Multi-Channel Phishing Detection Using Machine Learning, Deep Learning, and Behavioral Analysis

Shraddha Rajendra Bairagi[1], Shruti Pravin Bhangale[2], Aditya Dattatray Bhagwat[3], Asim Minaz Kazi[4], Archana L Rane[5], Pooja S Kurne[6]

[1,2,3,4,5,6]*Department of Computer Applications, K.K. Wagh Institute of Engineering Education and Research*

Abstract- ***Phishing attacks have become more sophisticated over time, evolving from simple email scams into complex threats that operate across multiple communication channels. Today, attackers use platforms such as SMS, voice calls, social media, DNS, and QR codes to exploit both technical weaknesses and human behavior, making these attacks harder to detect and prevent. Traditional detection methods, which are often rule-based or focused on a single channel, struggle to keep up with these adaptive and AI-driven techniques.***

This paper presents a systematic analysis of multi-channel phishing attacks and introduces an integrated detection framework that combines machine learning, deep learning, and behavioral analysis. The study reviews recent research from 2023 to 2025 and examines phishing methods in terms of their attack strategies, technical complexity, and impact on user behavior. The results show that AI-driven phishing attacks can increase user compromise rates by 12–30%, while advanced detection models can achieve accuracy levels of up to 90% in controlled settings.

To address these challenges, a multi-layered framework is proposed that includes data collection, feature extraction, intelligent classification, and risk-based decision- making. The findings highlight the need to combine advanced technological solutions with user awareness and supportive policies. Overall, this work aims to support the development of more adaptive, reliable, and scalable defenses against evolving phishing threats in modern digital environments.

*Keywords:***Phishing attacks, cybersecurity, multi-channel phishing, machine learning, deep learning, social engineering, artificial intelligence, behavioral analysis, phishing detection, cognitive bias, email phishing, SMS phishing, voice phishing, QR code phishing, and DNS-based attacks.**

I. INTRODUCTION

Phishing has become one of the most serious and rapidly evolving threats in modern cybersecurity. While earlier attacks mainly focused on exploiting system vulnerabilities, today's phishing techniques increasingly target human behavior, trust, and decision-making. What began as simple email scams has now evolved into a complex, multi-channel problem. Attackers use platforms such as email, SMS, voice calls, social media, Domain Name System (DNS) manipulation, and Quick Response (QR) codes to deceive users. These attacks are carefully designed to create urgency, imitate trusted sources, and influence users through psychological and contextual cues.

The widespread use of smartphones, digital payment systems, and social media has significantly increased opportunities for cybercriminals. As people rely more on digital platforms for communication, banking, and daily activities, attackers have adapted by using advanced technologies such as automation, artificial intelligence, and deepfake techniques. These technologies enable the creation of highly personalized and convincing phishing messages, making it increasingly difficult for users to distinguish between legitimate and malicious content. In addition, the growth of remote work, online banking, and e- commerce—especially after the pandemic—has further increased user exposure to such threats.

Recent studies indicate a rise in phishing attacks targeting mobile users and social media platforms, where traditional security measures are often less effective. SMS-based phishing (smishing) and voice phishing (vishing) can bypass standard email filtering

systems, while DNS-based attacks exploit network-level vulnerabilities. QR code phishing introduces additional challenges by encouraging users to act quickly without proper verification. Although various detection approaches, including rule-based systems and machine learning techniques, have been developed, they often struggle to keep pace with evolving attack strategies, limited user awareness, and privacy concerns.

Despite ongoing research, many existing solutions focus on single-channel detection and do not fully address the combined impact of multiple attack vectors and human behavior. This highlights the need for more comprehensive and adaptive approaches. In this context, this study aims to analyze multi- channel phishing attacks and propose an integrated framework that improves detection while also strengthening user awareness and resilience.

II. PROBLEM STATEMENT

Phishing attacks have become increasingly complex due to their ability to operate across multiple communication channels and exploit both technical vulnerabilities and human behavior. However, most existing detection systems are designed for specific platforms, such as email, and are not effective in identifying attacks that span multiple channels.

The use of artificial intelligence and automation has made phishing attacks more adaptive and personalized, reducing the effectiveness of traditional detection methods. At the same time, users remain vulnerable due to limited awareness, cognitive biases, and reliance on automated security tools.

Moreover, many existing approaches focus mainly on technical detection and do not adequately consider behavioral factors. As a result, they offer only partial protection against modern phishing threats. Therefore, there is a clear need for an integrated and adaptive framework that can effectively address both technical and human aspects of phishing attacks.

