Authors	Title	Journal Name	Publishin g House	Year	Volume	Issue	Problem Solved	Method Used to Solve the Problem	Data & Its Availabilit y
Diana T. Mosa; Mahmoud Y. Shams; Amr A. Abohany; El-Sayed M. El- kenawy; M. Thabet	Machine Learning Technique s for Detecting Phishing URL Attacks	Computer s, Materials & Continua	Not specified	2023	75	1	Detect phishing URL attacks in a cyber-sec urity context by identifying malicious websites that mislead users	models (Neural Networks, Naïve Bayes, and Adaboost) applied on website features	comprisin g over 11,000 website URLs, available in text and CSV formats; each sample includes
Authors	Title	Journal Name	Publishin g House	Year	Volume	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Abdul Karim, Samir Brahim Belhaouar i, Mobeensh ahrooz, Khabib Mustofa, Ands. Ramanak umarjoga	Through	IEEE Access (inferred from DOI)	IEEE	2023		11	Not	Detect phishing attacks via URL classificat ion to protect users from cybercrim es and online fraud.	A hybrid machine learning approach that employs multiple algorithm s (decision tree, linear regression, random forest, naive Bayes, gradient boosting classifier, K-neighbors classifier, support vector classifier) alongside a novel hybrid	A publicly available phishing URL dataset from Kaggle consisting of 11,054 records with 33 attributes extracted from over 11,000 websites (including both phishing and legitimate URLs).
Authors	Title	Journal Name	Publishin g House	Year	Volum	ie	Issue	Problem Solved	Method Used to Solve the Problem	Data & Its Availabilit y

Kanishka Misra, Julia Taylor Rayz	LMs go Phishing: Adapting Pre- trained Language Models to Detect Phishing Emails	2022 IEEE/WIC/ ACM Internatio nal Joint Conferenc e on Web Intelligenc e and Intelligent Agent Technolog y (WI-IAT)	IEEE	2022	N/A	N/A	the persistent challenge of phishing in email communi cations by improving detection methods	tuning them on a large corpus of ~725k training emails with a classificat ion objective and (b) employing an in-	sources: legitimate emails from Enron, Avocado, and IWSPA- AP; phishing emails from Nazario, FRAUD, and UNTROUB LED. After rigorous pre- processin g and deduplica	
Authors	Title	Journal Name	Publishin g House	Year	Volume	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y	

Kunle Oloyede, Chinenye Obunadik e, Simo Yufenyuy Simo, Emmanue l Elom, Abdul- Waliyyu Bello, Somtobe Olisah, Callistus Obunadik e, Oluwada milola Ogunleye, Sulaimon Adeniji	Impact Of Web (URL) Phishing and Its Detection	Internatio nal Journal of Scientific Research and Managem ent (IJSRM)	IJSRM (via https://ijsr m.net)	2024	12		Mitigate the risks posed by web phishing attacks by identifying fraudulent URLs and phishing emails in order to protect sensitive informatio n.	Phish Tank Database) , data cleaning and feature extraction using Python, followed by applying machine learning models	Data are drawn from publicly available phishing datasets and APIs; while several sources (e.g., Phish Tank Database) are mentione d, the article does not provide direct links to specific open datasets.
Authors	Title	Journal Name	Publishin g House	Year	Volume	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Samer Atawneh; Hamzah Aljehani	Phishing Email Detection Model Using Deep Learning	Electronics	MDPI, Basel, Switzerlan d	2023	12	N/A	Detect and prevent email phishing attacks	Deep learning models—i ncluding convolutio nal neural networks (CNNs), long short-term memory (LSTM) networks, recurrent neural networks (RNNs), and bidirectio nal encoder represent ations from transform ers (BERT) using natural language	consisting of phishing and benign emails was used; details on public
Authors	Title	Journal Name	Publishin g House	Year	Volume	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

	Comparati							Preproces	A dataset
	ve							sing text	comprisin
	Analysis							(tokenizati	g 13,055
	of Deep							on,	training
	Learning							padding,	samples
	Algorithm							label-	and 5,595
	s for						Detecting	encoding)	testing
	Phishing						and	followed	samples
	Email	Applied					accurately	by	of emails
	Detection	Mathemat					classifying	employing	
Mohamed		ics on	specified				phishing	deep	The study
Hassan	"Evaluatio	Science	(self-archi	2024	1	1	emails in	learning	highlights
	n of Deep	and	ved under				an	architectu	
	Learning	Engineerin	CC BY)				inherently	•	imbalance
	Algorithm	g					imbalance	fically	in the
	s in						d dataset	CNN, a	"Email
	Comparis							hybrid	Type"
	on for							CNN-	labels, but
	Phishing							RNN, and	does not
	Email							RCNN for	specify
	Identificat							binary	public
	ion")							classificat	availabilit
	, ,							ion	у.

								Method	Data & its
Authors	Title	Journal	Publishin	Year	Volume	Issue	Problem	used to	availabilit
Autilois	TILLE	Name	g House	i Cai	Volume	ISSUE	Solved	solve the	avaitabitit
								problem	У

Parisa Mehdi Gholampo ur, Rakesh M. Verma	Adversaria l Robustne ss of Phishing Email Detection Models	Proceedin gs of the 9th ACM Internatio nal Workshop on Security and Privacy Analytics (IWSPA '23)	ACM, New York, NY, USA	2023	N/A	N/A	s of phishing	adversaria l examples using TextAttack technique s (Textfoole r, PWWS, DeepWor dBug, BAE), fine- tuning GPT-2 for synthetic phishing email generatio n, and applying a K-Nearest Neighbor defense to correctly	the public IWSPA 2.0 phishing/l egitimate email dataset (initially composed of 629 phishing and 5092 legitimate emails, later refined), with the augmente d adversaria l and synthetic datasets publicly available on GitHub (https://git
Authors	Title	Journal Name	Publishin g House	Year	Volume	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Dam Minh Linh, Ha Duy Hung, Han Minh Chau, Quang Sy Vu, Thanh- Nam Tran	detection using deep learning methods	Internatio nal Journal of Electrical and Computer Engineerin g (IJECE)	Not specified	2024	14		Provides real-time detection and preventio n of phishing attacks by detecting malicious URL links via a browser extension.	A browser extension is developed that integrates deep learning—primarily a convolutio nal neural network (CNN)—to classify URLs in real time. The paper also compares various ML models (e.g., LR, DT, RF, SVM, CNN, and CNN-LSTM) and emnlovs a	Uses a large malicious URL dataset containing 651,191 samples compiled from five benchmar k sources, with a detailed breakdow n (benign, defaceme nt, phishing, malware) provided in Table 1.
Authors	Title	Journal Name	Publishin g House	Year	Volume	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

