RCNN BASED PHISHING EMAIL DETECTION USING DEEP LEARNING TECHNIQUES-DJANGO FRAMEWORK

[1]Ms. J Janisha, [2]Devendrakumar.R, [3]Deepakraj.S, [4]Dhanush.P, [5]Gampa Vikram Simha

[1]Assistant Professor, [2,3,4,5]Students
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research
Chennai, India-600073

***Abstract*- One of the biggest risks in the modern world is phishing emails, which have resulted in enormous financial losses. The current state of confrontation methods is not very satisfactory, even though they are continually being upgraded. Furthermore, the number of phishing emails has been alarmingly rising in recent years. Thus, to lessen the danger posed by phishing emails, more sophisticated phishing detection technology is required. First, we examined an email's structure in this essay. Next, we introduced a new phishing email detection model termed, which is used to simultaneously model emails at the character and word levels in the email body and email header. This model is based on the enhanced Recurrent Convolutional Neural Networks (RCNN) model with multilevel vectors and attention mechanism. To assess efficacy, we employ an imbalanced dataset.**

***Keywords*: phishing email detection, recurrent convolutional neural network (RCNN), email structure, threat mitigation, financial loss, email header, email body, character level, word level, multilevel vectors, attention mechanism.**

I. INTRODUCTION

The pervasive threat posed by phishing emails presents an ongoing challenge to cybersecurity on a global scale, imperiling the confidentiality and integrity of both personal and organizational data. These malicious communications, often masquerading as legitimate correspondence, are meticulously crafted to dupe recipients into divulging sensitive information or unwittingly executing harmful actions. Despite efforts to combat these deceitful tactics, traditional rule-based and heuristic approaches to phishing email detection have struggled to keep abreast of the evolving strategies employed by cybercriminals. Consequently, there is an urgent need for innovative solutions capable of swiftly and accurately discerning fraudulent emails in real-time.

In response to this imperative, our research endeavors to introduce a groundbreaking methodology for phishing email detection, harnessing the capabilities of deep learning techniques integrated within the Django Framework. This novel system represents a paradigm shift in the field, aimed at augmenting detection precision and resilience against sophisticated phishing endeavors. At its essence, the system leverages the formidable prowess of the Region-based Convolutional Neural Network (RCNN), enriched with multilevel vectors and an attention mechanism, to conduct a comprehensive analysis of email content and uncover malicious intent.

Diverging from conventional methodologies fixated on surface-level attributes like URL scrutiny or keyword matching, our approach plunges into the intricate structural and semantic dimensions of email discourse. By modeling emails across multiple strata—including header, body, character, and word levels—the system gains an intricate comprehension of contextual nuances indicative of phishing proclivities. This multifaceted analysis not only heightens detection accuracy but also endows the system with the agility to adapt to emergent phishing stratagems with dexterity. At the crux of our system's efficacy lies the integration of an attention mechanism, dynamically allocating focus to pertinent segments of email text during processing. This adaptive mechanism empowers the model to discern subtle aberrations and patterns signifying potential phishing endeavors, thereby amplifying detection sensitivity while curbing false positives.

Through methodical experimentation and comparative scrutiny against contemporary models employing cutting-edge techniques such as BERT (Bidirectional Encoder Representations from Transformers) and LSTM (Long Short-Term Memory), our proposed system showcases unparalleled performance in phishing email detection. These findings

underscore the formidable efficacy of deep learning methodologies, particularly RCNN coupled with attention mechanisms, in fortifying cybersecurity measures against the looming specter of phishing threats.
In summation, our research heralds a pioneering breakthrough in the realm of cybersecurity, furnishing a sophisticated yet accessible apparatus for mitigating the perils posed by phishing assaults. By harnessing the transformative potential of deep learning within the Django Framework, our proposed system represents a pivotal stride forward in safeguarding individuals and organizations against the insidious machinations of deceptive email communications.

II. Literature Survey

The literature survey encompasses a diverse array of studies that delve into the multifaceted landscape of cybersecurity, showcasing the innovative applications of machine learning and deep learning methodologies in fortifying defenses against evolving threats.

