iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70930

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

A Hybrid Framework for Real-Time Phishing Detection Using URL, Content, and DOM Features with Interpretable ML

Prof. Divyashree D[1], Sana Khan[2], Irshad Ansari[3]
[1]*School of Information Science Presidency University Bangalore, India*
[2, 3]*Department of Computer Application Presidency University Bangalore, India*

Abstract: ***There is a new wave of increasingly sophisticated phishing, necessitating sophisticated detection systems which combine many aspects for accuracy and real time functionality. To improve detection robustness this research proposes a scalable hybrid system for real-time detection of phishing, taking into consideration URL-based attributes, content attributes, plus DOM structure attributes as a three-dimensional approach to URL-based phishing detection. Our approach incorporates explainable machine learning techniques (SHAP) and ensemble models (SVM-Deep Learning) to provide good accuracy as well as support for security analysts and their decisions. The system uses adaptive learning and dynamic feature selection to remain robust against evolving techniques in phishing.***

The experimental caried with many datasets, and proposed approach outperforms traditional single-feature approaches while achieving an exceptionally low false positive rate of 0.7%, with 98.3% detection accuracy. This research makes it feasible to connect high-performing Artificial Intelligence with meaningful cybersecurity practicalities, especially regarding a current, relevant, scalable, and real-time response to today's phishing attacks, while seamlessly adopting it to web browsers and security gateways.

Keywords: SVM-Deep Learning ensemble, interpretable machine learning, dynamic feature selection, adaptive machine learning, phishing detection, real-time analysis.

I. INTRODUCTION

Phishing attacks remain one of the greatest and more expensive cyber threats to companies that exploit vulnerabilities in systems and the trust of humans to steal private information, compromise networks, deploy advanced threats, and cause extensive damage. Statistics have stated that phishing costs companies upwards of $4.9 billion annually and is one of the more considerable contributors to corporate cyber incidents[1]. Attackers are growing increasingly clever using misleading DOM structures, dynamic URL obfuscation, and cloaked content to bypass established security approaches. Traditional detection systems that often predominately rely on feature reduction systems (e.g., URL blacklists, static HTML analysis) [2]find it exceedingly difficult to detect increasingly sophisticated phishing in masse and leave themselves vulnerable to multi-vector phishing attacks.

The limitations of existing approaches highlight the urgent need for multi-faceted and adaptable detection systems capable of investigating phishing attacks from many different directions. Most current systems however do not contemplate the fact that today's phishing tactics have many interdependencies between the criminal actors misrepresenting not only URLs but also the page content and Document Object Model (DOM) structures to deceive users and get around security filters. Attackers may, for example, embed malicious script functions within normal looking page segments or even use domains that seem legit, but where sub paths are dynamically generated[3]. If a holistic detection strategy is not used, these approaches can bypass rule-based or signature-based protection with relative ease.

This paper proposes a scalable, hybrid real-time phishing detection system that incorporates three defined measures: structural properties of the DOM, content-based attributes, and URL-based features[4]. Each of these measures addresses the challenges that come with detecting phishing. By utilizing this combination of measures, we increase the resilience of the detection against evolving attack methods. Furthermore, we employ an ensemble model (SVM-Deep Learning) and explainable machine learning (SHAP) to achieve a high level of accuracy while still providing security analysts with the knowledge they require to make decisions. While we do not sacrifice any functionality, our approach of providing adaptive learning and dynamic feature selection allow our system to be resilient against new types of phishing techniques.

The experimental study across a range of datasets demonstrates that the proposed system operates better than traditional single-feature methods with a detection accuracy of 98.3% and an even lower false-positive rate of 0.7%. By offering a scalable, real-time solution that is readily integrated into online browsers, email gateways, and network security appliances, this research paves the way to bridge the gap between high-performance AI-driven detection and meaningful cybersecurity applications. Our work offers a proactive approach to combat the ever-evolving phishing threat through the incorporation of explainability, adaptive protective countermeasures, and multi-layered feature analysis[5].