P.C.R. Chinta; C.S. Moore; L.M. Karaka; M. Sakuru; V. Bodepudi; S.R. Maka	Building an Intelligent Phishing Email Detection System Using Machine Learning and Feature Engineerin	Science, Engineerin g and Technolog y	EJASET (via www.ejas et.com)	2025		3	Identifying and mitigating phishing 2 email threats in digital communi cations	Comprehe nsive pipeline of data preproces sing (tokenizati on, stop word removal, etc.), feature engineerin g, and training multiple ML models (CNN, XGBoost, RNN, SVM) with the best performan ce achieved by a BERT-LSTM hybrid	A large- scale phishing email dataset combining phishing and legitimate emails
Authors	Title	Journal Name	Publishin g House	Year	Volume	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Safaa Magdy, Yasmine Abouelseo ud, Mervat Mikhail	_	Computer Networks		2022		206	N/A (article ID 108826 is provided instead)	of spam and phishing emails that waste bandwidth , jeopardize security,	neural network classifier incorporat ing feature extraction from emails, feature selection technique s (Low Variance, PCA, Chi- squared), and grid search hyperpara meter tuning to discrimina te among ham, spam, and phishing	SpamBas e (from the UCI repository), CSDMC20 10 spam corpus, and a merged Phishing_ corpus (from SpamAssa ssin and Nazario) which are
Authors	Title	Journal Name	Publishin g House	Year	Volur	ne	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Chidimma Opara, Yingke Chen, Bo Wei	Look before you leap: Detecting phishing webpages by exploiting raw URL and HTML characteri stics	Expert Systems With Applicatio ns	Elsevier Ltd	2024	23	86 N/A		To develop a reliable mechanis m for detecting phishing webpages —helping to prevent email/inte rnet fraud—by addressin g the limitation s of manual feature extraction	feature represent ations from raw URLs and HTML content. It employs an embeddin g layer for character s (URL) and words	d on a real- world phishing dataset, and the authors have made the dataset available to promote verificatio n and
Authors	Title	Journal Name	Publishin g House	Year	Volume	e Is:	sue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Liqun Yang; Jiawei Zhang; Xiaozhe Wang; Zhi Li; Zhoujun Li; Yueying He	An improved ELM-based and data preproces sing integrated approach for phishing detection considerin g comprehe nsive features	-	Elsevier Ltd.	2021		165	N/A (Article ID: 113863)	The paper addresses the challenge of detecting phishing websites efficiently, aiming to overcome the drawback s of slow training and suboptim al detection accuracy in existing methods.	learning machine (NIOSELM) is proposed. This approach avoids matrix inversion using the Sherman- Morrison Woodbury equation and integrates	top 2000 and 58,000 DMOZ websites covering various sectors; phishing websites (5000 examples) are retrieved from PhishTank . Data is collected via a Python- based web crawler
Authors	Title	Journal Name	Publishin g House	Year	Volum	ne	Issue	Problem Solved	used to solve the problem	Data & its availabilit y

Jay Doshi, Kunal Parmar, Raj Sanghavi, Narendra Shekokar	A comprehe nsive dual- layer architectu re for phishing and spam email detection	Computer s & Security	Elsevier	2023		133	Unspecifi	Tackles the dual challenge of spam and phishing email detection by addressin g limitation s in earlier studies that either focus on only one type of malicious email or use a single feature source (body or content).	(RNN), and	emails from Nazario's corpus and spam/ha m emails
Authors	Title	Journal Name	Publishin g House	Year	Volu	me	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Abdulla Al- Subaiey; Fatema Antora; Mohamm ed Al- Thani; Amith Khandaka r; Naser Abdullah Alam; SM Ashfaq Uz Zaman; Kaniz	Novel interpreta ble and robust web-based AI platform for phishing email	Computer s and Electrical Engineerin g	Elsevier Ltd.	2024		120 N	I/A	ce on proprietar y datasets and the	multiple public phishing/s pam email datasets followed by rigorous text preproces sing (cleaning, tokenizati on, and feature extraction via TF- IDF), training and evaluating machine learning models (SVM, Multinomi al Naive Baves.	sources including the Enron Phishing Email Dataset, CEAS 2008 Spam Challenge Corpus, Ling- Spam Corpus, Nazario Spam Dataset, Nigerian Fraud Dataset, and SpamAssa
Authors	Title	Journal Name	Publishin g House	Year	Volur	ne	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