III. KEY CONTRIBUTIONS

This paper makes the following key contributions:

1. Comprehensive Multi-Channel Analysis:
A detailed examination of phishing attacks across multiple platforms, including email, SMS, voice, social media, DNS, and QR-based systems.

2. Behavioral and Psychological Insights:
An analysis of how human factors such as trust, urgency, and cognitive bias influence user susceptibility to phishing attacks.

3. Proposed Integrated Framework:
A multi-layered phishing detection framework that combines machine learning, deep learning, and behavioral analysis to improve detection accuracy and adaptability.

4. Comparative Evaluation:
A review of recent research (2023–2025) comparing existing phishing detection techniques based on performance, limitations, and practical applicability.

5. Challenges and Future Directions:
Identification of key technical, ethical, and practical challenges, along with directions for future research in phishing detection.

IV. LITERATURE REVIEW / RELATED WORK

A. Evolution and Technological Development

Phishing techniques have evolved steadily with advances in technology and changes in how people use digital systems. In the early stages, phishing mainly involved fraudulent emails that imitated trusted organizations to steal user credentials (Jakobsson & Myers, 2006). As internet access expanded and mobile usage increased, attackers broadened their strategies to include SMS-based phishing (smishing) and voice-based phishing (vishing), taking advantage of users' trust in communication channels.

The growth of social media further changed the

landscape of phishing attacks by enabling large-scale social engineering. Attackers began impersonating trusted individuals, hijacking accounts, and spreading malicious links more effectively (Albladi and Weir). At the same time, more advanced techniques such as domain spoofing, cache poisoning, and redirection attacks started targeting users at the infrastructure level (Kintis et al., 2020). More recently, QR code-based phishing (quishing) has introduced new risks by exploiting users'trust in QR codes used for payments and authentication (Abdelnabi et al., 2023).

With the introduction of artificial intelligence, phishing has moved beyond simple and generic messages to more advanced and adaptive campaigns. Attackers now use technologies such as natural language generation, deepfake voice synthesis, and automated domain creation to produce realistic and context-aware phishing messages (Dhar et al., 2024). In addition, phishing-as-a-service (PhaaS) platforms have made it easier for even less experienced attackers to launch large-scale and coordinated campaigns.

B. Adoption and Student Perceptions

User behavior plays an important role in determining the success of phishing attacks. Theoretical models such as Technology Threat Avoidance Theory (TTAT) and Protection Motivation Theory (PMT) explain how factors like perceived risk, trust, and self-efficacy influence user responses to potential threats (Workman, 2008; Sheng et al., 2019).

Studies indicate that users who frequently receive official-looking messages through email or SMS may become less cautious over time due to familiarity and time pressure (Kumar and Rao, 2024). This increases the likelihood of interacting with malicious content. Voice phishing and social media-based attacks further exploit this behavior by incorporating real-time interaction and social validation, making the messages appear more credible (Abawajy and Kim, 2023).

In addition, phishing techniques involving DNS systems and QR codes rely on users' natural trust in system infrastructure and simple interfaces. Emotional triggers such as urgency, fear, and curiosity also influence decision- making, increasing the chances of users falling victim to phishing attacks (Lee et al., 2025).

Table I. Factors Influencing User Susceptibility to Phishing Attacks:

Determinant	Description	Influence
Perceived Risk	Awareness of potential harm or data loss	High
Trust in Source	Credibility of sender or Platform	High
Emotional Triggers	Fear, urgency, curiosity exploited by attackers	High
Digital Literacy	Ability to identify deceptive cues	Moderate–High
Overreliance on Technology	Dependence on filters and automation	Moderate

C. Generative and Adaptive Phishing Systems

Modern phishing attacks are increasingly driven by generative and adaptive technologies that can produce deceptive content in real time. Recent studies highlight the role of machine learning, reinforcement learning, and generative models in enabling phishing campaigns to adapt based on user behavior (Zhang et al., 2024).

Unlike traditional phishing methods that rely on static templates, modern attacks use natural language generation and deepfake technologies to customize messages in terms of tone, timing, and context. For example, email and SMS phishing can use user data and interaction history to generate highly targeted messages (Gupta and Li, 2025). Voice phishing relies on speech synthesis to imitate trusted individuals, while social media attacks adjust their content based on user engagement patterns.