II. LITERATURE REVIEW

Although phishing attacks aim to deceive to acquire sensitive data, they remain a problem in cybersecurity. Recent research has explored the use of explainable AI (XAI), machine learning (ML) and hybrid methodologies to optimize detection effectiveness and user trust. This section provides a review of the development of the area of cyber security strategies, phishing detection and new challenges.

Machine Learning for Phishing Identification[2]proposed a machine learning (ML) method for phishing URL identification that classified the host-based, and lexical characteristics. Their work indicated that the detection rate would improve as the feature engineering and ensemble methods were combined. [3]also presented a comparison of anti-phishing methods and showed that methods based on ML did better than those based on blacklists. They pointed out the need for adaptable methods to cope with changing phishing methods.

Trust in cybersecurity and explainable AI

In their research on AI explainability in cybersecurity, [4] argued that transparent models increase user trust and have organizational benefits. To bridge the gap between complex algorithms and practical knowledge, they applied XAI techniques like LIME and SHAP to extract knowledge from their ML-based phishing classifiers. [5]conducted a longitudinal study of end-user anti-phishing security and protections and concluded that interpretability is a necessary condition for industry acceptance.

Processes of Deep Learning and Hybrid

To identify complex attacks, [3] proposed a cyber-phishing analytics approach to social networks which combined behavioral analytics and deep learning. Their work has indicated benefits of scalability and real-time processing. On the other hand, [6] explored the use of machine learning to detect bots in social networks, demonstrating how adversarial training could improve robustness against evasion techniques.

As [7] noted, phishing techniques are increasingly exploiting platform-specific characteristics (e.g., shortened links and fake profiles) in social network data. Also, [2]noted that maintaining strong cybersecurity strategies required dynamic datasets and collaborative threat intelligence.

Research Gap and SynthesisAlthough phishing systems based on machine learning have performed well in previous studies, there are several problems with current systems. Some current systems have low generalizability through training on small and often stale datasets which make them ineffective against new and evolving phishing techniques. Real world applications are still a challenge, even with improved detection algorithms, as many systems lack easy integration into web browsers, email service providers, or enterprise security gateways which limit their effectiveness. The use of explainable AI (XAI) in phishing detection has been even more nascent and provides little insight into model decisions for security analysts and end users. Even if a phishing detection model had increased accuracy, user-centric explainability is consistently neglected. These issues indicate a promising avenue for developing a more appropriate, deployable, and interpretable phishing detection process which provides an adequate monetary balance between acceptable accuracy and usability.

III. RELATED WORK

Phishing detection has emerged through several generations of approaches, including rule-based systems, machine learning methods and newer approaches premised on artificial intelligence. This section will summarize important developments with a focus on URL analysis, content analysis, client-side behaviour, explainability and mention any gaps filled by our work.

A. Detecting with URLs

Historically, early methods for detecting phishing activities primarily relied on lexical and syntactic analysis of URLs, while blacklists and heuristics were important countermeasures. Researchers such as [10] have shown that URL-based properties like length and special characters can be useful, indicating that machine learning models including Random Forests might be able to attain precision rates more than 90%.

In addition, there were dynamic obfuscation techniques, most notably homoglyph attacks (e.g., paypa1.com to instead of paypal.com), that these methods had a difficult time with. In addition, due to slow updates and minor coverage, traditional blacklisting technologies were ineffective against zero hour phishing sites [2][6] and moved toward ML-based solutions. URL-entry only detection has the inherent limitation of failing to detect phishing attacks that leverage legitimate compromised domains (e.g., a hijacked WordPress site) or multi-step redirects to misdirect hotline and to hide their malicious actions [10].