The first study, conducted by Dinil Mon Divakaran and Adam Oest, presents a comprehensive review of phishing detection methodologies, spotlighting the pivotal role of machine learning and deep learning models in combatting fraudulent emails. By leveraging large-scale data, their research underscores the importance of innovative approaches in accurately identifying phishing attacks, shedding light on various models built on different types of data and multiple deployment options.

Similarly, Ashit Kumar Dutta's study delves into the specific realm of detecting phishing websites, a prevalent threat in the era of electronic trading and online transactions. Dutta highlights the urgent need for intelligent techniques to safeguard users from cyber-attacks, particularly phishing attempts that exploit the visual resemblance between malicious and legitimate webpages. Employing machine learning approaches, Dutta proposes a URL detection technique utilizing recurrent neural networks, demonstrating superior performance in discerning malicious URLs from legitimate ones.

In a related vein, the study by Hossein Shirazi and Katherine Haynes tackles the escalating threat landscape posed by phishing attacks targeting mobile devices via SMS, social media, and gaming platforms. Their research introduces a lightweight phishing detection algorithm tailored for mobile devices, leveraging deep learning techniques to distinguish between legitimate and malicious URLs. Through meticulous evaluation, they underscore the feasibility of embedding phishing detection algorithms on mobile platforms, emphasizing the imperative for adaptive defences in the mobile ecosystem.

Expanding beyond the realm of cybersecurity, Marc Ribalta and Ramon Bejar delve into the domain of machine learning solutions applied to sewer systems. Their bibliometric analysis underscores the rising interest in leveraging machine learning to address predictive challenges in sewer infrastructure management, identifying existing gaps and opportunities for future research in this domain.

Moreover, Yuan Feng and Qihan Wang contribute to the discourse by presenting a machine learning-aided framework for fracture mechanics, offering a non-deterministic approach to damage prediction in 2D and 3D fracture problems. By integrating extended support vector regression with a phase field crack growth model, their methodology facilitates continuous damage diagnosis and prognosis, enhancing decision-making in structural engineering applications.

Collectively, these studies underscore the diverse applications of machine learning and deep learning methodologies acrossvarious domains, from cybersecurity to infrastructure management. Their findings provide valuable insights and inspiration for the proposed paper on "RCNN Based Phishing Email Detection Using Deep Learning Techniques - Django Framework," illuminating the novel approaches and methodologies that can be leveraged to enhance cybersecurity measures against phishing threats. Through a synthesis of these diverse perspectives, the proposed paper aims to contribute to the advancement of cybersecurity resilience in an increasingly interconnected digital landscape.

III. Methodology

The methodology proposed for the development of a phishing email detection system utilizing RCNN (Recurrent Convolutional Neural Networks) and deep learning techniques within the Django Framework follows a meticulously structured approach, delineated into several distinct steps.
Initially, the data collection phase entails gathering a diverse dataset comprising both phishing and legitimate emails, ensuring comprehensive representation across various sources and industries.

Following this, rigorous preprocessing techniques are applied to the dataset, encompassing tasks such as data cleaning, normalization, and tokenization, all aimed at preparing the data for subsequent model training.

Subsequently, feature extraction methodologies come into play, leveraging advanced techniques like TF-IDF and word embeddings to transform email text into numerical vectors, alongside the extraction of domain-specific features such as URL analysis and linguistic patterns indicative of phishing attempts.

The development of the model architecture is a pivotal stage, characterized by the integration of an RCNN design incorporating convolutional layers for feature extraction and recurrent layers for sequential modelling. This architecture is further enriched with multilevel vectors and attention mechanisms, strategically implemented to heighten detection accuracy.

Following model development, rigorous validation and hyperparameter tuning procedures are employed to optimize performance on a dedicated test set, with evaluation metrics including accuracy, precision, recall, and F1 score meticulously scrutinized.

Comparative analyses with alternative deep learning models and traditional techniques further enrich the evaluation process, providing valuable insights into the proposed system's efficacy.

Once validated, the model is seamlessly deployed in real-time within the Django Framework for phishing email detection, bolstered by continuous monitoring mechanisms to track performance and facilitate timely updates.

Lastly, iterative refinement processes are undertaken, incorporating user feedback and exploring advanced techniques such as transfer learning to ensure adaptability to evolving threats and sustained robustness over time.

This meticulously structured methodology underscores the systematic and comprehensive approach essential for addressing the multifaceted challenges of modern cybersecurity threats.