Similarly, DNS-based attacks use AI-driven domain spoofing and redirection techniques, and QR-based phishing delivers dynamic content depending on factors such as device type or location. These developments reflect a shift toward self-optimizing phishing systems (Rossi et al., 2025), which increase both the scale and effectiveness of attacks while making detection more challenging.

D. Psychological and Behavioral Impacts

Phishing attacks affect not only system security but also users' psychological and behavioral responses. Research shows that advanced phishing techniques—especially those involving voice, social media, and QR codes—can create urgency, stress, and fear, increasing the likelihood of user interaction (Kumar & Rao, 2024; Abawajy & Kim, 2023).

AI-driven personalization further strengthens these effects by exploiting cognitive biases such as trust, familiarity, and authority. Voice phishing increases perceived authenticity through tone and speech patterns, while social media attacks use peer influence to shape user behavior.

Although these techniques may initially increase user engagement, repeated exposure to phishing attempts can lead to desensitization or decision fatigue. Therefore, understanding these psychological factors is essential for designing effective detection systems, awareness programs, and user-centered security strategies. A balanced approach that combines automated detection with informed user behavior is necessary to reduce risks while maintaining trust in digital environments.

Table II presents a comparison of commonly used phishing detection techniques, including machine learning, deep learning, and hybrid approaches. The comparison highlights their performance, strengths, and limitations. It can be observed that while deep learning and hybrid models achieve higher accuracy, they also require greater computational resources. This emphasizes the need for balanced and adaptive frameworks, as proposed in this study.

Table II: Comparison of Phishing Detection Methods:

Method	Accuracy	Key Strength	Key Limitation
ML	70–85%	Fast, low cost, works with structure d data	Needs manual features, limited for complex patterns
DL	85–92%	High accuracy, automati c feature extraction	High cost, large data required
Hybrid	88–95%	Better accuracy, combine s ML + DL	Complex and resource intensive
AI-Adaptive	90%+	Dynamic , adapts to new attacks	Early stage, high complexity

V. METHODOLOGY

This study uses an integrative meta-synthesis approach to combine insights from multiple peer-reviewed studies published between 2023 and 2025. By bringing together both qualitative and quantitative methods, it aims to provide a balanced understanding of the technological, behavioral, and ethical aspects of phishing attacks.

The selected studies were chosen based on their relevance to different phishing channels, how clearly they explain attack mechanisms, and their overall contribution to the field. Each study was analyzed across four key areas: (i) attack vectors, including email, SMS, voice, social media, DNS, and QR-based attacks; (ii) technical aspects, such as automation, AI- driven adaptation, and generative techniques; (iii) psychological impact, focusing on factors like urgency, stress, and trust manipulation; and (iv) the effectiveness of countermeasures, including detection models, user awareness programs, and policy-level strategies.

To ensure consistency in the analysis, this study is guided by three well-established frameworks:
Technology Threat Avoidance Theory (TTAT), Protection Motivation Theory (PMT), and an AI-assisted phishing detection framework. These frameworks help explain both user behavior and the technical processes involved in phishing detection, as illustrated in Fig. 1.

Although this approach provides a comprehensive view of phishing threats, it does have some limitations. These include differences in research methods, variations in sample populations, and inconsistencies in evaluation metrics across the selected studies. Despite these challenges, the methodology still
offers valuable insights into current trends and supports the development of more effective and adaptive phishing detection strategies.

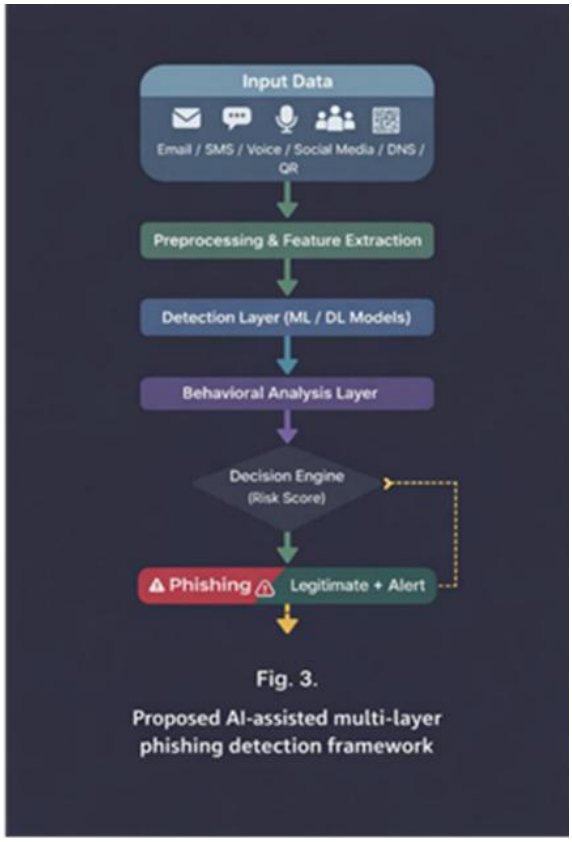

Fig. 1. Proposed AI-assisted multi-layer phishing detection framework.