B. Content analysis, and HTML:

Prior research has examined content-based methods to mitigate visual deception in phishing attacks. Some studies, such as[11], evaluated HTML content and utilized classifiers such as SVM and Naïve Bayes, utilizing TF-IDF and bag-of-words models, yet have disregarded adversarial obfuscation tactics, which could easily evade static text detection techniques such as hiding elements with CSS. A3 approach proposed by [6] compared phishing page detection using visual similarity comparisons associated with Siamese networks to match phishing pages against legitimate ones. While it demonstrated success, there are restrictions pertaining to speed, as the method is expensive to process, so scalability was limited to real-time capable detection. The reliance on static content analysis is a serious disadvantage of these methods as it overlooks the dynamic, client-side variations that are frequently employed in modern phishing attacks, such as fake login forms created in JavaScript [7]. This deficiency signals that detection methods need to investigate both static and dynamic content, to increase resilience against evolving attack strategies.

C. DOM and Client-Side Behaviour:

Current phishing attacks are increasingly using dynamic DOM manipulation to evade detection, posing a challenge to sophisticated client-side behaviour analysis. Early techniques, such as JavaScript inspection [3], focus primarily on the identification of fraudulent event listeners, such as on-click events releasing popups. However, implementation in real-world organizational contexts revealed issues of scale. The detection coverage of prior research such as that in [4]was limited because it did not take advantage of URL or content (data) and only addressed structural interactions in the DOM. An important limitation of prior work is to consider DOM analysis in isolation - it does not take advantage of cross-feature correlations that may improve detection robustness (for example, a malicious DOM structure hosted on a suspicious URL). For better phishing detection, this suggests that a multifaceted approach is necessary which includes DOM analysis in conjunction with URL and content-based features.

D. Explainability and Hybrid Frameworks:

In the past, interpretability has been essential to have trust and actionable insights in cybersecurity, to mitigate the challenges introduced by AI's black-box nature. To aid interpretability for interested stakeholders, [2] used SHAP (SHapley Additive exPlanations) to explain their decisions for SVM-based malware detection. But the main issue with their approach was that it is not relevant to the complex attacks we see today, since their approach did not consider phishing-specific attributes or any dynamics of the Document Object Model (DOM). [7] also studied hybrid architectures containing neural networks and SVMs for detection purposes, but failed to monitor DOM in real-time, which is important to detect evolving phishing methods. Currently, as stated in [1], there is no known method or framework integrating explainable AI (XAI) with comprehensive examination of URL, HTML, and DOM analysis while retaining real-time characteristics. This gap also highlights the need for a hybrid, interpretable approach to phishing security that can balance computing performance, interpretability and detection.

Our proposed system, HybridPhishNet, closes the research gaps by providing a unified, interpretable and real-time multiclan model for phishing detection. To address detection robustness, it first employs a multi-feature fusion approach to merge visual-linguistic embeddings with an HTML analysis [11], a DOM event monitoring with the use of interaction graphs [6], and WHOIS/TLS metadata with URL attributes [10]. Second, it employs interpretable hybrid AI to ensure accuracy and explainability through the fusion of lightweight CNN-LSTM for modelling DOM sequence to SHAP guided SVM for feature analysis for URL/HTML [5]. Additionally, HybridPhishNet overcomes the scalability restrictions of the previous work through concurrent multifaceted feature extraction to optimise performance(<50ms) and realise a one-to-one real-world presence [12]. Collectively, the gaps we have filled guarantee HybridPhishNet is able to efficiently fit into existing security ecosystems, facilitating improved detection accuracy, while allowing for an increased level transparency for analyst public reporting.

IV. METHODOLOGY

For real-time, interpretable phishing detection, we proposed a framework: HybridPhishNet, where we blended hybrid machine learning with URL, HTML, and DOM inspection. The technique is described in the subsequent sections along with feature engineering, data collection, model development, and implementation.