A. PROBLEM STATMENT

In today's interconnected digital realm, the ubiquitous presence of phishing emails has emerged as a paramount concern for both individuals and organizations on a global scale. These insidious phishing attacks, renowned for their deceptive tactics, are crafted with the malicious intent to deceive recipients into divulging sensitive information or unwittingly engaging in harmful activities, posing a dire threat to data security and integrity. Despite concerted efforts, traditional rule-based and heuristic methodologies employed in phishing email detection have revealed inherent limitations in keeping abreast with the evolving sophistication of such attacks. Consequently, there has been a notable surge in the prevalence of successful phishing attempts, underscoring the urgent need for more adaptive and accurate detection mechanisms. Existing detection systems often falter in their capacity to swiftly adapt to emerging threats, thereby underscoring the critical necessity for innovative and robust solutions capable of identifying and thwarting phishing emails in real-time.

In response to this escalating challenge, our paper endeavors to address this exigency by proposing an advanced phishing email detection system leveraging the prowess of RCNN (Recurrent Convolutional Neural Networks) and deep learning techniques, all encapsulated within the versatile Django Framework. By delving into a thorough comprehension of the intricate landscape of this pervasive problem, our research aspires to craft a sophisticated and streamlined solution. This solution seeks not only to bolster security measures against the evolving permutations of phishing threats but also to proactively safeguard both individuals and organizations from the nefarious consequences of deceptive email communications.

Through our exploration and where application of cutting-edge technologies, we strive to forge a path towards a safer digital environment, the risks posed by phishing attacks are diligently mitigated, thereby fostering trust and confidence in online interactions.

B. EXISTING SYSTEM

The current system employed for phishing email detection relies on the utilization of Support Vector Machines (SVM) grounded in deep learning methodologies. This system is structured around a series of preprocessing techniques designed to meticulously extract pertinent features from email data, encompassing crucial components such as email headers and body text. Subsequently, these extracted features serve as the foundation for training an SVM classifier, which is tasked with discerning subtle distinctions between phishing and legitimate emails by analyzing patterns inherent within the dataset. Moreover, to further refine the performance of the SVM classifier, the system integrates various optimization techniques, including feature scaling, kernel selection, and parameter tuning, aimed at enhancing the model's accuracy and efficacy in distinguishing between malicious and benign emails. In summation, the existing system capitalizes on the robust capabilities of SVM within the realm of cybersecurity to fortify email security measures, thereby bolstering defenses against phishing attempts through the automated detection and mitigation of potential threats.

Existing System Disadvantages:
The system's reliance on Support Vector Machines (SVM) may hinder its ability to adapt to evolving phishing tactics, potentially leading to decreased accuracy over time.

Relying heavily on predefined features during preprocessing may render the system less effective against novel phishing tactics that evade traditional feature extraction methods.

Despite mining text features from various email components, the system may struggle to grasp the contextual intricacies of phishing emails, affecting its ability to differentiate between legitimate and malicious messages accurately.

SVM-based systems are susceptible to adversarial attacks, where attackers manipulate input data to evade detection. This vulnerability undermines the system's effectiveness in mitigating phishing threats, as adversaries can exploit weaknesses in the model's decision-making process.

C PROPOSED SYSTEM

The proposed system introduces an innovative approach to phishing email detection, leveraging an RCNN model enhanced with multilevel vectors and an attention mechanism. This methodology enables the system to comprehensively analyze email content at various levels, including the header, body, character, and word levels. By examining emails at these granular levels, the system gains a deeper understanding of their contextual nuances, which is essential for accurate phishing detection. Furthermore, the incorporation of an attention mechanism allows the model to prioritize important segments of the email text, facilitating the identification of features indicative of phishing attempts. As a result, the system achieves remarkable accuracy in detecting phishing emails, surpassing the performance of existing state-of-the-art methods. Comparative analysis with models utilizing BERT and LSTM further reinforces the superiority of the proposed system, underscoring its effectiveness in enhancing security measures against phishing threats. In summary, the proposed system signifies a significant advancement in phishing email detection, offering a robust solution that harnesses the power of deep learning techniques to fortify security measures against phishing attempts.

Proposed System Advantages:
Multilevel Feature Modeling: Enables comprehensive understanding of email content by modeling emails at header, body, character, and word levels, enhancing detection accuracy.