VI. EXPERIMENTAL SETUP AND RESULTS

To evaluate the effectiveness of the proposed framework, experiments were carried out using a publicly available phishing dataset obtained from sources such as Kaggle and PhishTank. The dataset includes both phishing and legitimate samples, comprising URL-based features along with relevant behavioral indicators. Overall, the dataset contains approximately 10,000 samples (5,000 phishing and 5,000 legitimate instances) with 30 extracted features.

Prior to model training, the data was preprocessed using feature extraction techniques such as lexical analysis and URL structure analysis. The dataset was then divided into training and testing sets using an 80:20 split to ensure a fair and reliable evaluation.

For performance comparison, a Random Forest model was employed as the machine learning approach. The models were implemented using

Python with Scikit-learn and TensorFlow libraries. The results were compared with those of a deep learning model (LSTM) and the proposed hybrid model. The performance of all models was assessed using standard evaluation metrics, including accuracy, precision, recall, and F1-score.

Table III: Performance Evaluation:

Model	Accura cy	Precision	Recall	F1- score
Random Forest (ML)	82%	80%	83%	81%
LSTM (DL)	89%	87%	90%	88%
Proposed Hybrid Model	92%	91%	93%	92%

The performance comparison of different models is illustrated in Fig. 2. and other evaluation metrics. By combining behavioral analysis with AI-based detection techniques, the hybrid approach becomes more adaptable and effective in identifying complex phishing attacks across multiple channels.

VII. DISCUSSION

A. Risk and Behavioral Outcomes

Recent studies highlight that phishing attacks have a noticeable impact on user behavior, especially when they are delivered through adaptive or multi-channel approaches. Research by Kumar & Rao (2024) and Abawajy & Kim (2023) shows that AI-enhanced phishing messages can increase the chances of users sharing sensitive information by about 12–18% compared to traditional static attacks.

This increase is mainly driven by the adaptive nature of modern phishing systems. These systems can modify message content, timing, and delivery based on how users behave. For instance, attackers can study previous interactions to craft more convincing messages and direct users to malicious websites with minimal effort. Such personalization makes it easier to exploit human tendencies like trust and urgency.

These findings make it clear that phishing attacks are no longer static but continuously evolving. This emphasizes the importance of stronger technical defenses, better user awareness, and continuous behavioral training.

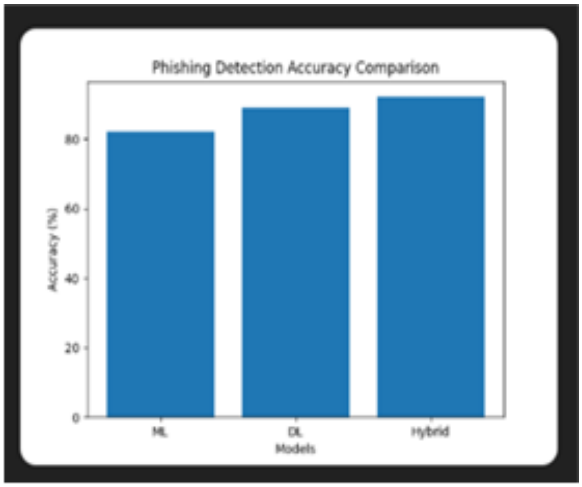

Fig. 2. Performance comparison of ML, DL, and Hybrid models based on accuracy, precision, recall, and F1-score

The results indicate that the proposed hybrid model outperforms both the machine learning and deep learning models in overall accuracy

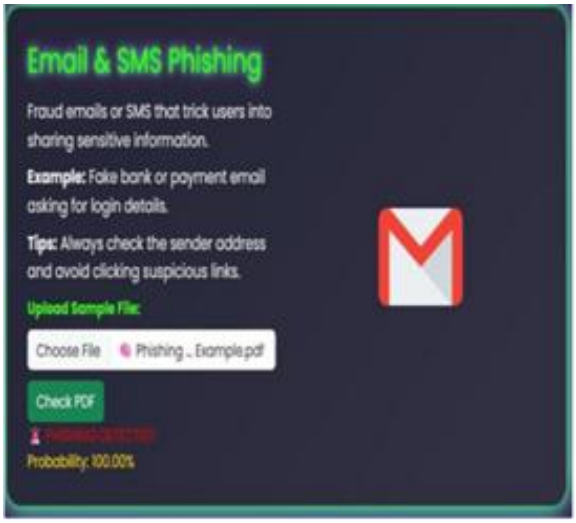

Fig. 3. Email and SMS phishing interface

B. Cognitive and Emotional Impacts

Psychological and emotional factors play a critical role in shaping how users respond to phishing attacks. Research shows that personalized and context-aware phishing messages significantly increase both engagement and compliance rates. Kumar & Rao (2024) observed that multi-channel phishing campaigns delivered through email, SMS, or social media can lead to up to 30% higher interaction rates compared to generic attacks.

The addition of voice-based phishing further increases this effect by creating a sense of immediacy and authenticity, making it more convincing than text-based communication. Similarly, QR code phishing takes advantage of users' trust in physical-digital interactions, encouraging quick actions without proper verification.

Table IV: Relationship Between Phishing Features and Cognitive/Emotional Outcomes:

Phishing Feature	Emotional/Co gnitive Outcome	Reported Effect Size
Personalized Messaging	Increased Compliance	Medium–High
MultiChan nel Delivery	Higher Interaction	High
Voice/Audio Cues	Enhanced Perceived Authenticity	High
QR Code Integration	Rapid Action	Moderate
Urgency & Scarcity Cues	Cognitive Overload	Moderate–High

Also organizations and their day-to-day operations. Many organizations actively monitor phishing activities to improve their email filtering, mobile security, and network protection systems. According to Lee et al. (2025), automated detection systems can identify up to 70% of routine phishing attempts, significantly reducing response times.

In addition, awareness programs and simulated phishing exercises help employees and students better recognize and respond to threats. These efforts provide useful insights into user behavior and vulnerabilities, allowing organizations to strengthen their security policies and allocate resources more effectively.

Taking a multi-channel approach to phishing—covering email, SMS, voice, social media, DNS, and QR codes—enables organizations to build more robust and resilient defense systems, ultimately lowering the risk of data breaches.

C. Organizational and Operational Implications

Phishing attacks impact not only individuals but

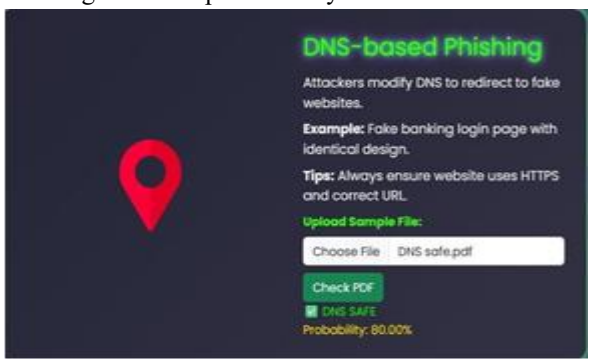

Fig. 4. DNS-based phishing interface

D. Ethical and Technical Challenges

Despite progress in detection and awareness, several challenges remain in effectively addressing phishing attacks. These include concerns related to data privacy, algorithmic bias, regulatory compliance, and the ethical implications of exploiting user behavior.

Phishing campaigns often rely on personal and behavioral data to create highly targeted messages, raising concerns about privacy and unauthorized data use. Without proper governance and transparency, organizations risk losing user trust.

Additionally, bias in detection systems can lead to uneven levels of protection, leaving certain groups more vulnerable. Phishing attacks also exploit human emotions such as urgency and trust, which raises ethical concerns about manipulation and potential harm.

To overcome these challenges, organizations need to implement strong governance frameworks that focus on fairness, accountability, transparency, and explainability. These principles should be applied to both technical solutions and user awareness initiatives to ensure a balanced and effective defense against phishing threats.

VIII. FUTURE PROSPECTS

Phishing attacks are likely to become more advanced in the coming years, with a growing emphasis on automation, adaptability, and context awareness. As technologies such as generative AI, machine learning, and behavioral analytics continue to evolve, attackers will be able to create highly personalized phishing messages across platforms like email, SMS, voice, social media, DNS, and QR codes. By analyzing user behavior, previous interactions, and contextual factors, these attacks can be carefully timed and tailored, making them more convincing and harder to detect.

At the same time, defense strategies are also improving. Technologies such as federated learning and AI-based anomaly detection can help identify new and emerging phishing patterns while still protecting user privacy. Explainable AI (XAI) is becoming increasingly important as well, as it allows security teams to better understand how detection systems make decisions, improving both trust and effectiveness.

Organizations are gradually shifting from reactive security approaches to more proactive ones. Future cybersecurity systems may continuously monitor threats, predict potential user vulnerabilities, and work closely with IT teams to provide adaptive training and faster responses. In the context of the Fifth Industrial Revolution (5IR), there is a growing focus on collaboration between humans and AI. This approach aims to improve resilience, increase user awareness, and support better decision- making in complex digital environments.

IX. CONCLUSION

This study brings together insights from multiple peer-reviewed works and shows that phishing attacks continue to be a serious and evolving threat in today's digital environment. These attacks take advantage of both human factors—such as trust and cognitive biases—and technical weaknesses, often using multiple communication channels to increase their success. Because of this, protecting users and organizations requires more than just technical solutions; it also

depends on awareness and informed decision-making.

Preventing phishing attacks should be seen as a shared responsibility. Detection systems, users, and security teams need to work together, supported by clear policies, continuous monitoring, and regular awareness programs. Improving user understanding and encouraging safe digital practices are just as important as strengthening technical defenses.

Looking ahead, proactive and AI-assisted defense frameworks offer a strong path forward. By combining advanced detection techniques with human oversight, these systems can better identify and respond to new and evolving phishing strategies. Overall, integrating technological advancements with user awareness can help create more secure and resilient digital environments and reduce the impact of increasingly sophisticated phishing attacks.

ACKNOWLEDGMENT

The authors would like to sincerely thank the researchers and institutions whose work contributed to this study, including publications from Springer, Elsevier, and IEEE journals (2023–2025). Their research has provided valuable insights into the evolving field of phishing detection and cybersecurity.

The authors also extend their appreciation to cybersecurity professionals, IT teams, and organizations who shared practical experiences and case studies related to phishing detection and prevention.

Finally, the authors would like to thank the participants involved in awareness programs and simulated phishing exercises, whose experiences offered valuable insights into user behavior and vulnerabilities.

REFERENCES

[1] Shaalan,“ A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Technique,” Information, vol. 16, p. 235, 2025.

[2] R. Al-Yozbaky, M. Alanazi, “Detection and Analyzing Phishing Emails Using NLP Techniques,” Journal of Computer Security, vol. 34, pp. 55–72, 2023.

[3] T. Halder, A. Yakin, S. Esha, S. Hasan, F. M. Hussain, “Enhancing Email Safety: Harnessing ML, DL, and LLM Models for Spam Detection,” Int. J. Cybersecurity, vol. 12, pp. 110-128, 2024.

[4] M. S. Ujjwal, “Exploring Machine Learning Techniques for Real-Time Malicious URL Detection,” Proc. Int. Conf. Inf. Syst. Cybersecurity, vol. 29, pp. 150– 160, 2021.

[5] N. Divani, A. Vinitha, “Machine Learning Based Detection of Malicious URLs in Twitter,” Int. J. Data Sci. Cybersecurity, vol. 11, pp. 215 227, 2022.

[6] B. Geetha, P. Malathi, T. Thirumalakumari, V. Janakiraman, “Machine Learning Approaches for Proactive Phishing Attack Detection,” Proc. Natl. Conf. Cyberdefense, vol. 21, pp. 66–78, 2023. AI

[7] Abdelnabi, M. Fritz, and M. Fritz, “Large Language Models for Phishing Detection and Generation: A New Cybersecurity Threat Landscape,” IEEE Security & Privacy, vol. 22, pp. 45–58, 2024.

[8] S. Gupta and J. Li, “Adaptive Phishing Detection Using Deep Learning and User Behavior Analytics,” Computers & Security, vol. 135, pp. 103–118, 2025.

[9] Y. Zhang, H. Chen, and X. Liu,“Reinforcement Learning-Based Adaptive Phishing Attack and Detection Framework,”IEEE Transactions on Information Forensics and Security, vol. 19, pp. 220–235, 2024.

[10] R. Rossi, L. Marchetti, and F. Cavalli, “AI Driven Phishing-as-a-Service Platforms: Emerging Threats and Countermeasures,”ACM Computing Surveys, vol. 57, pp. 1–30, 2025.