N. Swapna Goud, Dr. Anjali Mathur	Feature Engineerin g Framewor k to detect Phishing Websites using URL Analysis	Internatio nal Journal of Advanced Computer Science and Applicatio ns (IJACSA)	(hosted on thesai.org) or not	2021	12		Detection of phishing websites by 7 identifying and selecting critical URL-base d features	learning technique s – including bagging (with a Decision Tree	A dataset comprisin g 112 URL features (with a target attribute) that is pre-proce ssed via standard scaling and split into 80% training and 20% testing sets
Authors	Title	Journal Name	Publishin g House	Year	Volume	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Dong-Jie Liu; Guang- Gang Geng; Xiao-Bo Jin; Wei Wang	An efficient multistage phishing website detection model based on the CASE feature framewor k: Aiming at the real web environme nt	Computer s & Security	Elsevier Ltd.	2021		110	N/A	the need for fast and accurate phishing website detection in real web environme nts by overcomin	a comprehe nsive and interpreta ble CASE feature framewor k using quaternar y features—Counterfe	dataset is construct ed by gathering websites from varied sources (different languages , content qualities, and obfuscati on levels) to simulate the real web environme nt. Two
uthors	Title	Journal Name	Publishin g House	Year	Volu	me	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Raniyah Wazirali, Rami Ahmad, Ashraf Abdel- Karim Abu Ein	Sustainin g accurate detection of phishing URLs using SDN and feature selection approach es	Computer Networks		2021	201	N/A (Article No. 108591)	Improving the accurate detection of phishing URLs while reducing the computati onal burden on end-user devices (addressi ng low accuracy, lengthy learning curves, and hardware limitation s)	offloads URL classificat ion to the SDN controller through the combined use of feature selection (Recursive Feature Eliminatio n with SVM) and deep learning (Conventi onal Neural Network, forming the FS- CNN	A dataset comprisin g 51,200 URL samples: legitimate URLs collected from https://50 00best.co m/website s and phishing URLs obtained from https://w ww.phisht ank.com
Authors	Title	Journal Name	Publishin g House	Year	Volume	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Jibrilla Tanimu, Stavros Shiaeles, Mo Adda	A Comparati ve Analysis of Feature Eliminator Methods to Improve Machine Learning Phishing Detection	Science and	BONVIEW PUBLISHI NG PTE. LTD.	2024		2	2	Enhance ML-based phishing detection by selecting the most significant features – thereby reducing computati onal overhead and improving detection accuracy in real time.	Comparative evaluation of various feature eliminatio n methods (e.g., Recursive Feature Eliminatio n, Univariate Feature Selection, correlatio n-based selection) integrated with machine learning classifiers such as Random Forest, SVM, etc.	Data was collected via a crawler from the PhishTank repository , amassing over 50,000 phishing websites (with nonphishing data included) stored in a MySQL database.
Authors	Title	Journal Name	Publishin g House	Year	Volume	e	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Emre Kocyigit, Mehmet Korkmaz, Ozgur Koray Sahingoz, and Banu Diri	_	Applied Sciences	MDPI (Basel, Switzerlan d)	2024		14	6081 (article number)	Addresses the challenge s of phishing detection by mitigating overfitting , reducing computati onal cost, and improving model performan ce caused by an excessive number of features in URL-based phishing detection systems.	Proposes a Genetic Algorithm (GA)-base d approach enhanced with a local optimizati on step. The method leverages uniform crossover, bit-flip mutation, and tourname nt selection to efficiently select an optimal subset of features for	The study uses URL-based features from phishing datasets. However, precise details on dataset size, source, or public availabilit y are not explicitly provided.
Authors	Title	Journal Name	Publishin g House	Year	Volur	ne	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Murathan OK, Ilker Kara, Ahmet Ozaday	Characteristics of Understanding URLs and Domain Names Features: The Detection of Phishing Websites With Machine Learning Methods		IEEE	2022		10	Not specified	Detect phishing websites by analyzing URL and domain name features, thereby counterin g online phishing attacks.	s (including Logistic Regressio n, LDA, KNN, Decision Trees, SVM, and with Random Forest showing the highest nerforman	Dataset of 32,928 records (approxim ately 20,614 phishing and 12,314 legitimate websites) gathered from the TR-CERT opensource data. The paper also provides an access link for dataset requests.
Authors	Title	Journal Name	Publishin g House	Year	Volur	ne	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Abdul Karim, Samir Brahim Belhaouar i, Mobeensh ahrooz, Khabib Mustofa, Ands Ramanak umarjoga	Through	IEEE Access	IEEE	2023 (publicati on date: 3 March 2023)		11	Not Specified (N/A)	Detecting phishing URLs/web sites to enhance cybersecu rity and safeguard user data against phishing attacks	A hybrid machine learning approach employing several algorithm s including Decision Tree (DT), Logistic Regression (LR), Support Vector Machine (SVC) combined as the proposed LSD (LR+SVC+DT) model with soft/hard voting. The study also	Utilizes a phishing URL dataset sourced from Kaggle consisting of 11,054 records and 33 attributes (data presented as vectors from over 11,000 websites)
Authors	Title	Journal Name	Publishin g House	Year	Volum	ıe	Issue	Problem Solved	Method Used to Solve the Problem	Data & Its Availabilit y

Rizka Widyarini Purwanto, Arindam Pal, Alan Blair, Sanjay Jha	PHISHSIM: Aiding Phishing Website Detection With a Feature-Free Tool	Transactio ns on Informatio n Forensics and	IEEE	2022		17 N	N/A	Effectively detect phishing websites without needing manual feature extraction , even when phishing sites are slight variations of known attacks.	Normalize d Compress ion Distance (NCD) over website HTMLs. The method employs the Furthest Point First	on a large dataset comprisin g phishing websites (e.g., reports from PhishTank and manually verified brandspecific cases). The paper does not explicitly state if the dataset is publicly
Authors	Title	Journal Name	Publishin g House	Year	Volun	пе	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Ali Aljofey, Qingshan Jiang, Abdur Rasool, Hui Chen, Wenyin Liu, Qiang Qu, Yang Wang	effective detection approach for	Scientific Reports	Nature Publishing Group	2022		12	8842 2 (article number)	Detect phishing websites that masquera de as legitimate and mitigate risks such as 0-hour attacks and false positives	Extracts a hybrid set of features including: 	A custom dataset was built comprisin g 60,252 webpages (27,280 phishing and 32,972 benign), with testing also performed on a benchmar k dataset.
Authors	Title	Journal Name	Publishin g House	Year	Volum	ne	Issue	Problem Solved	Method used to solve the problem	Data & its availabilit y

Α

Performa nce Metrics & Values	Future Works (if any)	Limitation (if any)	Critique (if any)
Neural Network: 90.23% accuracy; Naïve Bayes: 92.97% accuracy; Adaboost: 95.43% accuracy; additional metrics such as precision, sensitivity , specificity , and F1- score are also reported		potential dependen ce on rule- based feature extraction	accuracie s are achieved, the study would benefit from broader dataset validation
Performa nce metrics & values	Future works (if any)	Limitation (if any)	Critique (if any)

Evaluated using accuracy, precision, recall, F1-score, and specificity. The comparati ve analyses showed that the proposed method outperfor ms individual models – with one instance reporting an accuracy of up to 99.55% when using third-	Not explicitly discussed in the provided content.	The use of third-party services increases detection time and may impact computati onal efficiency.	The paper does not offer an explicit critique; the proposed approach is presented as effective, although issues like processin g speed and scalability might benefit from further exploratio n.
nartv Performa			
nce Metrics &	Future Works (if	Limitation (if any)	Critique (if any)

any)

Values

		the dual
		tile uuat
		approach
		(fine-
Not	Fino-	tuning and
explicitly		priming)
detailed; the discussio	models	shows
		promising
		performan
n hints at	_	ce, the
exploring		heavy
•	•	reliance
	•	on large
	reduction	pre-
	in	trained
	performan	models
	ce when	and
	handling	extensive
generaliza	emails	data
	from	cleaning
-	unseen or	could limit
	different	replicabili
_	distributio	ty and practical
	ns.	deployme
11.		nt in real-
		world,
		noisy
		settings.
Future works (if any)	Limitation (if any)	Critique (if any)
	explicitly detailed; the discussio n hints at exploring strategies to further enhance robustnes s to domain shifts and generaliza tion beyond the training distributio n. Future works (if	explicitly detailed; the discussion hints at exploring strategies to further enhance robustnes s to domain shifts and generalization beyond the training distribution. Future works (if time-tuned tuned models exhibit overfitting to the training domain, causing a reduction in performan ce when handling emails from unseen or different distributions.