Selective Attention Mechanism: Incorporates attention mechanism to prioritize crucial email components, aiding in the identification of phishing indicators and reducing false positives.
Superior Performance: Outperforms BERT and LSTM models in phishing email detection, showcasing the effectiveness of deep learning techniques in enhancing security measures against evolving threats.

IV. SYSTEM IMPLEMENTATION

Enhanced Data Collection and Preprocessing: Consider collecting a diverse dataset that includes emails from different sources, industries, and languages to improve the model's generalization capability. Implement advanced preprocessing techniques such as spell checking, entity recognition, and sentiment analysis to enrich the dataset and capture more contextual information.

Advanced Feature Extraction: Explore additional feature extraction techniques specific to phishing detection, such as lexical analysis of URLs, HTML content parsing, and analysis of attachment metadata. Consider incorporating domain-specific knowledge or external threat intelligence feeds to augment feature extraction and enhance model performance.

Optimized Model Architecture: Experiment with various RCNN architectures, including different configurations of convolutional and recurrent layers, to find the most suitable architecture for phishing email detection. Investigate the use of advanced attention mechanisms, such as self-attention or hierarchical attention, to further improve the model's ability to capture important email content.

Comprehensive Training and Validation: Implement robust cross-validation techniques to ensure the stability and reliability of model performance evaluation. Conduct extensive hyperparameter tuning and model optimization using techniques such as grid search, random search, or Bayesian optimization to maximize detection accuracy.

Thorough Evaluation and Comparison: Perform a comprehensive comparative analysis with a wide range of baseline models, including traditional machine learning methods, deep learning architectures, and ensemble techniques. Consider evaluating the model's performance under various scenarios, such as imbalanced datasets, adversarial attacks, and temporal drifts, to assess its robustness and scalability.

Real-time Deployment and Monitoring: Develop a scalable and efficient deployment pipeline for deploying the trained model in production environments, considering factors such as latency, scalability, and resource utilization. Implement comprehensive monitoring and alerting mechanisms to detect model degradation, data drift, and security vulnerabilities in real-time, ensuring continuous monitoring and maintenance of the system.

Iterative Continuous Improvement: Establish a systematic process for collecting feedback from end-users and domain experts to identify areas for improvement and prioritize future enhancements. Regularly update the model with new data, features, and techniques to adapt to emerging phishing threats and maintain effectiveness over time.

V. System Architecture

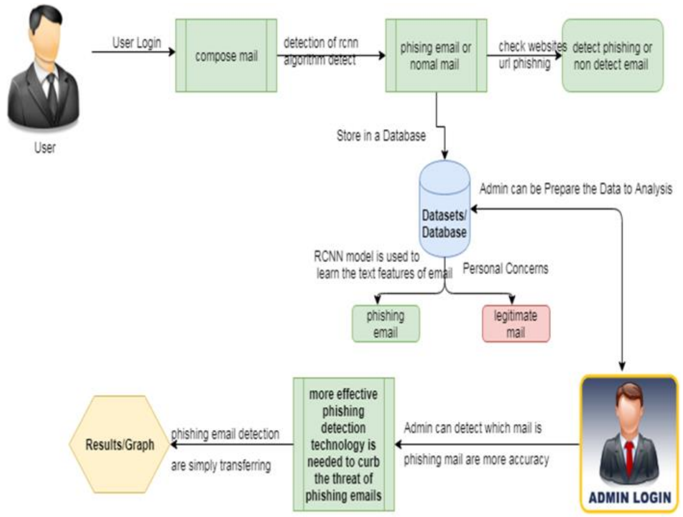

User
User Login
compose mail
detection of rcnn algorithm detect
phising email or nomal mail
check websites url phishnig
detect phishing or non detect email
Store in a Database
Datasets/ Database
Admin can be Prepare the Data to Analysis
RCNN model is used to learn the text features of email
Personal Concerns
phishing email
legitimate mail
Results/Graph
phishing email detection are simply transferring
more effective phishing detection technology is needed to curb the threat of phishing emails
Admin can detect which mail is phishing mail are more accuracy
ADMIN LOGIN