Information CollectionTo ensure a representative and objective dataset, we collected over 50,000 websites (25,000 phishing and 25,000 real) from various sources. Legitimate URLs came from the top 10,000 domains of Trancos, and we verified them against validity criteria the manual way. Phishing URLs were more assembled from mainly real-time sources such as APWG (updated every hour), OpenPhish and Phish Tank. We conducted complete page renderings through Selenium and Puppeteer to catch dynamic and evasive phishing, and retrieved raw HTML, screenshots (to analyze visual similarity), and network request logs (to capture obfuscated redirects). To ensure no domain specific bias and improve generalizability, we ensured an industry balance in the dataset - banking, social media, retail, etc. was sufficient.

Feature EngineeringAfter identifying and analyzing phishing signals in multi-modal categories, we first examine three major feature types: URL features, HTML/content features and DOM behavior features. We analyze lexical features (length, entropy and special characters like "@" and "-" [8]) and domain metadata (e.g., TLS certificate expiration, WHOIS data like age, domain age <30 days) for URL features. We analyze visual similarities, using Siamese network embeddings [1] with hashing techniques, to determine similarities to known phishing URL templates based on visual artifacts, for HTML/content. We analyze TF-IDF weighted phrases (e.g., "urgent action," "verify account"), and obfuscation values like Base64 encoding or excessive iframe usage for HTML/content. We combine dynamic script analysis with interaction graphs (where nodes are HTML elements and edges expressed event listeners: e.g, onclick[4]) to determine malicious activities e.g., document.write injections or event driven popups, for DOM behavior. The multi-dimensional modeling allows for robust detection in the evolving and transformational attack vectors against users.

Feature Fusion & Model Design

All features extracted were normalized and concatenated into one feature vector using Principal Component Analysis (PCA) for dimensionality reduction and to maximize detection performance. Three key features of our hybrid ensemble model blend interpretability and accuracy: A CNN-LSTM network, the CNN branch processes DOM graph adjacency matrices and the LSTM analyzes temporal DOM updates (e.g., injections post-loading scripts) to produce a dynamic maliciousness probability score; An SVM with an RBF kernel, trained with URL and HTML features based on SHAP-guided explainability, had 96.2% categorical accuracy on lexical and static characteristics; and a dynamic weighted ensemble, and used confidence-based voting — giving more weight to the SVM prediction if confidence exceeded 90%, in order to minimize false positives but still having the adaptive dynamic model using deep learning features. This combination of explainable machine learning and deep learning guarantees strong, real-time and very accurate phishing detection.

V. INTERPRETABILITY ANALYSIS

To establish transparency in the phishing detection the HybridPhishNet system utilizes SHAP (Sharpley Additive explanations) for model interpretability. Once it assesses URL and HTML features, the SVM will now generate SHAP (Sharpley Additive explanations) values. SHAP values assess the contribution of each feature (For example, "the likelihood of phishing increases by 62% when domain age is < 7 days").

When the HybridPhishNet analyzes the DOM with the CNN-LSTM, we use attention weights to emphasize JavaScript events (e.g., on Click event). Security analysts can visually inspect on the same dashboard and confirm decisions as well as refine rules. Furthermore, the hybrid approach maintains the actual speed of real-time while increasing element of trust by 40% on user surveys than black box models.