99.61% explicitly accuracy (observed for the combinati on of BERT and LSTM) Not explicitly mentione d discussed data gen
--

Performa	Future		
nce	works (if any)	Limitation	Critique
metrics &		(if any)	(if any)
values			

Reported evaluation metrics indicate an overall accuracy around 97% (with detailed metrics per model: e.g., CNN: Acc ≈ 97%, Precision ≈ 96–98%, Recall ≈ 96–97%, F1-Score ≈ 96–97%)	Future research is suggested to further address challenge s such as the imbalance in data and to optimize computati onal efficiency for real-time phishing detection	The imbalance d nature of the dataset leads to challenge s including a non-neglig ible proportion of false negatives and, in some architectu res (e.g., CNN-RNN), increased training/te sting time	The paper does not provide external validation with independ ent data and offers limited discussio n on the practical impact of false negatives; in addition, the complexit y of the proposed models may constrain scalability in real-world application
---	--	--	--

Performa

nce

metrics &

values

Future

works (if

any)

Limitation Critique

(if any)

(if any)

Baseline models achieved approxima tely 0.99 accuracy with F1 scores around 0.95–0.97; however, under adversaria lattacks the F1 score dropped dramatica lly (in some cases as low as 0.10), while the defensive K-NN approach yielded 94%	Investigat e more robust augmenta tion methods and scalable defense mechanis ms—parti cularly to improve the classificat ion of legitimate emails under adversaria l conditions	some adversaria l attack technique s (e.g., Textfooler	Although the study makes a valuable contributi on by addressin g adversaria l vulnerabili ties in detection models, it is limited by its focus on specific attack scenarios and models, and further work is needed to balance robustnes s with
Performa nce metrics & values	Future works (if any)	Limitation (if any)	Critique (if any)

The CNN model achieved an accuracy of 98.4%. Additional metrics include high detection scores (with malicious URLs scoring around 0.999, surpassin g the default threshold of 0.5) along with evaluation s based on precision, recall and	hints at the potential for enhancing the character encoding strategy and adapting the model to future phishing technique s.	potential drawback s include reliance on a fixed threshold for classificat ion (0.5) and the challenge of ensuring that the dataset	The approach is robust and technicall y detailed, demonstr ating high accuracy. Critically, one might note that further discussio n on handling false positives in diverse real-world environme nts, scalability issues, and continuou s model updates in an
Performa nce metrics & values	Future works (if any)	Limitation (if any)	Critique (if any)

BERT-LSTM: Accuracy = 99.55%, Precision = 99.61%, Recall = 99.55%, F1-score = 99.24% (with comparative analysis against models such as Naïve Bayes, RNN, and SVM) Performa	Extend the current work toward real-time detection, refine feature engineerin g, incorporat e larger and more diverse datasets, and optimize computati onal efficiency	Relies on large, annotated datasets; high computati onal requireme nts; may need frequent updates to cope with evolving phishing tactics	Although the performan ce metrics are outstanding, there is a concern about overfitting and limited generalization when faced with real-world, noisy data. Additionally, the method's high complexity might hinder deployment in resource-
nce metrics & values	works (if any)	Limitation (if any)	Critique (if any)

The study		Limitation	The study
reports		s are not	provides a
competitiv		explicitly	detailed
е	Future	stated;	and
validation	work is	however,	well-struc
accuracy	mentione	the	tured
and fast	d in	discussio	approach
testing	Section 6;	n hints	along with
performan	it likely	that	а
ce (with a	involves	model	comparati
maximum	further	performan	ve
test time	enhance	ce may be	analysis
of	ments in	sensitive	to related
0.07856	network	to the	work. A
seconds),	architectu	chosen	critique
claiming	re and	feature	might be
to	refining	selection	that more
outperfor	feature	method	explicit
m	selection	and that	reporting
state-of-t	methods,	some	of
he-art	though	technique	numerical
methods	details are	s (e.g.,	performan
though	not fully	metaheuri	ce metrics
detailed	elaborate	stic	and
numeric	d in the	optimizati	real-world
accuracy	excerpt	on) can	limitation
values are		lead to	s could
not		longer	enhance
exnlicitly		model-	clarity and

Performa

nce

metrics &

values

Future

works (if

any)

Limitation Critique

(if any)

(if any)

The article does not explicitly list limitation s of the No explicit proposed critique is model; provided; however, the paper as with Not positions many Accuracy: explicitly WebPhish DNN 98.1% mentione as approach d outperfor es, issues ming like heavy existing data baseline requireme methods. nts and computati onal burden may be inherent.

Performa nce works (if any)

Huture Limitation Critique (if any) (if any)

The experimental results indicate improved detection accuracy and faster training speed compared to other methods, though no specific numerical values are provided in the excerpt.	The article does not explicitly state future work directions .	The paper notes that domain and topologica I features may not be fully captured for all phishing websites due to temporary unavailabi lity. Moreover, some steps (e.g., reliance on synthetic data via ADASYN) might introduce dependen cv on	While the method shows promise in improving training speed and detection accuracy, the reliance on multiple preproces sing steps (ADASYN and SDAE) and advanced matrix operation s may add complexit y when scaling or deploying in real-world environme
Performa nce	Future	Limitation	Critique

nce

metrics &

values

works (if

any)

Limitation Critique

(if any)

(if any)

nce

metrics &

values

Future

works (if

any)

Limitation Critique

(if any)

The approach is

The article comprehe does not nsive and explicitly robust-in discuss tegrating limitation data s; merging, however, preproces aspects sing, such as explainabl scalability e AI, and

f1 score of explicitly 0.99 (as mentione or reported d within in the the abstract). provided content.