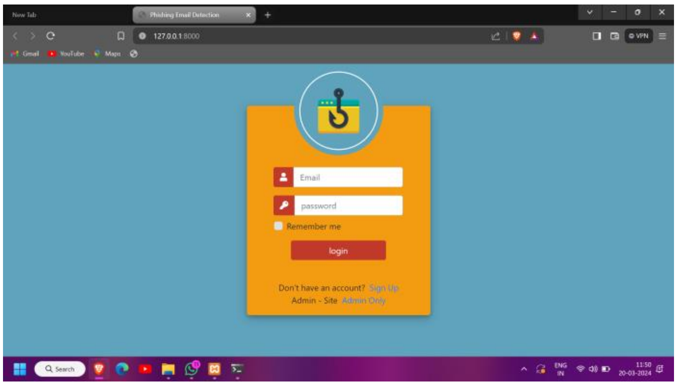
FIGURE 1: system architecture

Components:
User Login: This represents a login interface where users can enter their credentials to access the system.
Compose Mail: This functionality allows users to compose new emails, likely for analysis by the system to identify potential phishing attempts.
Phishing Email Detection Algorithm (RCNN Model): This is the core component responsible for identifying phishing emails. It likely utilizes a pre-trained RCNN model (e.g., Faster R-CNN or Mask R-CNN) to analyze emails and detect suspicious elements like URLs or urgency wording.
Datasets/Database**:** This represents the storage for the training data used to train the RCNN model. It likely contains pre-classified emails (phishing and legitimate) and their corresponding features.
Prepare Data for Analysis: This could involve preparing new email data for the RCNN model, potentially including feature engineering or data cleaning steps.
Admin Login: This provides a separate login for administrators to access the system's administrative functions.
Results/Graph (phishing email detection): This section allows admins to view the results of the phishing email detection process, possibly including visualizations of the model's performance or identified phishing attempts.

VI. Algorithm Used

R-CNN Algorithm: The R-CNN family encompasses a series of algorithms, including R-CNN, Fast R-CNN, and Faster R-CNN, each designed to tackle object detection tasks. In R-CNN, the process begins with the extraction of numerous regions from the input image using a technique called selective search. Subsequently, each region undergoes convolutional neural network (CNN) processing to extract specific features relevant to object detection. These extracted features are then utilized to identify objects within the regions. However, R-CNN's performance is hindered by its sequential nature, resulting in slow execution due to the involvement of multiple steps in the process. Fast R-CNN addresses this limitation by introducing a more efficient approach. It passes the entire image through a ConvNet, which directly generates regions of interest instead of relying on selective search. Moreover, Fast R-CNN streamlines the process by employing a single model for feature extraction, classification into different classes, and bounding box prediction, thereby significantly improving execution speed compared to R-CNN. However, despite its advancements, Fast R-CNN still faces challenges, particularly when applied to large datasets, as it continues to utilize selective search for region extraction, which can impact its efficiency.

VII. Results Analysis



Email

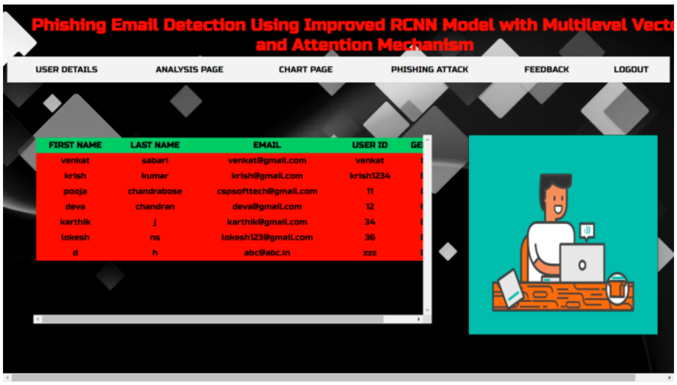
password

□ Remember me

Don't have an account? Sign Up
Admin - Site Admin Only

FIGURE 2: Login page

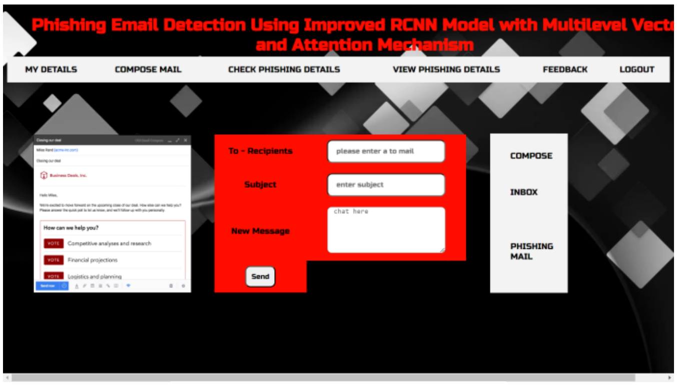
The image showcases the login interface of the proposed phishing email detection system, providing users with secure access to the platform. The login page features a clean and intuitive design, with fields for entering username and password credentials. Additionally, prominent login and registration buttons offer clear navigation options for users. The interface is designed with usability and security in mind, incorporating elements such as encryption indicators and error message prompts to enhance the user experience and protect sensitive information. With its user-friendly layout and robust authentication mechanisms, the login page exemplifies the system's commitment to providing a secure and accessible environment for users to combat phishing threats effectively.


Phishing Email Detection Using Improved RCNN Model with Multilevel Vect
and Attention Mechanism

FIRST NAME	LAST NAME	EMAIL	USER ID	GE
venkat	sabari	venkat@gmail.com	venkat	
krish	kumar	krish@gmail.com	krish1234	
pooja	chandrabose	cspsofttech@gmail.com	11	
deva	chandran	deva@gmail.com	12	
karthik	j	karthik@gmail.com	34	
lokesh	ns	lokesh123@gmail.com	36	
d	h	abc@abc.in	zzz	

FIGURE 3: Admin Interface

The image illustrates the administrative interface of the proposed phishing email detection system, offering administrators comprehensive control over system management and monitoring functionalities. The admin interface presents a dashboard overview displaying key metrics and analytics, providing insights into system performance and threat detection rates. Administrators can access various modules and features, including user management, data visualization tools, and configuration settings. Additionally, the interface incorporates interactive elements such as dropdown menus, buttons, and navigation panels for seamless navigation and interaction. With its intuitive layout and robust functionality, the admin interface empowers administrators to effectively oversee and optimize the system's operations, ensuring maximum efficiency and security in combating phishing threats.



Phishing Email Detection Using Improved RCNN Model with Multilevel Vect
and Attention Mechanism

FIGURE 4: User Interface

The user interface showcased in the image provides a user-friendly and intuitive platform for users to interact with the phishing email detection system. The interface offers a streamlined experience, featuring clear navigation menus, input fields, and action buttons for easy operation. Users can access essential functionalities such as uploading email samples, initiating phishing detection scans, and reviewing detection results. The interface incorporates informative prompts and tooltips to guide users through the process, ensuring smooth and efficient usage. Additionally, the design emphasizes visual clarity and responsiveness, optimizing usability across various devices and screen sizes. With its user-centric approach, the interface facilitates seamless interaction, empowering users to leverage the system's capabilities in identifying and mitigating phishing threats effectively.

VIII. Conclusion

We employ a novel deep learning model called "RCNN++" to address the challenge of phishing email detection. This model utilizes an enhanced RCNN architecture to meticulously analyze both the email header and body, operating at both the character and word levels. By adopting this approach, we aim to minimize noise within the model while ensuring a comprehensive understanding of the email content. Furthermore, our model incorporates an attention mechanism within both the header and body sections, enabling it to prioritize critical information during the detection process. To evaluate the model's efficacy, we conduct experiments using an unbalanced dataset that closely resembles real-world scenarios, yielding promising results. Additionally, we perform several experiments to illustrate the advantages of our proposed model in detecting phishing emails. Looking ahead, our future research will focus on further refining the model to effectively detect phishing emails lacking an email header and containing only an email body.

REFERENCES:

[1] N. Z. Harun, N. Jaffar, and P. S. J. Kassim, ‘‘Physical attributes significant in preserving the social sustainability of the traditional malay settlement,’’ in Reframing the Vernacular: Politics, Semiotics, and Representation. Springer, 2020, pp. 225–238.

[2] D. M. Divakaran and A. Oest, ‘‘Phishing detection leveraging machine learning and deep learning: A review,’’ 2022, arXiv:2205.07411.

