filtering, black list interception, and machine learning prediction through a browser plug-in. Their RNN-GRU model achieves an accuracy of 99.18%, showcasing the effectiveness of integrating multiple detection strategies in real-time environments.

Liu et al. (2021) introduce a multistage phishing detection model based on the CASE feature framework, designed for high efficiency and performance with low false alarm rates. Their extensive validation, including real-world experiments, underscores the practical applicability of comprehensive feature frameworks in phishing detection.

Kumar & Subba (2021) present a lightweight machine learning-based security framework that analyzes URLs and extracts discriminating features for phishing detection. Their approach demonstrates high precision and low false positive rates, highlighting the role of feature extraction in enhancing detection performance.

Sadique et al. (2020) present an automated framework for real-time detection of phishing URLs, achieving 87% accuracy. Their work addresses challenges in real-time detection through incremental learning and selective sampling, proposing solutions to improve accuracy and adaptability.

Saravanan & Subramanian (2020) proposed a framework that enhances phishing website detection by extracting features from phishing and legitimate sites. Their framework integrates a feature

selection module to refine the feature set and a detection module for classification. Experimental results demonstrate that this approach outperforms existing classifiers, highlighting the effectiveness of feature-based detection in phishing scenarios.

Rendall et al. (2020) propose a multi-layered detection framework that involves classifying potential phishing domains multiple times using different feature sets. Their two-layered detection system, evaluated with active phishing attack datasets, demonstrates performance comparable to state-of-the-art methods, emphasizing the efficacy of multi-layered approaches.

Hr et al. (2020) introduce a novel browser-based anti-phishing system called the Embedded Phishing Detection Browser (EPDB). This system uses a rule-of-extraction framework and a Random Forest Classification model, achieving real-time detection with an accuracy of 99.36%, highlighting advancements in browser integration and rule-based extraction methods.

Zeng et al. (2020) present PhishBench 2.0, a benchmarking framework for phishing detection systems that supports the dynamic evaluation of features, classifiers, and metrics. This framework facilitates comprehensive assessments of detection methods across various datasets, promoting continued advancements in phishing detection research.

Cuzzocrea et al. (2019) present a machine learning framework employing decision tree algorithms to analyze web phishing attacks. Their experimental evaluation confirms the effectiveness of decision trees in phishing detection, reinforcing the role of algorithmic approaches in threat analysis.

Rao & Pais (2019) introduce a feature-based machine learning framework that utilizes heuristic features extracted from URLs, source code, and third-party services. Their model, evaluated with various machine learning algorithms, demonstrates superior performance with the Random Forest algorithm, achieving an accuracy of 99.31%, emphasizing the importance of heuristic features and external data sources.

Elnagar & Thomas (2019) Elnagar et al. (2019) propose a cognitive framework leveraging a bidirectional long-short-term memory recurrent neural network (BLSTM-RNN) and a convolutional neural network (CNN), incorporating image recognition to enhance phishing detection capabilities. This approach integrates advanced neural network architectures and image processing to address emerging phishing techniques.

Niakanlahiji et al. (2018) developed PhishMon, a machine learning-based framework utilizing present PhishMon, a machine-learning framework utilizing fifteen novel features to detect phishing web pages. With an accuracy of 95.4% and a 1.3% false positive rate, PhishMon demonstrates the importance of diverse feature sets in improving detection precision.

Yi et al. (2018) focus on a deep learning framework using Deep Belief Networks (DBN), incorporating original and interaction features for phishing detection. Their model achieves a true positive rate of approximately 90% with a 0.6% false positive rate, demonstrating the potential of deep learning in capturing complex phishing characteristics.

Park et al. (2017) propose the Phishing-Detective framework, which utilizes web scraping and data mining techniques to detect phishing websites. This framework offers a dynamic and accurate approach by analyzing heuristics and their contribution to phishing detection. The diverse frameworks and methodologies presented highlight the ongoing evolution in phishing detection, revealing critical areas for further development. The need for more sophisticated, multiclass approaches that integrate various detection techniques and leverage deep learning is evident, paving the way for future research and advancements in combating phishing threats. Table 1 shows an overview of Phishing Detection Frameworks.

Table 1: Overview of Phishing Detection Frameworks

Study	Framework/Model	Key Features	Accuracy/Performance	Key Insights	Research Gaps/Limitations
Alsharaiah et al. (2023)	Machine learning	RM-KmC	98.64%	A novel framework integrating random forest classifiers with k-means clustering	Improvement in the performance
Subba (2023)	Deep learning	Heterogeneous stacking ensemble; 3 base classifiers, 1 meta-classifier	99% for binary, 98% for multi-class	A security framework utilizing a diverse stacking ensemble approach	Improvement needed in the multi-class prediction
Tenis & Santhosh (2023)	Deep learning	Deep learning approach, including whitelisting and blacklisting mechanisms.	99.18%	Adaptive Recurrent Neural Networks (a-RNN)	Improvement in the performance
Tang and Mahmoud (2022)	RNN-GRU with whitelist and blacklist filtering	Combines machine learning and real-time browser plug-in	99.18% accuracy	Effective integration of multiple detection strategies.	Limited scope on non-browser-based phishing attacks.
Liu et al. (2021)	CASE feature framework	Multistage detection with real-world validation	High efficiency and low false alarms	Demonstrates practical applicability of comprehensive features.	Performance may vary with evolving phishing tactics.
Kumar and Subba (2021)	Lightweight machine learning	URL analysis and feature extraction	High precision, low false positives	Emphasizes the role of feature extraction.	Struggle with sophisticated phishing techniques.
Sadique et al. (2020)	Automated real-time detection framework	Incremental learning and selective sampling	87% accuracy	Addresses real-time detection challenges.	Real-time adaptability in dynamic environments is limited.
Saravanan & Subramanian (2020)	Feature extraction and classification module	Integrated feature selection and detection	Outperforms existing classifiers	Highlights effectiveness of feature-based detection.	Feature selection might not cover all phishing variations.
Rendall et al. (2020)	Multi-layered detection framework	Two-layered Classification	Comparable to state-of-the-art methods	Emphasizes multi-layered	Computational complexity may