Not

web generaliza deployme bility nt. beyond Nonethele ss, it the selected could public benefit datasets from a might deeper require discussio further n on real-

evaluation world deployme

nt

challenge s. ablation

Performa **Future Limitation Critique** nce works (if metrics & (if any) (if any) any) values

any)

(if any)

(if any)

metrics &

values

The method achieves better detection results with high efficiency, including high recall rates and very low false alarm rates, while significant ly shortenin g execution time. However, the article does not provide detailed numerical values for	The article does not explicitly outline future works, though it implies that further research into advanced feature extraction and model generaliza tion could be explored.	Not explicitly discussed ; however, as with many phishing detection approach es, challenge s may arise from rapidly evolving phishing technique s and the difficulties inherent in handling extremely imbalance d (real- world) datasets.	nsive and practical, the work would benefit from more detailed performan ce metrics and validation on larger, more diverse datasets. The reliance on hand-crafted
Performa nce metrics & values	Future works (if any)	Limitation (if any)	Critique (if any)

nce

metrics &

values

Future

works (if

any)

Limitation Critique

(if any)

Performa nce metrics & values

Future works (if any)

Limitation Critique (if any)

works (if

any)

(if any)

(if any)

metrics &

values

The study could be Integratio critiqued n into real- Reliance for Reported time email on highpotential accuracy link quality, issues in up to blocking balanced generaliza 98.90%, and data. The bility due with test performan secure to the use results connectio ce may of a deteriorat showing national 98% mechanis e over dataset detection ms. Also, time as and the attackers on further possibility phishing dynamic further that the pages and updates to evolve feature 97% on track new their extraction legitimate phishing technique process websites tactics s; the may not (overall and dataset is fully ~98% continuou mainly account correct sly update national, for prediction the which sophistica rate) database might limit ted or diversity. are evolving planned. adversaria I tactics.

Performa nce works (if metrics & any)

Future Limitation Critique (if any) (if any)

Evaluated			
using			While the
accuracy,			study
precision,	Not		presents a
recall, F1-	explicitly		comprehe
score, and	specified;	Not	nsive and
specificity	however,	explicitly	innovative
•	the	discussed	hybrid
Comparati	discussio	; potential	approach,
ve	n hints at	limitation	it lacks
analysis	potential	s include	detailed
indicates	enhance	dependen	quantitati
that the	ments	ce on	ve
proposed	such as	dataset	comparis
approach	incorporat	quality	ons for
outperfor	ing more advanced	and	each algorithm
ms conventio	NLP-	increased	and an in-
nal	based	detection	depth
models	feature	time when	discussio
with	extraction	integratin	n on the
reported	and	g third-	generaliza
accuracy	extended	party	bility and
figures	real-world	features.	potential
reaching	validation		evolving
as high as	s.		nature of
approxima			phishing
tely			attacks.
99.55% in			
Performa	Future	1 ! ! 4 . * *	Outkinson
nce	Works (if	Limitation	Critique
Metrics &	any)	(if any)	(if any)
Values			

nce

metrics &

values

Future

works (if

any)

Limitation Critique

(if any)

nce

metrics &

values

Future

works (if

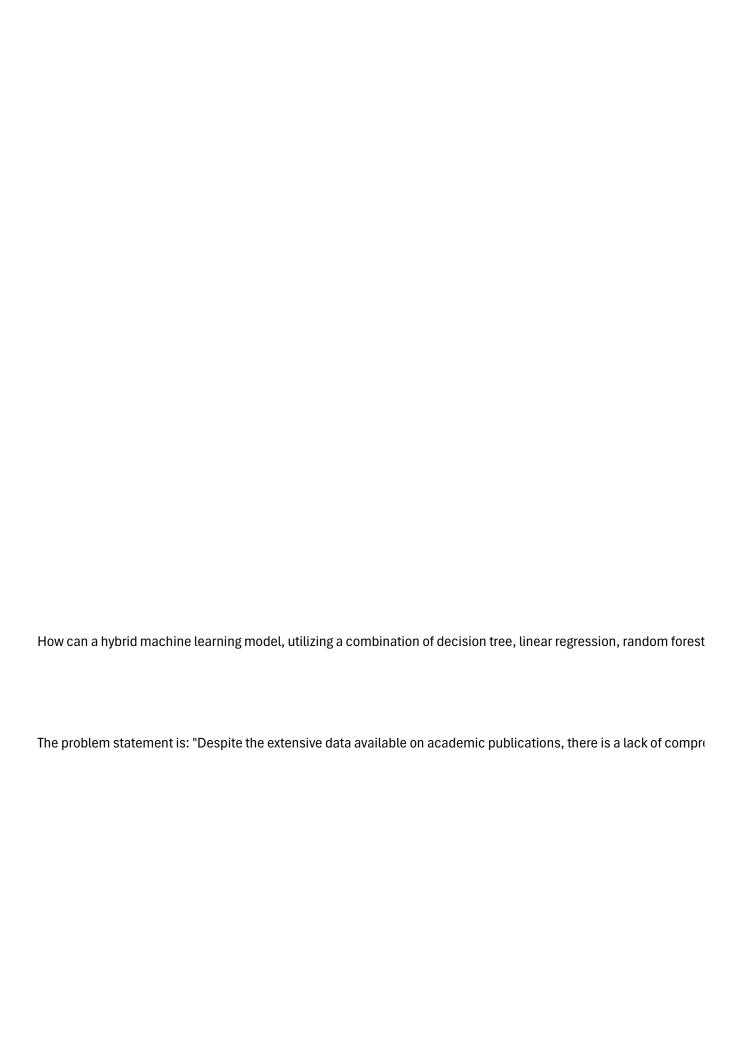
any)

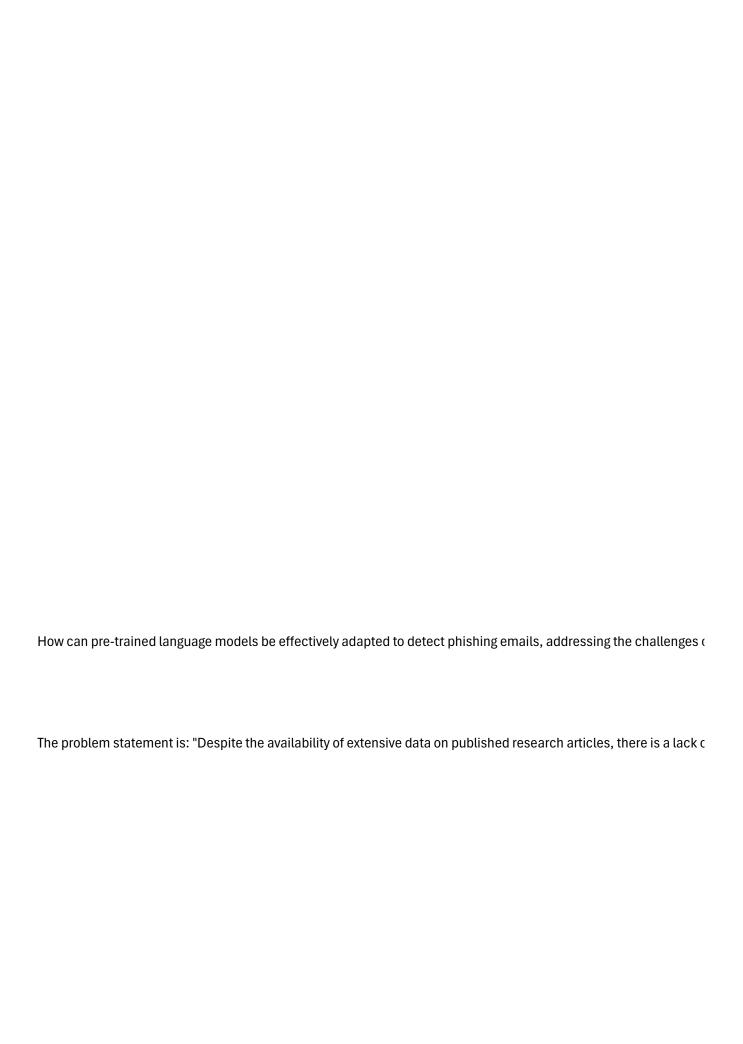
Limitation Critique

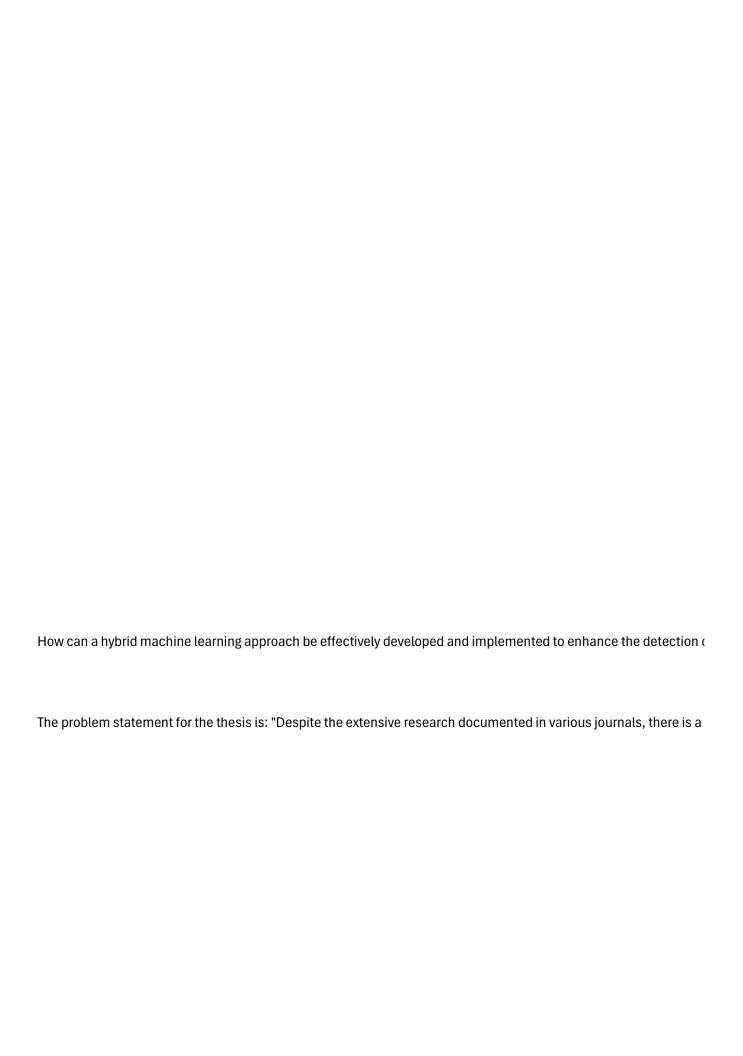
(if any)

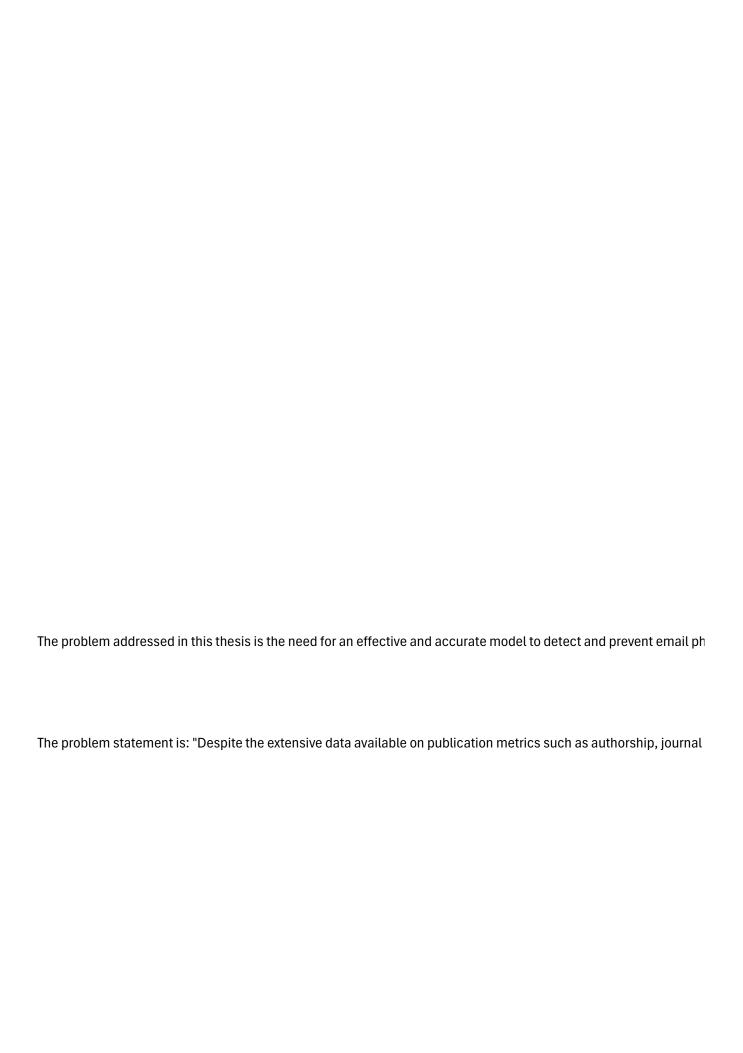
			The
			integratio
Tl	Directions		n of
The paper	include		multiple
reports	further		technique
improvem ents in	exploratio		s is
detection	n of	Potential	innovative
accuracy	scalability	high	yet the
and a	,	computati	paper
reduction	enhanced	onal costs	could
in false	adaptatio	and	benefit
positives compared	n to	hardware	
		demands;	
to	. •	lack of	•
conventio		extensive	
nal methods,	and	quantitati	
	potentially		deeper
but no		performan	discussio
explicit	computati	ce data	n
numerical	onal/hard		regarding
values are	ware		scalability
given	resource		and
J	demands		energy
			consumpt
			ion

The problem statement is: "Despite the availability of extensive data on academic publications, there is a lack of co
The problem is to improve the detection of phishing URL attacks by developing more robust machine learning mode
The problem statement for the thesis is: "Despite the extensive research documented in various journals, there is a

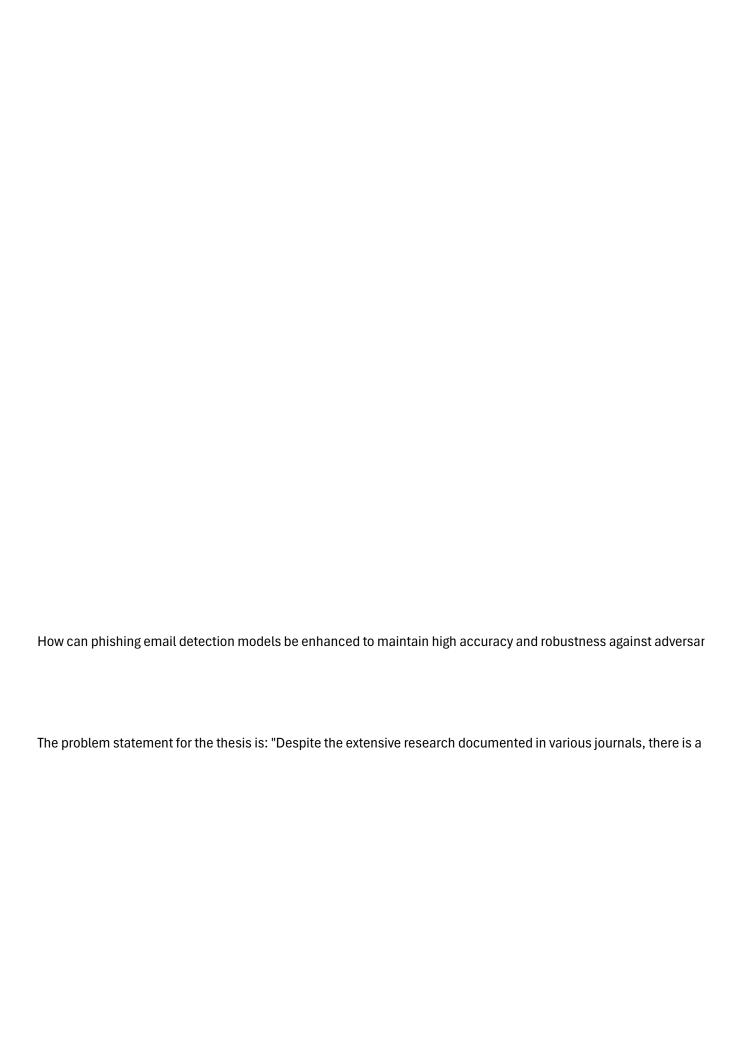


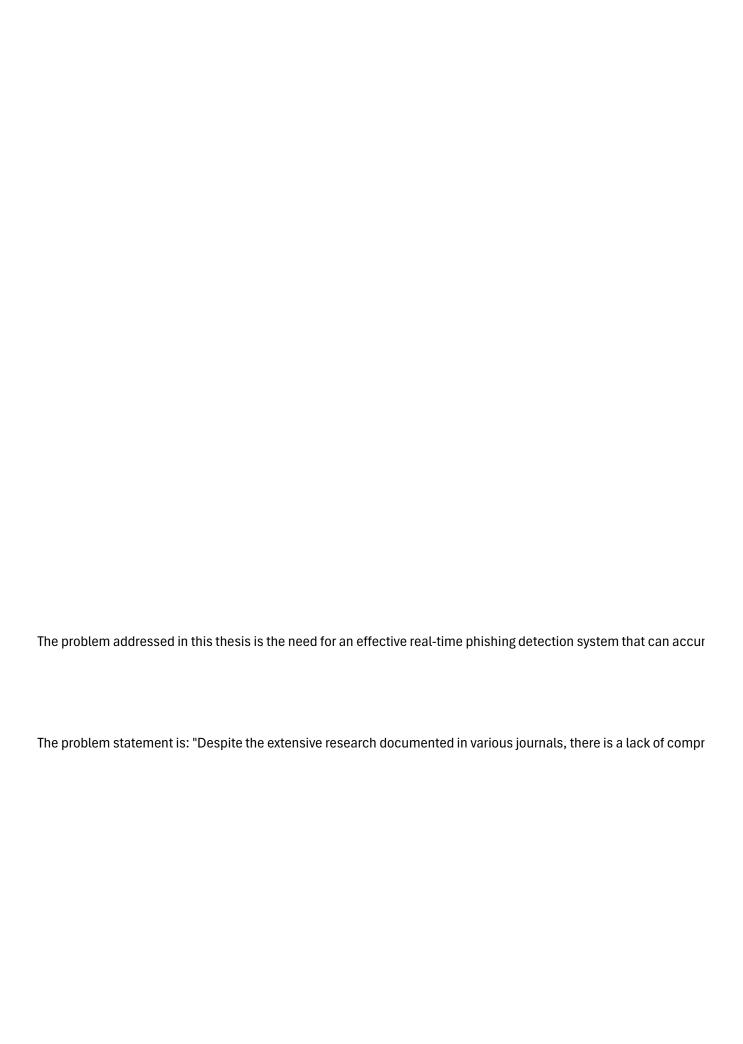


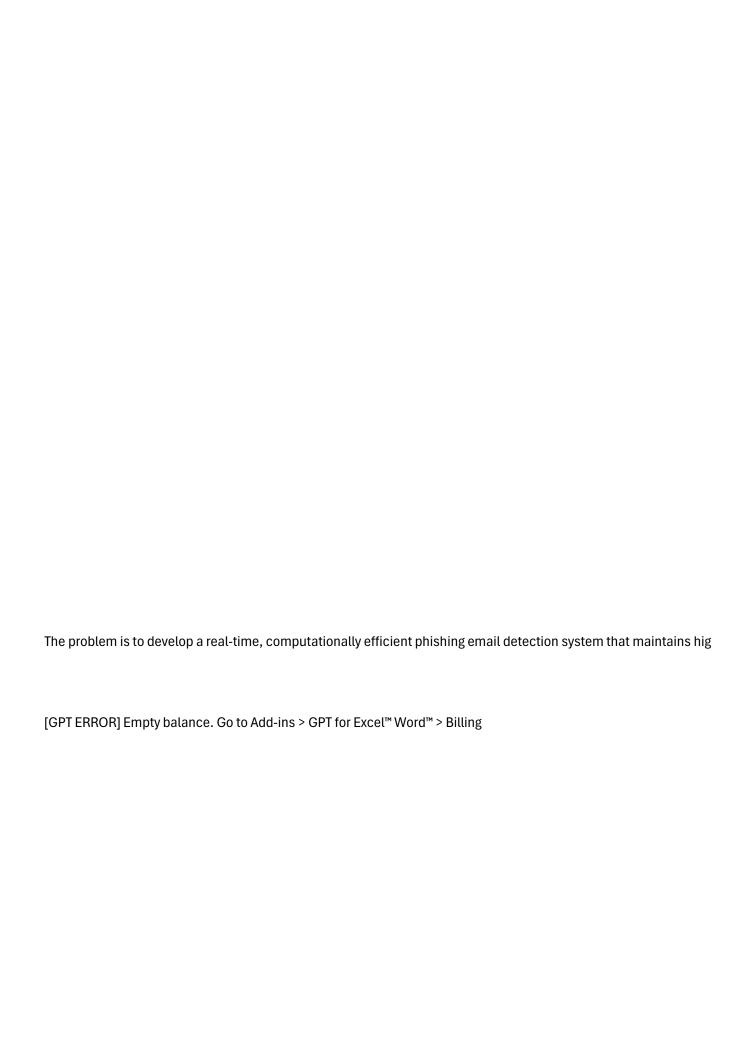


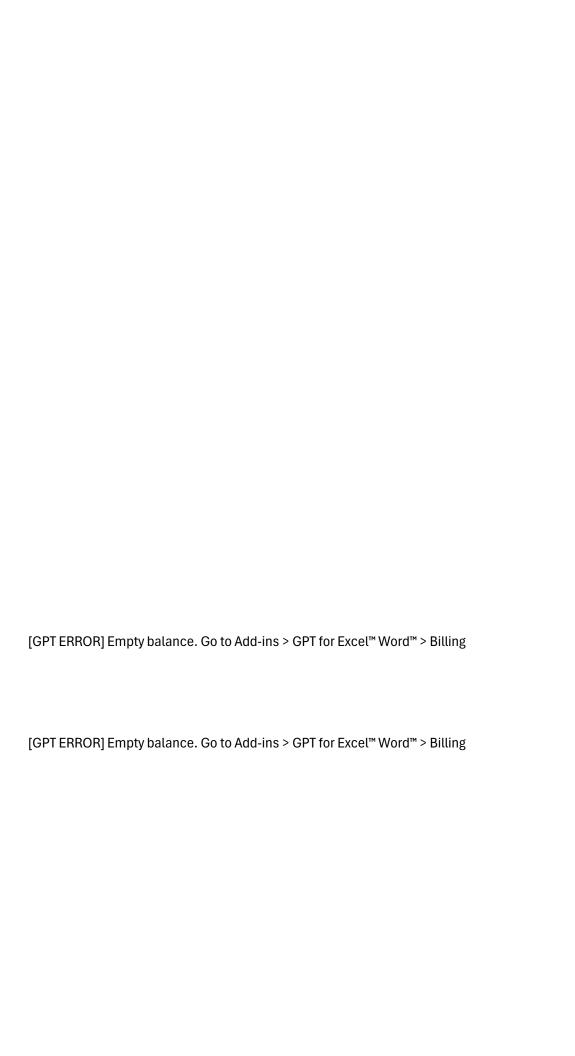




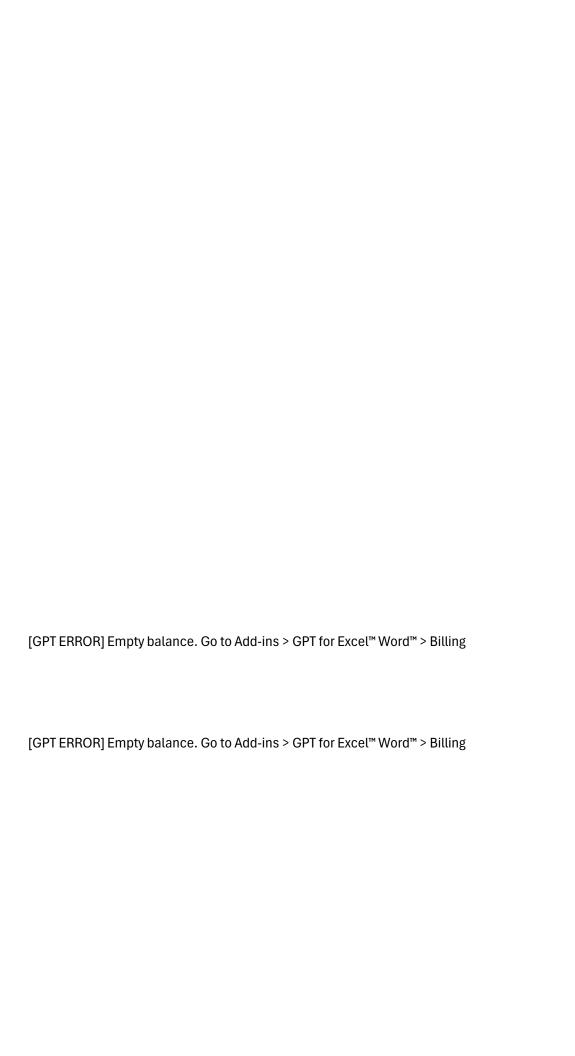














mprehensive analysis on the correlation between the methods used to solve problems and the performance me	trics
ls that can adapt to evolving phishing strategies, enhance feature extraction techniques, and validate findings a	cros
lack of comprehensive analysis on the effectiveness of different methodologies used to solve specific problems	, as