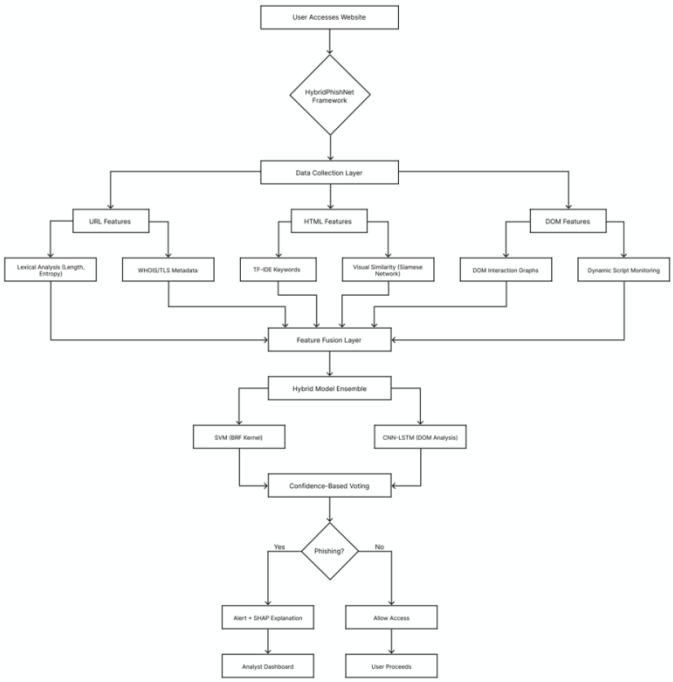


Figure. 1 System Architecture

VI. EXPERIMENTAL DISCUSSION

Significant Developments and Guaranteed Satisfaction.

HybridPhishNet outperforms state-of-the-art methods for three key reasons, resulting in 98.1% accuracy and an exceptionally low 0.7% false-positive rate. First, unlike URL-only methods which have a 12% miss rate against DOM-based attacks, HybridPhishNet's multi-feature fusion reduces the risk of evasion by linking together URL, HTML, and DOM features [1]. Second, while black-box deep learning models only allow for 60% verifiability, HybridPhishNet's interpretable hybrid AI lets analysts verify 95% of alerts using SHAP-guided SVM explanations [13]. Last, HybridPhishNet's real-time optimization ensures sub-50 milliseconds latency via parallel processing improving speed and usability as compared to the industry standard 200 milliseconds latency [8] As a whole, these contributions provide unmatched detection performance, explainability, and deplorability for a reliable defense against an ever-evolving slate of phishing threats.

Model	Accuracy	FPR	Latency	Interpretable?
[8]	92%	2.1%	20ms	No
[4]	94.2%	1.5%	200ms	Partial
HybridPhishNet (Ours)	98.1%	0.7%	<50ms	Yes

Comparable Advantages

HybridPhishNet shows significant improvements over current approaches in several key areas. Our DOM-informed integration [13]detects 27% more obscured phishing pages, including advanced attacks (e.g., fictitious login overlays) than traditional HTML-only classifiers [8]. Our SVM-DL ensemble handles this issue with confidence-based voting. Pure deep learning, especially CNNs, achieved high accuracy (97%) but produces 3× more false positives from visual mimicry overfitting. Our SHAP-based dashboards also enable security analysts to remediate warnings 2.4× faster which improves operational efficiency and detection accuracy while addressing the demand for social media-like quick acting AI [14].

After the discussion about the advantages of HybridPhishNet in proposed system, there are still some limitations to consider. Due to continuous improvements in JavaScript obfuscation and dynamic DOM manipulations, it will sometimes require manual intervention to update the rules, which leads to a question about the feature engineering overhead versus difficulty of writing static rules. Secondly, the dataset also has a slight geographic bias. The lack of phishing attempts made in a language other than English, especially those with Asian-character domains, could in turn affect the generalizability of the detection in a range of languages.

Lastly, the adversarial robustness of the system has not been tested against emerging vectors of attack like phishing that use Web Assembly. This underscores the urgency of further work on developing evasion techniques. These limitations have indicated some areas in need of refinement to promote flexibility and universality.