HR et al. (2020)	Embedded Phishing Detection Browser (EPDB)		with varied feature sets Rule-based extraction and Random Forest Classification	99.36% accuracy	detection efficacy. Advanced browser integration and rule-based methods.	impact real-time performance. Browser-based limitations and rule-based constraints.
Zeng et al. (2020)	PhishBench 2.0 benchmarking framework		Dynamic evaluation of features, classifiers, and metrics	Supports comprehensive assessments	Facilitates continued research and evaluation.	Benchmarking may not address all phishing attack vectors.
Cuzzocrea et al. (2019)	Decision tree-based machine learning		Uses decision tree algorithms for phishing analysis	Effective in phishing detection	Reinforces the role of algorithmic approaches.	Decision trees may not handle complex attack patterns well.
Rao and Pais (2019)	Feature-based machine learning		Utilizes heuristic features from URLs and third-party services	99.31% accuracy with Random Forest	Highlights importance of heuristic features and external data.	Heuristic features may be less effective against novel attacks.
Elnagar et al. (2019)	Cognitive framework with BLSTM-RNN and CNN		Incorporates image recognition and advanced neural networks	Enhanced phishing detection capabilities	Integrates image processing with neural network architectures.	High computational resources required; image processing constraints.
Niakanlahiji et al. (2018)	PhishMon machine learning framework		Utilizes fifteen novel features for detection	95.4% accuracy, 1.3% false positive rate	Importance of diverse feature sets in detection precision.	Novel features might not be universally applicable.
Yi et al. (2018)	Deep Networks (DBN) framework	Belief (DBN)	Incorporates original and interaction features	90% true positive rate, 0.6% false positive rate	Demonstrates deep learning's capability in capturing phishing characteristic s.	DBNs may require extensive training data and resources.
Park et al. (2017)	Phishing-Detective framework		Uses web scraping and data mining techniques	Dynamic and accurate approach	Challenges with evolving phishing tactics.	Evolving phishing tactics present ongoing challenges.

a. Classification of Phishing Attack

In the work of Aslam et al. (2023); Kalaharsha & Mehtre (2021); Tandale & Pawar (2020), phishing attacks are made up of the following types:

- i. **Email Phishing:** In this type of phishing, an attacker sends an email regarding any problem, update, or sensitive matter that must be changed immediately once the user clicks the email. All the input details the end-users enter will be redirected to the attacker.

- ii. Spear Phishing: This type of phishing attack targets specific individuals or enterprises instead of random application users. It is a more in-depth version of phishing that requires special knowledge about an organization, including its power structure. Unlike phishing, emails are sent to specific persons in this attack.
- iii. Whale-phishing: This spear-phishing attack targets high-profile employees, such as the CEO and CFO, to steal sensitive information from a company. As these people hold higher positions within the company, they will have complete access to sensitive data, and it will be easy to obtain more information.
- iv. Smishing (SMS phishing): This attack is carried out to steal users' data, such as credentials, money and financial information, among others. Malicious link: The phishing messages trick recipients into clicking the malicious link, redirecting them to a phishing page where personal information is generated.
- v. Vishing (Voice Phishing): This type of phishing attack is done via telephone, where voice messages or automated voice recordings are used to attain personal information or money from victims. The voice message then requests the recipient to call a stated toll-free number. Once victims call that toll-free number, the victim's bank account number and other personal details are harvested via the phone keypad.
- vi. Content-injection Phishing: In this, the content of the legitimate website is replaced with some random content with different input fields similar to the legitimate site so that end-users trust easily and give their data easily
- vii. Website Phishing: This type creates entirely fake websites that closely resemble legitimate ones (for example, banks, social media platforms, online stores), which aims to lure users into entering personal information like passwords or credit card details on these fake websites. It often involves more elaborate design and content, mimicking the genuine website to gain trust.
- viii. URL Phishing: Uses deceptive website addresses (URLs) to trick users into clicking on them. These URLs can lead to phishing websites, malware downloads, or spam pages. It may not involve a full-fledged fake website, just a misleading URL designed to entice clicks.
- ix. Pharming: Pharming is sometimes known as "phishing without a lure." When a user attempts to navigate to a site, their computer can determine the IP address by consulting a local file of defined mappings, a host file, or a DNS server on the internet. Pharming is usually conducted either by changing the host file on a victim's computer (host file pharming) or by exploiting a vulnerability in DNS server software (DNS poisoning).

For this study, the five types of phishing attacks was considered due to the dataset's availability and the dangerous nature of damages they can cause. The types the phishing attack depicted in Figure 1



Figure 1: Types of Phishing Attack

b. Unveiling Deception with Deep Learning

Phishing attacks rely heavily on deception to lure victims into divulging sensitive information or taking harmful actions (Adebowale et al., 2023). Deception involves the creation of fraudulent emails, websites, or messages designed to trick users into disclosing sensitive information such as login credentials, financial details, or personal data (Jha & Kumar, 2023). However, Deep Learning (DL) is emerging as a powerful tool to counter this deception and protect individuals and organizations. It offers a powerful approach to detecting and mitigating phishing attacks by leveraging advanced algorithms to analyze and identify deceptive patterns in email content, website structure, and user behavior (Lansky et al., 2021).

c. Deep Learning Algorithms

- i. Convolutional Neural Networks (CNNs): CNNs are primarily used for processing structured grid-like data, such as images. They consist of multiple layers of convolutional filters that extract hierarchical features from input images. CNNs are widely employed in image classification, object detection, and image segmentation (Cheng & Parhi, 2020).
- ii. Recurrent Neural Networks (RNNs) and variants (LSTMs, GRUs): RNNs process information sequentially, similar to how we read and understand language. They can remember information from previous words, which is crucial for understanding context and meaning (Baruah & Organero, 2023).
- iii. Transformers: Transformers utilize an attention mechanism, allowing them to pay attention to specific parts of the text relevant to the task. This improves their ability to capture long-range dependencies in complex sentences (Yang et al., 2021).
- iv. Hybrid Models: This model combines two approaches to create a more robust and comprehensive solution. They leverage the strengths of each approach to overcome their limitations and achieve better performance in various tasks (Tang & Mahmoud, 2022).

e. Deception Techniques in Phishing

The following are the Deception Techniques in Phishing according to (Chandra et al., 2020)

- i. Mimicry: Attackers create fake emails, websites, and even phone calls that convincingly resemble legitimate ones, exploiting our trust in familiar brands and institutions.

- ii. Urgency and Scarcity: Phishing messages often create a sense of urgency or limited-time offers to pressure victims into quick actions without proper thought.
- iii. Personalization: Attackers leverage data breaches or social media information to personalize phishing attempts, making them appear more relevant and trustworthy.
- iv. Emotional Manipulation: Phishing messages can trigger fear, guilt, or excitement to cloud judgment and influence victim behaviour.

d. Deep Learning for Phishing Detection Approaches

Text Analysis: DL models can analyze email content, website text, and social media messages to identify deceptive language patterns, suspicious keywords, and impersonation attempts.

Visual Analysis: DL models trained on large image datasets can detect inconsistencies in website design, logos, or images, potentially revealing phish.

Network Traffic Analysis: DL models can analyze traffic patterns for anomalies linked to phishing attempts, like unusual IP addresses or suspicious data transfers.

III. Proposed Multiclass Phishing Framework

The framework presents an architecture integrating two deep learning models to analyze diverse aspects of phishing attacks. The framework consists of four (4) states, namely input, preprocessing, deep learning and classification stage, each having distinct features tailored towards the same purpose. The following are the detailed disruptions of the stages depicted in Figure 2.

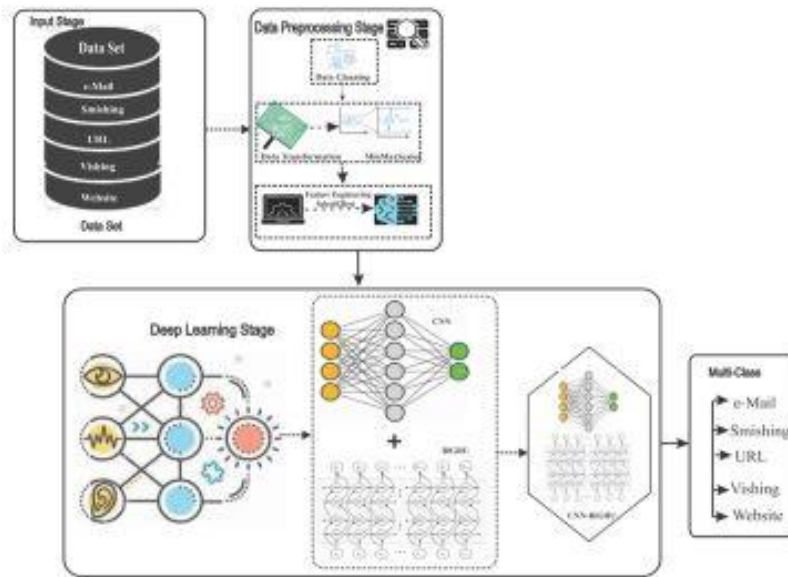


Fig 2: Proposed Multiclass Phishing Framework

- i. Input Stage: This is the first stage comprising five types (email, smishing, URL, vishing and website) of phishing attack datasets, which will be integrated to form a single dataset for Classification. These datasets were generated from PhishTank because it has been widely used in prior research, reliable and publicly available (Karbab et al., 2018) and contains information on phishing attacks reported by users and verified by a community of security experts. This stage forms the input of the next stage in the framework.

- ii. **Data Preprocessing Stage:** During the data preprocessing stage, three crucial phases were carried out: data cleaning, transformation, and feature engineering. Data cleaning, an indispensable aspect of preprocessing, involved identifying and rectifying inconsistencies, errors, and irrelevant data within the dataset to enhance its quality and prepare it for utilization in deep learning models. Following data cleaning, a Minmax scaler was applied to transform the data, aiming to improve its compatibility with deep learning algorithms, preserve the original distribution's shape, and mitigate the influence of feature scales on the optimization process. Subsequently, the dataset was stratified into two sets: 80% allocated for training and validation and 20% designated for testing. The values will then be scaled between 0 and 1 using the min-max scaler, which has been fitted to the training set and transformed to the testing set using equation 1 (Chou *et al.*, 2023; Huang, Peng & Wu, 2021)

$$\text{MinMaxScaler} (v'i) = \frac{x_i - \min_A}{\max_A - \min_A} (\text{new_max}_A - \text{new_min}_A) + \text{new_min}_A \quad (1)$$

Where x_i represents the i th value, \max_A and \min_A denote a feature's maximum and minimum values and new_max_A and new_min_A are the values 0 and 1, respectively.

Feature engineering ensued, incorporating a feature selection technique known as Select K-Best (SelectKBest) to enhance model performance, generalization, and computational efficiency and mitigate the impact of irrelevant or noisy features. The score was determined utilizing equation 3.2, as proposed by 2 (Olatunji *et al.*, 2023; Sharifai & Zainol, 2020; Thuy & Wongthanasu, 2022)

$$x^2 = \sum_{i=1}^n \frac{(OFi - EFi)}{EFi} \quad (2)$$

Where OFi is the frequency observed for the feature F 's i -th value, and EFi is the frequency anticipated for feature F 's i -th value.

- iii. **Deep Learning Stage:** Deep Learning, a subset of machine learning, has garnered significant attention in recent years due to advancements in processing power and expanded data storage capacities. These developments have greatly facilitated the application of deep learning methodologies, which have demonstrated remarkable efficacy across various domains, including image processing, natural language processing, and machine translation, particularly when handling large datasets. Leveraging these advantages, our study adopts two prominent deep learning algorithms: Convolutional Neural Network (CNN) and Bidirectional Gated Recurrent Unit (BiGRU). The selection of these algorithms is based on the belief that combining different approaches enhances overall accuracy, as demonstrated by (Do *et al.*, 2021; Gupta *et al.*, 2018). The CNN component extracts high-level features from the input dataset within this multiclass framework. It is adept at capturing local patterns and features. Subsequently, the BiGRU component sequentially processes these features, considering sequential dependencies and temporal features across different dataset segments. The integration of a fully connected layer atop the BiGRU facilitates final Classification. This framework is poised to enhance the accuracy and effectiveness of phishing attack classification by harnessing the complementary strengths of the CNN-BiGRU architectures.

Let $X = \{x_1, x_2, \dots, x_n\}$ represent the input sequence, where x_i , is the word embedding of the i -th feature in the sequence

$$z_i^l = f \left(\sum_{j=1}^m w_j^l \cdot x_{i+j-1} + b^l \right) \quad (3)$$

Where z_i^l is the output of the $l - th$ convolutional filter at position i , w_j^l are the filter weights, b^l is the bias term, and f is the activation function ReLU.

$$p^l = \max(z_1^l, z_2^l, \dots, z_{n-m+1}^l) \quad (4)$$

where p^l is the output of the max-pooling layer for the $l - th$ filter

$$\vec{h}_t = GRU(x_t, \vec{h}_{t-1}) \quad (5)$$

$$\vec{h}_t = GRU(x_t, \vec{h}_{t+1}) \quad (6)$$

$$h_t = [\vec{h}_t ; \vec{h}_t] \quad (7)$$

Where $[\cdot; \cdot]$ denotes concatenation

$$h = h^1, h^2, \dots, h^L \quad (8)$$

where h^l is the output feature vector from the $l - th$ convolutional filter or BiGRU layer.

$$z = hW + b \quad (9)$$

Where W is the weight matrix and b is the bias vector.

$$\hat{y} = \text{softmax}(z) \quad (10)$$

Where \hat{y} is the predicted probability distribution over the classes.

- iv. Multiclass Stage: this is where the Classification of the phishing attack takes place. After the model has been trained and evaluated, Classification can be used to make predictions on new, unseen data. The model assigns each input instance to the predefined classes based on its learned patterns and features.

V. Results and Discussion

Studies based on Framework, Attack type, and Detection/Classification

The results of the studies based on the existing framework, attack type, and detection/classification are presented in Table 2.

Table 2: Studies Based on Existing Framework, Attack Type, and Detection/Classification

S/N	Author & Year	Framework Proposed	No. of Attack type	Detection
1	Park et al. (2017)	Phishing-Detective, web scraping, data mining	1	Detection
2	Niakanlahiji et al., (2018)	PhishMon	1	Detection
3	Yi et al. (2018)	Deep Belief Networks (DBN)	1	Detection
4	Cuzzocrea et al., (2019)	Decision tree algorithms	1	Detection
5	Elnagar et al., (2019)	BLSTM-RNN, CNN, image recognition	1	Detection
6	(Rao & Pais, 2019).	Feature-based machine learning	1	Detection
7	Hr et al. (2020)	Rule-of-extraction, Random Forest, EPDB	1	Detection
8	(Rendall et al., 2020a).	Multi-layered detection	1	Detection
9	Sadique et al., (2020)	Automated real-time detection framework	1	Detection
10	Saravanan & Subramanian, (2020)	Feature extraction, phishing detection module	1	Detection
11	(Zeng et al., 2020)	PhishBench 2.0	1	Detection
12	Kumar & Subba, (2021)	Machine learning-based security framework	1	Detection
13	Liu et al. (2021)	CASE feature framework	1	Detection
14	(Tang & Mahmoud, 2022).	White list filtering, black list interception, RNN-GRU	1	Detection

15	Alsharaiah et al. (2023)	Random Forest integrated with k-means clustering(RM-KmC)	1	Detection
16	Subba (2023)	Heterogeneous ensemble; 3 base classifiers, 1 meta-classifier	1	Detection
17	Tenis & Santhosh (2023)	Adaptive Recurrent Neural Networks (a-RNN)	1	Detection

Table 2 outlines various studies focused on phishing detection frameworks, each addressing a single type of attack detection through multiple methodologies. It shows that 2020 has the highest number of papers that worked on phishing detection, detected only a kind of phishing attack and frameworks proposed, followed by 2023 and 2019 with 3 papers, 2018 and 2021 with two papers each and 2017 and 2022 with 1. It also depicted the number of frameworks proposed from 2017 to 2023 on phishing attack detection. Figures 3 and 4 present the charts of the analyses, each showing number of attack types detected per year and frameworks proposed per year.

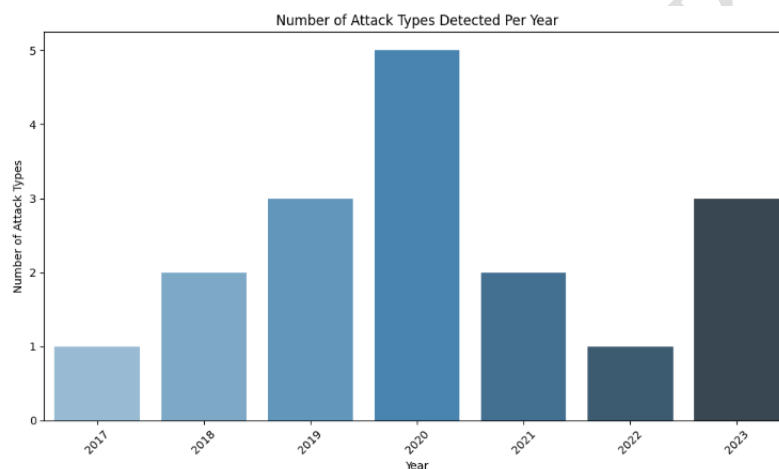


Figure 3: Number of Attack Types Detected Per Yaer

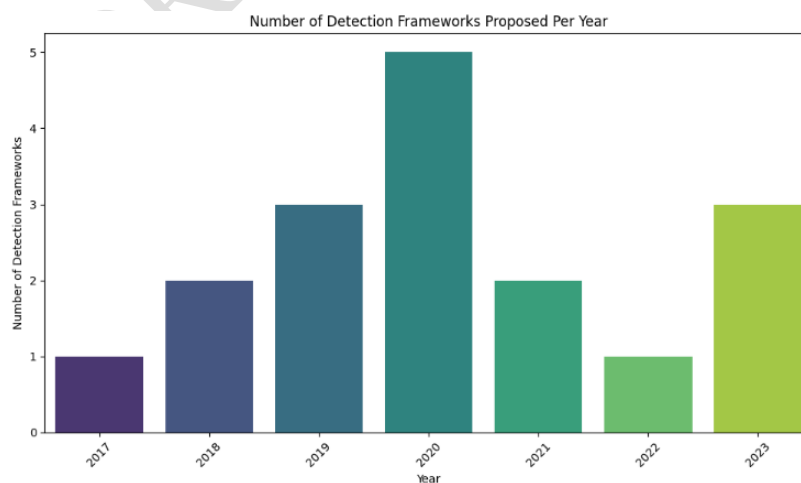


Figure 4: Number of Frameworks Proposed Per Yaer

Frequency of each algorithm used in the Existing Studies

The number of times each algorithm was used is presented in Table 3, which highlights a range of machine and deep learning algorithms tailored to specific data types and applications, showcasing the versatility and broad impact of machine and deep learning techniques. Figure 5 illustrated the frequencies of each algorithm adopted by the different papers in the literature.

Table 3: Frequency of each Algorithm used in the Studies

S/N	Author & Year	Algorithm(s)
1	Yi et al. (2018)	DBN
2	Cuzzocrea et al., (2019)	Decision tree
3	Elnagar et al., (2019)	BLSTM-RNN, CNN
4	Rao & Pais, (2019)	Random Forest
5	Hr et al., (2020)	Random Forest
5	Tang & Mahmoud, (2022)	RNN-GRU
6	Subba (2023)	FCNN
7	Tenis & Santhosh (2023)	a- RNN
8	Alsharaiah et al. (2023)	RM-KmC

Table 3 indicates an evident shift in phishing detection strategies over time. Early studies relied on typical machine learning algorithms, such as Random Forest, which emerged from 2019 and 2020 research. Decision Trees and RNN-GRU were also employed in studies from 2019 and 2022, respectively. As phishing assaults became more complex, researchers began using more advanced approaches, including DBN, BLSTM-RNN, CNN, and FCNN. More recently, hybrid models, notably RM-KmC and a-RNN, have become more prominent, suggesting a tendency toward integrating diverse algorithms to increase detection accuracy and better meet the shifting nature of phishing attacks. Figure 5 shows the frequencies of each algorithm adopted by the different papers in the literature.

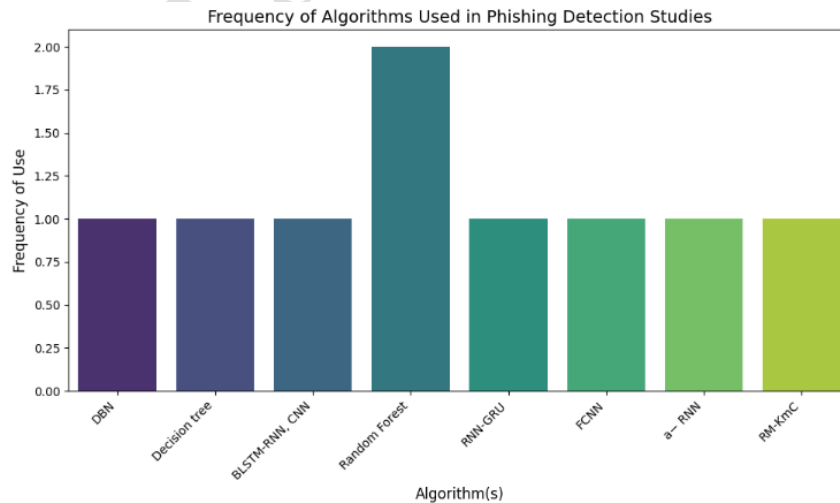


Figure 5: Frequencies of each Algorithm Adopted

Table 4: Different Methods Adopted for Framework Development in Phishing Detection

S/N	Studies	Method	Number of studies
1	Elnagar et al. (2019), Tang & Mahmoud (2022), Yi et al. (2018), Liu et al. (2021), Saravanan & Subramanian Subba (2023) Tenis & Santhosh (2023)	Deep Learning	7
2	Rao & Pais (2019), HR et al. (2020), Rendall et al. (2020), Niakanlahiji et al. (2018), Cuzzocrea et al. (2019), Park et al. (2017), Kumar & Subba (2021), Sadique et al. (2020), Zeng et al. (2020) Alsharaiah et al. (2023)	Machine Learning	10

Table 4 illustrates that Machine Learning approaches are more prevalent in phishing detection investigations, with 10 studies adopting techniques including Random Forests, Decision Trees, and Support Vector Machines. This supremacy can be due to machine learning's capacity to effectively handle structured data and its known performance in phishing detection. In contrast, Deep Learning approaches, applied in 7 research, are increasing, notably in handling the intricacies of current phishing assaults. Techniques such as CNN and RNN are widely employed for their potential to analyze massive, unstructured data, hence enhancing detection accuracy in dynamic, developing situations. Figure 6 depicts the methods adopted by various works to develop the framework.

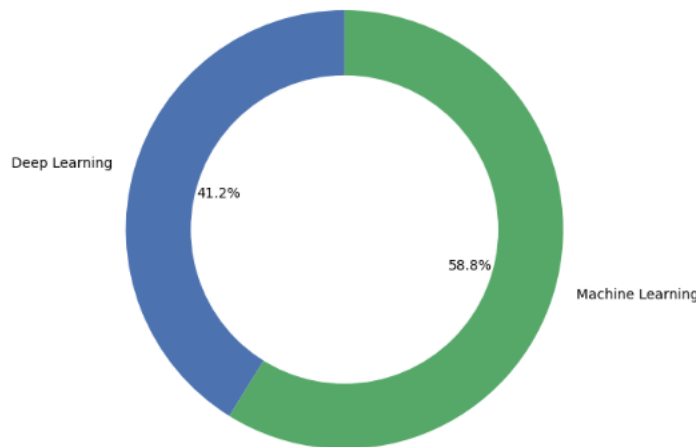


Figure 6: Methods Adopted in Phishing Detection

Comparison of Different Existing Studies based on their Accuracies

The comparison of different Existing studies based on their accuracies is presented in Table 4.

Table 5: Comparison of Different Studies based on Their Accuracies

S/N	Studies	Accuracy (%)
1	Yi et al. (2018)	90
2	Niakanlahiji et al. (2018)	95.4
3	Rao & Pais (2019)	99.31
4	HR et al. (2020)	99.36
5	Sadique et al. (2020)	87
6	Tang & Mahmoud (2022)	99.18
7	Subba (2023)	99
8	Tenis & Santhosh (2023)	98.64
9	Alsharaiah et al. (2023)	99.18

Table 4 analyzes accuracy rates in phishing detection across several studies. HR et al. (2020) established a high standard for phishing detection with the most incredible accuracy of 99.36%, closely followed by Rao & Pais (2019) at 99.31%. Other research, such as Tang & Mahmoud (2022) and Alsharaiah et al. (2023), indicate a high accuracy of 99.18%, while Subba (2023) obtains 99%, placing it among the best performers. However, Sadique et al. (2020) is an anomaly with a substantially lower accuracy of 87%. Niakanlahiji et al. (2018) obtained 95.4%, making it one of the more vigorous studies, albeit still behind the top-tier performances. Figure 7 effectively visualizes the accuracies reported across various studies

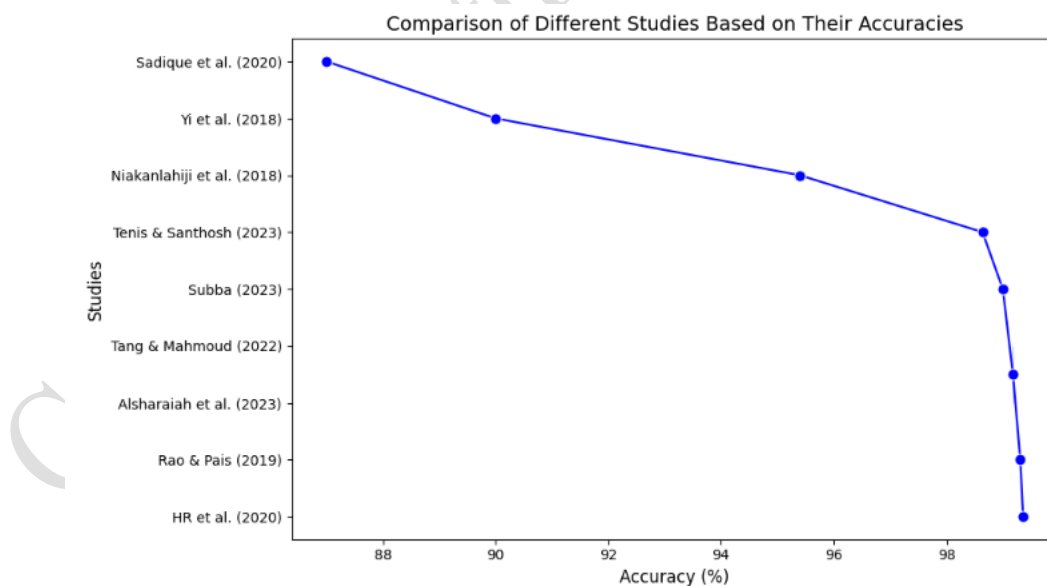


Figure 7: Comparison of Accuracy of Different Studies

Discussion

Advanced detection techniques are required due to the dynamic nature of phishing attacks. Deep learning offers a convincing way to address these changing dangers, whereas traditional approaches frequently fail. To increase detection accuracy and flexibility, the suggested Multi-class phishing detection framework combines the advantages of Convolutional Neural Networks (CNN) with Bidirectional Gated Recurrent Units (BiGRU).

A thorough analysis of current phishing detection systems reveals the various approaches used. Even though machine learning models have been used widely, current research has shown a rising need for deep learning techniques due to the complexity of phishing attempts. However, notable detection precision disparities highlight this domain's ongoing difficulties.

VI. Conclusion

Phishing attacks have become more advanced, rendering traditional detection methods increasingly inadequate. The study reviewed various studies of phishing detection frameworks, highlighting the methodology's strengths and weakness and their efficiencies. The authors discovered the need to introduce a more robust deep learning framework to classify phishing attacks. The proposed multi-class phishing detection framework integrates CNN and BiGRU models to enhance accuracy and adaptability by effectively analyzing local patterns and long-range dependencies. Future studies should prioritize evaluating the framework through experimental testing with standardized performance metrics to offer deeper insights into the model's assessment and effectiveness.

About Authors



Abdullahi Raji Egigogo: Is a Nigerian academic and cybersecurity expert with extensive experience in teaching, research, and community service. Born in Minna, Niger State, he holds a B.Sc. in Computer Science, an M.Tech. in Cybersecurity, and is currently pursuing a Ph.D. in Cybersecurity Science at the Federal University of Technology, Minna. He serves as a lecturer in Software Engineering and Cyber Security at Al-Qalam University, Katsina. Dr. Egigogo's work focuses on machine learning applications for phishing detection, cybersecurity in healthcare and financial sectors, and educational technology. He has authored numerous publications, including research papers and book chapters, and has presented at national and international conferences. His professional credentials include certifications in CCNA, project management, and forensic studies. A dedicated community leader, he actively engages in initiatives to promote technological awareness and education. Fluent in English, Hausa, and Nupe, Dr. Egigogo combines his technical expertise with a commitment to advancing cybersecurity and empowering future generations.



Ismaila Idris: Ismaila Idris holds a B.Tech. in Mathematics Computer Science (2002), M.Sc. in Information Security (2009), and a PhD in Computer Security (2014). With over 19 years of experience, he is an IT specialist in information security, digital forensics, and software development. Idris is a Professor of Cyber Security and Head of the Department of Cyber Security Science at the Federal University of Technology, Minna. He has authored over 70 international publications and holds two patents. Idris has held leadership roles, including Deputy Director of IT Services and National Vice President of the Cyber Security Expert Association of Nigeria. He has contributed to national cybersecurity policies and serves on various academic editorial boards. His research focuses on information security, data mining, software engineering, and computational intelligence. Idris is a member of several professional organizations, including ACM and IAENG.



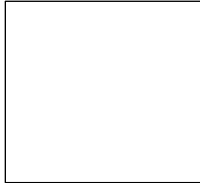
Morufu Olalere: Morufu Olalere holds a Ph.D. in Security in Computing with a focus on Access Control from University Putra Malaysia (2016), an MSc in Computer Science (2014), and a B.Tech. in Industrial Mathematics (2005). His career began at the Federal University of Technology, Minna, where he served as an Assistant Lecturer in 2007 and later contributed to the establishment of the Department of Cyber Security. With over 15 years of experience, he specializes in machine learning applications for cyber security, including areas such as access control, biometric security, and malware detection. Dr. Olalere has mentored numerous Ph.D. and Master's students and held various academic leadership roles. He is an Associate Professor of Cyber Security and joined the National Open University of Nigeria in 2023. His expertise in cyber security and information security makes him an asset to institutions focused on enhancing their cyber security operations.



Opeyemi Aderiike Abisoye: Opeyemi Aderiike Abisoye is currently a Senior Lecturer and the Head of the Department of Computer Science, Federal University of Technology, Minna, Nigeria. She attended the University of Ilorin, Nigeria, where she obtained a PhD in Computer Science. Her Research Interests are Artificial Intelligence, Bioinformatics, Wireless Communication and Information Security. She has more than forty (40) publications in reputable journals and International conferences.



Joseph Adebayo Ojeniyi: Joseph Adebayo Ojeniyi holds a B.Tech., M.Sc., and Ph.D. from the Federal University of Technology, Minna, where he currently serves as the Departmental Anchor for the Cyber Security Science Department at the School of Information and Communication Technology. He is lecturer and an expert in Information Security, Digital Forensics, and Cyber Security, with specialized skills in Cryptography, Penetration Testing, Intrusion Prevention, IDS Data Protection, Steganography, Malware, Cybercrime Investigation, and Digital Forensics. His research focuses on securing digital systems and addressing cybercrime through innovative methods in data security and applied cryptography. Dr. Ojeniyi is a key member of the University's Board of Research, advancing research in cybersecurity and related fields. His contributions to academia and practical cybersecurity make him a valuable figure in both research and the fight against cybercrime.



Idowu Afe : Idowu Afe is a Ph.D. student at the Federal University of Technology, Minna, specializing in Cyber Security. With a strong academic background, he is focused on advancing knowledge in Information Security, Digital Forensics, Cybercrime Investigation, and Data Protection. His research interests include exploring innovative solutions to secure digital systems and combat cyber threats. As a dedicated student, Idowu contributes to the academic community through his work and commitment to addressing challenges in the field of cybersecurity. His ongoing studies and contributions position him as a promising future leader in the domain of Cyber Security.

VII. References

- Adebowale, M. A., Lwin, K. T., & Hossain, M. A. (2023). Intelligent phishing detection scheme using deep learning algorithms. *Journal of Enterprise Information Management*, 36(3), 747–766. <https://doi.org/10.1108/JEIM-01-2020-0036>
- Alsharaiah, M. A., Abu-Shareha, A. A., Abualhaj, M., Baniata, L. H., Adwan, O., Al-Saaidah, A., & Oraiqat, M. (2023). A new phishing-website detection framework using ensemble classification and clustering. *International Journal of Data and Network Science*, 7(2), 857–864. <https://doi.org/10.5267/j.ijdns.2023.1.003>
- Aslam, N., Srivastava, S., & Gore, M. M. (2023). A Comprehensive Analysis of Machine Learning- and Deep Learning-Based Solutions for DDoS Attack Detection in SDN. *ARABIAN JOURNAL FOR SCIENCE AND ENGINEERING*. <https://doi.org/10.1007/s13369-023-08075-2>
- Baruah, R. D., & Organero, M. M. (2023). Integrating Explicit Contexts with Recurrent Neural Networks for Improving Prognostic Models. *IEEE Aerospace Conference Proceedings, 2023-March*. <https://doi.org/10.1109/AERO55745.2023.10115751>
- Chandra, J. V., Challa, N., & Pasupuleti, S. K. (2020). Detection of Deceptive Phishing Based on

- Machine Learning Techniques. *Lecture Notes in Networks and Systems*, 105, 13–22. https://doi.org/10.1007/978-981-15-2407-3_2
- Cheng, C., & Parhi, K. K. (2020). Fast 2D Convolution Algorithms for Convolutional Neural Networks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 67(5), 1678–1691. <https://doi.org/10.1109/TCSI.2020.2964748>
- Chou, C.-Y., Hsu, D.-Y., & Chou, C.-H. (2023). Predicting the Onset of Diabetes with Machine Learning Methods. *Journal of Personalized Medicine* 2023, Vol. 13, Page 406, 13(3), 406. <https://doi.org/10.3390/JPM13030406>
- Cuzzocrea, A., Martinelli, F., & Mercaldo, F. (2019). A machine-learning framework for supporting intelligent web-phishing detection and analysis. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3331076.3331087>
- Damaševičius, R., Maskeliūnas, R., Misra, S., Salaudeen, B. B., & Azeez, N. A. (2020). Identifying phishing attacks in communication networks using URL consistency features. *International Journal of Electronic Security and Digital Forensics*, 12(2), 200. <https://doi.org/10.1504/ijesdf.2020.10027595>
- Do, N. Q., Selamat, A., Krejcar, O., Yokoi, T., & Fujita, H. (2021). Phishing webpage classification via deep learning-based algorithms: An empirical study. *Applied Sciences (Switzerland)*, 11(19). <https://doi.org/10.3390/app11199210>
- Elnagar, S., Thomas, M. A., Elnagar, S., & Thomas, M. (2019). A Cognitive Framework for Detecting Phishing Websites Arabic OCR View project Deep learning View project A Cognitive Framework for Detecting Phishing Websites. March. <https://www.researchgate.net/publication/331535390>
- Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247–267. <https://doi.org/10.1007/S11235-017-0334-Z>
- Hr, M. G., Mv, A., Gunesh Prasad, S., & Vinay, S. (2020). Development of anti-phishing browser based on random forest and rule of extraction framework. *Cybersecurity*, 3(1). <https://doi.org/10.1186/s42400-020-00059-1>
- Huang, Z., Li, Y., Peng, H., & Wu, J. (2021). An ensemble learning approach for predicting the grade of brain glioma using MRI images. *Biomedical Signal Processing and Control*. <https://doi.org/10.1016/j.bspc.2020.102529>
- Jha, A. K., & Kumar, S. (2023). ‘Don’T Fool Me, As It Is Your Loss’ - Impact of Deception on Information Privacy. *Journal of Organizational Computing and Electronic Commerce*, 33(3–4), 117–132. <https://doi.org/10.1080/10919392.2023.2253086>
- Kalaharsha, P., & Mehtre, B. M. (2021). *Detecting Phishing Sites -- An Overview*. 1–13. <http://arxiv.org/abs/2103.12739>
- Karbab, E. B., Debbabi, M., Derhab, A., & Mouheb, D. (2018). MalDozer: Automatic framework for android malware detection using deep learning. *DIGITAL INVESTIGATION*, 24(5th Annual DFRWS European Conference (DFRWS EU) CL-Florence, ITALY), S48–S59. <https://doi.org/10.1016/j.diin.2018.01.007>
- Kumar, Y., & Subba, B. (2021a). A lightweight machine learning based security framework for detecting phishing attacks. *2021 International Conference on COMMunication Systems & NETWORKS (COMSNETS)*, 184–188. <https://doi.org/10.1109/COMSNETS51098.2021.9352828>
- Kumar, Y., & Subba, B. (2021b). A lightweight machine learning based security framework for detecting phishing attacks. *2021 International Conference on COMMunication Systems and*

<https://doi.org/10.1109/COMSNETS51098.2021.9352828>

- Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., Hosseinzadeh, M., & Rahmani, A. M. (2021). Deep Learning-Based Intrusion Detection Systems: A Systematic Review. *IEEE Access*, 9, 101574–101599. <https://doi.org/10.1109/ACCESS.2021.3097247>
- Liu, D. J., Geng, G. G., Jin, X. B., & Wang, W. (2021). An efficient multistage phishing website detection model based on the CASE feature framework: Aiming at the real web environment. *Computers and Security*, 110. <https://doi.org/10.1016/j.cose.2021.102421>
- Niakanlahiji, A., Chu, B. T., & Al-Shaer, E. (2018). PhishMon: A machine learning framework for detecting phishing webpages. *2018 IEEE International Conference on Intelligence and Security Informatics, ISI 2018*, 220–225. <https://doi.org/10.1109/ISI.2018.8587410>
- Olatunji, S. O., Alsheikh, N., Alnajrani, L., Alanazy, A., Almusairii, M., Alshammasi, S., Alansari, A., Zaghdoud, R., Alahmadi, A., Basheer Ahmed, M. I., Ahmed, M. S., & Alhiyafi, J. (2023). Comprehensible Machine-Learning-Based Models for the Pre-Emptive Diagnosis of Multiple Sclerosis Using Clinical Data: A Retrospective Study in the Eastern Province of Saudi Arabia. *International Journal of Environmental Research and Public Health*, 20(5), 4261. <https://doi.org/10.3390/IJERPH20054261/S1>
- Park, A. J., Quadari, R. N., & Tsang, H. H. (2017). Phishing website detection framework through web scraping and data mining. *2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2017*, 680–684. <https://doi.org/10.1109/IEMCON.2017.8117212>
- Rao, R. S., & Pais, A. R. (2019). Detection of phishing websites using an efficient feature-based machine learning framework. *Neural Computing and Applications*, 31(8), 3851–3873. <https://doi.org/10.1007/s00521-017-3305-0>
- Rendall, K., Nisioti, A., & Mylonas, A. (2020a). Towards a multi-layered phishing detection. *Sensors (Switzerland)*, 20(16), 1–18. <https://doi.org/10.3390/s20164540>
- Rendall, K., Nisioti, A., & Mylonas, A. (2020b). Towards a Multi-Layered Phishing Detection. *SENSORS*, 20(16). <https://doi.org/10.3390/s20164540>
- Sadique, F., Kaul, R., Badsha, S., & Sengupta, S. (2020). An Automated Framework for Real-time Phishing URL Detection. *2020 10th Annual Computing and Communication Workshop and Conference, CCWC 2020*, 335–341. <https://doi.org/10.1109/CCWC47524.2020.9031269>
- Saravanan, P., & Subramanian, S. (2020). A Framework for Detecting Phishing Websites using GA based Feature Selection and ARTMAP based Website Classification. *Procedia Computer Science*, 171, 1083–1092. <https://doi.org/10.1016/j.procs.2020.04.116>
- Sharifai, G. A., & Zainol, Z. (2020). Feature Selection for High-Dimensional and Imbalanced Biomedical Data Based on Robust Correlation Based Redundancy and Binary Grasshopper Optimization Algorithm. *Genes* 2020, Vol. 11, Page 717, 11(7), 717. <https://doi.org/10.3390/GENES11070717>
- Subba, B. (2023). A heterogeneous stacking ensemble-based security framework for detecting phishing attacks. *2023 National Conference on Communications, NCC 2023*. <https://doi.org/10.1109/NCC56989.2023.10068026>
- Tandale, K. D., & Pawar, S. N. (2020). Different Types of Phishing Attacks and Detection Techniques: A Review. *Proceedings of the 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing, ICSIDEMPC 2020*, 295–299. <https://doi.org/10.1109/ICSIDEMPC49020.2020.9299624>

- Tang, L., & Mahmoud, Q. H. (2022). A Deep Learning-Based Framework for Phishing Website Detection. *IEEE Access*, 10, 1509–1521. <https://doi.org/10.1109/ACCESS.2021.3137636>
- Tenis, A., & Santhosh, R. (2023). Modelling of an Adaptive Network Model for Phishing Website Detection Using Learning Approaches. *Fusion: Practice and Applications*, 12(2), 159–171. <https://doi.org/10.54216/FPA.120213>
- Thuy, N. N., & Wongthanavas, S. (2022). A Novel Feature Selection Method for High-Dimensional Mixed Decision Tables. *IEEE Transactions on Neural Networks and Learning Systems*, 33(7), 3024–3037. <https://doi.org/10.1109/TNNLS.2020.3048080>
- Yang, G., Tang, H., Ding, M., Sebe, N., & Ricci, E. (2021). Transformer-Based Attention Networks for Continuous Pixel-Wise Prediction. *Proceedings of the IEEE International Conference on Computer Vision*, 16249–16259. <https://doi.org/10.1109/ICCV48922.2021.01596>
- Yeung, C. A., Liccardi, I., Lu, K., Seneviratne, O., & Berners-Lee, T. (2023). Decentralization: The Future of Online Social Networking. *Linking the World's Information*, 187–199. <https://doi.org/10.1145/3591366.3591383>
- Yi, P., Guan, Y., Zou, F., Yao, Y., Wang, W., & Zhu, T. (2018a). Web phishing detection using a deep learning framework. *Wireless Communications and Mobile Computing*, 2018. <https://doi.org/10.1155/2018/4678746>
- Zeng, V., Zhou, X., Baki, S., & Verma, R. M. (2020). PhishBench 2.0: A Versatile and Extendable Benchmarking Framework for Phishing. *Proceedings of the ACM Conference on Computer and Communications Security*, 2077–2079. <https://doi.org/10.1145/3372297.3420017>
- Zhao, Y., Ma, B., Wang, Z., Liu, Z., Zeng, Y., & Ma, J. (2022). Trajectory Obfuscation and Detection in Internet-of-vehicles. *2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 769–774. <https://doi.org/10.1109/CSCWD54268.2022.9776163>

CAPCDR 8th CONFERENCE