[3] A. Akanchha, ‘‘Exploring a robust machine learning classifier for detecting phishing domains using SSL certificates,’’ Fac. Computer. Sci., Dalhousie Univ., Halifax, NS, Canada, Tech. Rep. 10222/78875, 2020.

[4] H. Shahriar and S. Nimmagadda, ‘‘Network intrusion detection for TCP/IP packets with machine learning techniques,’’ in Machine Intelligence and Big Data Analytics for Cybersecurity Applications. Cham, Switzerland: Springer, 2020, pp. 231–247.

[5] J. Kline, E. Oakes, and P. Barford, ‘‘A URL-based analysis of WWW structure and dynamics,’’ in Proc. Netw. Traffic Meas. Anal. Conf. (TMA), Jun. 2019, p. 800.

[6] A. K. Murthy and Suresha, ‘‘XML URL classification based on their semantic structure orientation for web mining applications,’’ Proc. Comput. Sci., vol. 46, pp. 143–150, Jan. 2015.

[7] A. A. Ubing, S. Kamilia, A. Abdullah, N. Jhanjhi, and M. Supramaniam, ‘‘Phishing website detection: An improved accuracy through feature selection and ensemble learning,’’ Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 1, pp. 252–257, 2019.

[8] A. Aggarwal, A. Rajadesingan, and P. Kumaraguru, ‘‘PhishAri: Automatic realtime phishing detection on Twitter,’’ in Proc. eCrime Res. Summit, Oct. 2012, pp. 1–12.

[9] S. N. Foley, D. Gollmann, and E. Snekkenes, Computer Security— ESORICS 2017, vol. 10492. Oslo, Norway: Springer, Sep. 2017.

[10] P. George and P. Vinod, ‘‘Composite email features for spam identification,’’ in Cyber Security. Singapore: Springer, 2018, pp. 281–289.

[11] H. S. Hota, A. K. Shrivas, and R. Hota, ‘‘An ensemble model for detecting phishing attack with proposed remove-replace feature selection technique,’’ Proc. Comput. Sci., vol. 132, pp. 900–907, Jan. 2018.

[12] G. Sonowal and K. S. Kuppusamy, ‘‘PhiDMA—A phishing detection model with multi-filter approach,’’ J. King Saud Univ., Comput. Inf. Sci., vol. 32, no. 1, pp. 99–112, Jan. 2020.

[13] M. Zouina and B. Outtaj, ‘‘A novel lightweight URL phishing detection system using SVM and similarity index,’’ Hum.-Centric Comput. Inf. Sci., vol. 7, no. 1, p. 17, Jun. 2017.

[14] R. Ø. Skotnes, ‘‘Management commitment and awareness creation—ICT safety and security in electric power supply network companies,’’ Inf. Comput. Secur., vol. 23, no. 3, pp. 302–316, Jul. 2015.

[15] R. Prasad and V. Rohokale, ‘‘Cyber threats and attack overview,’’ in Cyber Security: The Lifeline of Information and Communication Technology. Cham, Switzerland: Springer, 2020, pp. 15–31.

[16] T. Nathezhtha, D. Sangeetha, and V. Vaidehi, ‘‘WC-PAD: Web crawling based phishing attack detection,’’ in Proc. Int. Carnahan Conf. Secur. Technol. (ICCST), Oct. 2019, pp. 1–6.

[17] R. Jenni and S. Shankar, ‘‘Review of various methods for phishing detection,’’ EAI Endorsed Trans. Energy Web, vol. 5, no. 20, Sep. 2018, Art. no. 155746.

[18] (2020). Accessed: Jan. 2020. [Online]. Available: https://catches-of-themonth-phishing-scams-for-january-2020

[19] S. Bell and P. Komisarczuk, ‘‘An analysis of phishing blacklists: Google safe browsing, OpenPhish, and PhishTank,’’ in Proc. Australas. Comput. Sci. Week Multiconf. (ACSW), Melbourne, VIC, Australia. New York, NY, USA: Association for Computing Machinery, 2020, pp. 1–11, Art. no. 3, doi: 10.1145/3373017.3373020.

[20] A. K. Jain and B. Gupta, ‘‘PHISH-SAFE: URL features-based phishing detection system using machine learning,’’ in Cyber Security. Switzerland: Springer, 2018, pp. 467–474. [21] Y. Cao, W. Han, and Y. Le, ‘‘Ant