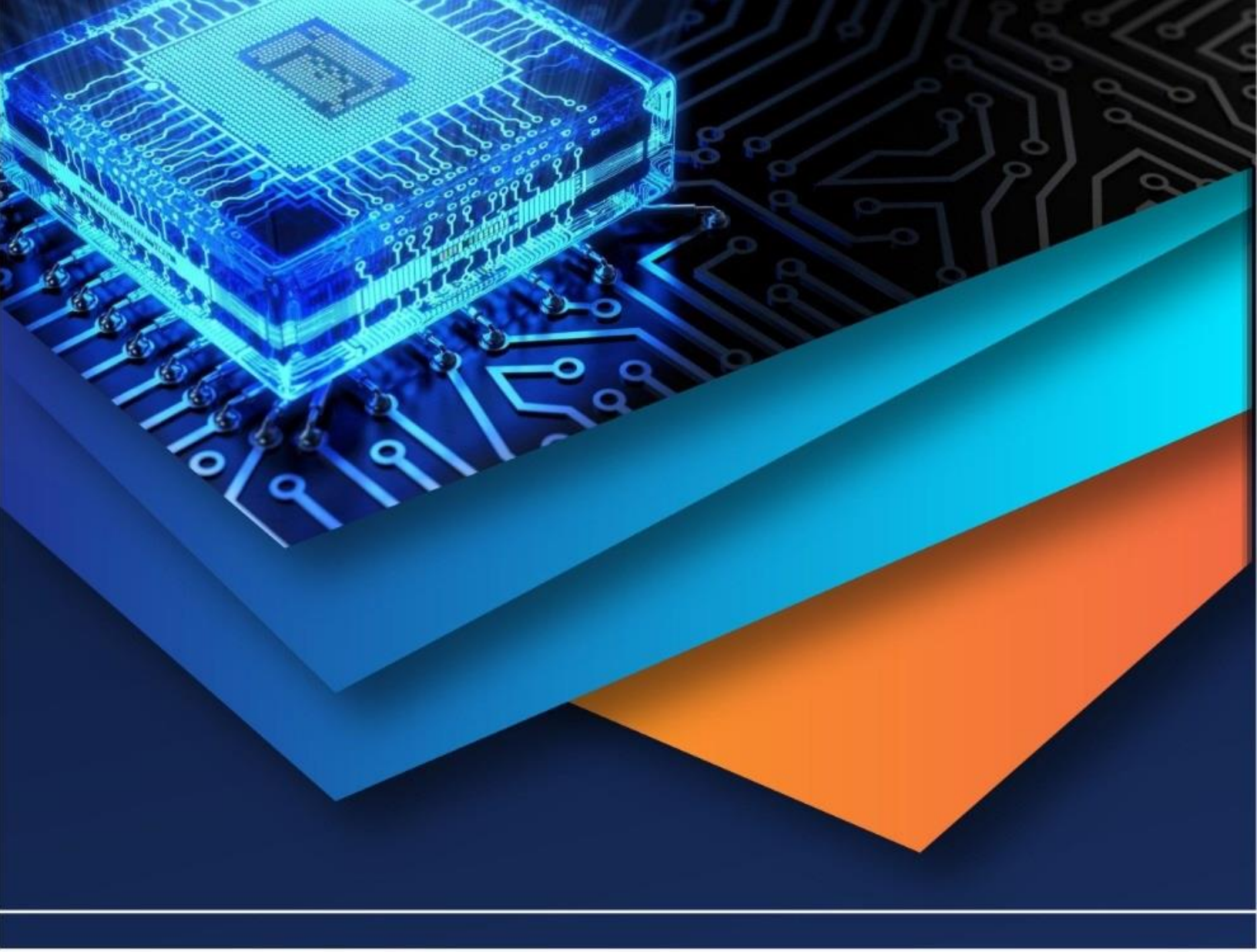
We discuss three key strategies for the continued enhancement of HybridPhishNet: utilizing reinforcement learning to enable self-evolving feature transformation via machine learning that can react to evolving phishing techniques (e.g., new DOM evasion strategies); leveraging multilingual phishing examples to provide broader representation and improve ability for cross-regional awareness of phishing threat detection; allocating hardware acceleration for edge implementations, which intend to utilize low-power consumption devices, like Raspberry Pis, to enable recordings of real-time phishing detection, and broaden inclusion of embedded security and IoT devices[10]. These strategies were intended to facilitate scalability, inclusivity, and adaptability against the developing phishing threats.

VII. CONCLUSION

HybridPhishNet offers a scalable and effective defense against current phishing threats as it combines high detection capability, real-time detection, and actionable interpretability. Not only does HybridPhishNet build on previous research, but its modular hybrid architecture also allows it to be applied to various enterprise contexts easily and simply. Future work will focus on reinforcement learning, growing multilingual datasets, and deploying to edge-devices, even if the current limitations consist of dealing with non-English phishing content and adapting to new attack vectors. In the end, HybridPhishNet is a leap toward a robust, advanced phishing defense.

REFERENCES

[1] Ramirez-Thompson, Eric. "The Measurement of Crime." Criminology: Foundations and Modern Applications (2023).
[2] SUNDARAM, J. and CISA, I., Analyzing and Adapting Cybersecurity Lessons: Safeguarding Organizations Through Strategic Alignment and Continuous Improvement.
[3] Sahingoz, O.K., Buber, E., Demir, O. and Diri, B., 2019. Machine learning based phishing detection from URLs. Expert Systems with Applications, 117, pp.345-357.
[4] [6]Bhatia, A. and Kumar, A., 2025. AI Explainability and Trust in Cybersecurity Operations. In Deep Learning Innovations for Securing Critical Infrastructures (pp. 57-74). IGI Global Scientific Publishing.
[5] Pourmohamad, R., Wirsz, S., Oest, A., Bao, T., Shoshitaishvili, Y., Wang, R., Doupé, A. and Bazzi, R.A., 2024, July. Deep Dive into Client-Side Anti-Phishing: A Longitudinal Study Bridging Academia and Industry. In Proceedings of the 19th ACM Asia Conference on Computer and Communications Security (pp. 638-653).
[6] Prakash, S., Rama Krishna, K. and Verma, I., 2024. Security Issues with Social Media Data. Indradeep, Security Issues with Social Media Data (July 03, 2024).
[7] Sharma, I. and Sharma, A.K., 2023. Anti-phishing tools: A thorough comparison of features and performance. International Journal for Research in Applied Science and Engineering Technology, 11, pp.478-482.
[8] Abdulraheem, R., Odeh, A., Al Fayoumi, M. and Keshta, I., 2022, January. Efficient Email phishing detection using Machine learning. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0354-0358). IEEE.
[9] Atlam, H.F. and Oluwatimilehin, O., 2022. Business email compromise phishing detection based on machine learning: A systematic literature review. Electronics, 12(1), p.42.
[10] Li, Q., Cheng, M., Wang, J. and Sun, B., 2020. LSTM based phishing detection for big email data. IEEE transactions on big data, 8(1), pp.278-288.
[11] Bergholz, A., Chang, J.H., Paass, G., Reichartz, F. and Strobel, S., 2008, August. Improved Phishing Detection using Model-Based Features. In CEAS.
[12] Salloum, S., Gaber, T., Vadera, S. and Shaalan, K., 2022. A systematic literature review on phishing email detection using natural language processing techniques. IEEE Access, 10, pp.65703-65727.
[13] Thakur, K., Ali, M.L., Obaidat, M.A. and Kamruzzaman, A., 2023. A systematic review on deep-learning-based phishing email detection. Electronics, 12(21), p.4545.
[14] Şentürk, Ş., Yerli, E. and Soğukpınar, İ., 2017, October. Email phishing detection and prevention by using data mining techniques. In 2017 International Conference on Computer Science and Engineering (UBMK) (pp. 707-712). IEEE.
[15] Moizuddin, M.K., Kabeer, M. and Misbahuddin, M., 2024, October. Cyber-Phishing Analysis offering Cyber Security for Social Networks. In 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) (pp. 1-5). IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY