Advancements in Phishing Detection: A Comprehensive Review of Deep Learning and Hybrid Approaches

[1]Ayisha Sana.K.K
Department of Computer Science
Vimal jyothi engineering college
Chemperi, Kannur
ayishasanakk12@gmail.com

[2]Anugrah VS
Department of Computer Science
Vimal jyothi engineering college
Chemperi, Kannur
Anugrahsunil123@gmail.com

[3]Alan Antony
Department of Computer Science
Vimal jyothi engineering college
Chemperi, Kannur
alenantony69822@gmail.com

[4]Jinsu Anna John
Assistant Professor
Department of Computer Science
Vimal jyothi engineering college
Chemperi, Kannur
jinsuanna23@gmail.com

***Abstract*—Phishing attacks continue to be one of the most prevalent forms of cybercrime, leveraging social engineering techniques to trick users into disclosing sensitive information or unknowingly installing malicious software. These attacks often rely on deceptive URLs that lead victims to fraudulent websites designed to steal login credentials, financial data, or personal information. Despite numerous studies focused on detecting phishing through HTML and URL-based methods, there is a lack of comprehensive surveys that systematically review these approaches. This paper addresses this gap by offering an in-depth analysis of modern deep learning techniques applied to phishing detection, with a particular emphasis on URL-based and hybrid methods. The study examines key aspects such as data preprocessing, feature extraction, model architecture, and overall performance, while also highlighting research gaps in the application of deep learning to phishing detection. This paper provides valuable insights for both researchers and cybersecurity professionals, offering a roadmap for future developments in phishing detection technologies.**

keywords:Machine learning,Deep learning,Phishing

I. INTRODUCTION

Phishing attacks have evolved into one of the most widespread and damaging forms of cybercrime, exploiting human vulnerabilities to deceive individuals into revealing sensitive personal information, such as login credentials, financial details, and confidential data. Cybercriminals craft fraudulent websites and deceptive messages that closely resemble legitimate communications, making it increasingly difficult for users to distinguish between authentic and malicious entities. With the increasing sophistication of phishing techniques, these attacks have expanded from simple email scams to complex multi-step social engineering schemes that target both individuals and organizations on a global scale.

The growth of phishing incidents has driven the need for effective automated detection mechanisms capable of identifying malicious websites and phishing attempts in real-time. Traditional detection approaches, such as blacklists, URL filtering, and heuristic methods, have proven to be insufficient in combating the dynamic nature of phishing attacks, especially as cybercriminals continuously modify their tactics to evade detection. As a result, artificial intelligence (AI), particularly machine learning (ML) and deep learning (DL) technologies, have emerged as promising solutions for phishing detection. These methods offer the advantage of automating feature extraction, adapting to new phishing tactics, and improving detection accuracy over time.

While deep learning and hybrid-based models have gained significant attention in recent years for their potential to address the shortcomings of conventional approaches, there remains a gap in comprehensive research exploring their application to phishing detection. In particular, URL-based and hybrid-based techniques, which combine multiple detection methods, have shown promising results, yet remain underexplored in terms of data preprocessing, feature extraction, and model optimization. This paper aims to fill that gap by reviewing existing literature on phishing detection and providing a detailed analysis of deep learning and hybrid-based approaches. It also identifies key research challenges and opportunities for further development to enhance the effectiveness of phishing detection technologies.

II. LITERATURE SURVEY

A. Phishing Attacks and Their Challenges [3]

Phishing attacks remain a growing cybersecurity concern, exploiting human psychology to manipulate users into re-

vealing sensitive information. Traditionally, attackers have used emails, social media, and other platforms to distribute fraudulent messages containing phishing links. These links lead to counterfeit websites where attackers steal personal data, login credentials, and financial information. Additionally, phishing attacks can serve as gateways for installing malicious software, contributing to malware infections and ransomware attacks. The challenges in detecting phishing are magnified by the use of deceptive URLs and websites designed to closely resemble legitimate ones, which necessitate advanced detection techniques.

To counter these threats, various detection techniques have been developed, ranging from rule-based filtering to advanced artificial intelligence models. Traditional approaches rely on blacklists and heuristic rules to block known phishing sites, but these methods struggle against newly generated attacks. Machine learning and deep learning techniques offer more adaptive solutions by analyzing URL structures, webpage content, and behavioral patterns to identify anomalies. Features such as domain age, lexical analysis, and page elements help in distinguishing legitimate sites from fraudulent ones. Moreover, real-time monitoring systems enhance security by continuously updating threat databases and detecting emerging phishing tactics. As cybercriminals refine their strategies, a combination of AI-driven analysis, user awareness training, and robust cybersecurity measures remains essential for effective phishing prevention.

B. Traditional Phishing Detection Methods [8]

Traditional detection methods like blacklist-based approaches have been widely used but are proving to be ineffective against evolving phishing tactics. Blacklists rely on previously identified malicious URLs, meaning they fail to detect new or modified phishing websites. As attackers continuously modify their techniques to bypass blacklist detection, these traditional methods become increasingly inadequate. Furthermore, relying on blacklists does not scale well to handle large numbers of phishing sites, making the need for more adaptive and automated solutions even more pressing.

Blacklist-based detection has been a common approach for identifying phishing sites, but it struggles to keep up with evolving threats. Since blacklists rely on known malicious URLs, they fail to detect newly created or altered phishing websites. Cybercriminals frequently modify their tactics to evade detection, rendering these static lists less effective. Additionally, maintaining and updating blacklists for the vast number of phishing sites is challenging and lacks scalability. This limitation highlights the need for more adaptive and automated techniques that can identify phishing attempts in real time, even when attackers use novel strategies.

C. Machine Learning for Phishing Detection [6]

In response to the limitations of traditional methods, machine learning (ML) models have been introduced to improve phishing detection. These models use data to ”learn” and automatically identify phishing patterns, reducing the need for manual feature extraction. However, ML models require large, labeled datasets and are often prone to overfitting. The effectiveness of these models can also be limited by the quality of the input data, particularly when handling sophisticated phishing tactics that evolve quickly. ML models also often rely heavily on manual feature selection, which can be time-consuming and error-prone.

To address these challenges, deep learning techniques have been explored as a more advanced alternative to traditional ML models. Unlike conventional approaches, deep learning methods, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, can automatically extract features from raw data, reducing the need for manual intervention. These models are capable of identifying complex patterns in phishing attacks by analyzing URL structures, website content, and user interactions. However, deep learning requires significant computational resources and large, diverse datasets to perform effectively. Despite these challenges, integrating deep learning with other cybersecurity measures, such as real-time monitoring and threat intelligence, enhances phishing detection and helps counter increasingly sophisticated attack techniques.

D. Deep Learning for Phishing Detection [5]

Recently, deep learning (DL) techniques have emerged as an effective solution for phishing detection due to their ability to automatically extract features and learn complex patterns from data. Unlike traditional ML models, DL methods use neural networks to process vast amounts of data and improve detection accuracy. Deep learning offers several advantages, including the ability to handle unstructured data, such as raw HTML and URL information, and the capability to adapt to new phishing tactics without requiring manual feature engineering. However, deep learning models face challenges in terms of data preprocessing, computational demands, and their ability to generalize to new, unseen phishing strategies.Phishing detection methods typically analyze URLs, webpage content, or both to identify malicious patterns.

URL-based techniques examine features such as domain names, URL length, and special characters to classify links. Content-based methods assess elements like HTML structure, JavaScript, and page layout. Advanced approaches use machine learning and deep learning models, including CNNs, LSTMs, and hybrid techniques. These models preprocess data, break it into meaningful components, and convert it into vector representations for training. Some systems rely on blacklists and heuristic rules, while others use unsupervised learning like clustering to detect similarities. Hybrid models integrate URL and content analysis for more accurate detection, enhancing protection against evolving phishing threats.

E. Deep Learning Approaches for URL-Based Phishing Detection [7]

URL-based phishing detection is a critical area of focus for deep learning techniques, as attackers often rely on deceptive URLs to lure victims to fraudulent websites. Many deep

learning models for phishing detection extract features from the structure and content of URLs to identify potential phishing threats. Common methods include using Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to analyze URL strings and detect patterns that may indicate phishing attempts. These models are highly effective at identifying suspicious URL structures, but their performance can be influenced by the variability of URL encoding and obfuscation techniques used by attackers.

To enhance detection accuracy, hybrid models combining multiple deep learning architectures have been developed. For instance, integrating CNNs with Long Short-Term Memory (LSTM) networks allows models to capture both spatial and sequential patterns within URLs, improving their ability to identify phishing attempts. Additionally, attention mechanisms and transformer-based models have been explored to further refine feature extraction and decision-making processes. However, these approaches require large-scale datasets and significant computational power to train effectively. Despite these challenges, advancements in deep learning continue to improve the reliability of URL-based phishing detection, making it more resilient against evolving obfuscation techniques and adversarial attacks.

F. Hybrid Approaches in Phishing Detection [10]

Hybrid approaches combine multiple detection techniques to enhance phishing detection accuracy. For example, combining URL-based analysis with HTML content analysis can improve the ability to detect phishing sites that employ a variety of tactics to deceive users. Deep learning models can integrate both structured and unstructured data, allowing for a more comprehensive analysis of phishing websites. Hybrid models offer significant advantages in terms of detection accuracy and adaptability, as they can leverage the strengths of different methods to identify phishing websites more effectively.

In addition to improving detection accuracy, hybrid approaches enhance resilience against sophisticated phishing techniques that evade single-method detection. By integrating machine learning, deep learning, and heuristic-based analysis, these models can detect anomalies in both URL patterns and webpage content. For instance, combining lexical feature extraction with visual similarity analysis helps identify phishing pages that mimic legitimate websites. Furthermore, real-time data processing in hybrid models enables quicker identification of emerging threats. While these approaches require more computational resources and complex model training, their ability to adapt to evolving phishing strategies makes them a powerful solution for modern cybersecurity challenges.

G. Data Preprocessing in Deep Learning Models [2]

Data preprocessing plays a critical role in improving the performance of deep learning models for phishing detection. Preprocessing steps such as data cleaning, normalization, and feature extraction help ensure that the model is trained on high-quality data, which can lead to better generalization and more accurate predictions. Proper data handling techniques are particularly important when working with large, complex datasets, as the quality and relevance of the input data directly impact model performance. Moreover, preprocessing can help mitigate issues such as imbalanced datasets or noisy data, which can lead to biased or inaccurate prediction.

Effective data preprocessing also involves transforming raw data into meaningful representations that deep learning models can efficiently process. Techniques such as tokenization, vectorization, and encoding are commonly used to convert URL strings and webpage content into numerical formats suitable for model training. Additionally, feature engineering plays a crucial role in extracting relevant attributes, such as domain age, character distributions, and keyword presence, which help distinguish phishing URLs from legitimate ones.

H. Challenges in Detecting Novel Phishing Techniques [4]

One of the main challenges in phishing detection is the ability to detect new and evolving phishing tactics. Attackers are constantly developing new techniques to bypass existing detection systems, such as using domain generation algorithms, URL obfuscation, and other methods to disguise malicious links. Deep learning models, while powerful, can struggle to detect novel phishing strategies without sufficient training data that includes these new tactics. Additionally, adversarial attacks can trick models into misclassifying phishing sites as legitimate.

I. The Need for Scalable and Efficient Detection Models [9]

To address scalability concerns, researchers are exploring methods such as distributed computing and parallel processing to handle the massive amounts of data generated by phishing attacks. These techniques allow models to process large datasets in a more efficient and timely manner. Additionally, leveraging cloud-based infrastructures can provide the necessary computational power to support resource-intensive deep learning models without requiring significant on-premise hardware. Furthermore, the development of more efficient algorithms and data processing pipelines can reduce training time and improve real-time detection capabilities.

J. Future Research Directions in Phishing Detection [1]

The future of phishing detection lies in the development of more efficient and adaptable deep learning models. Researchers should focus on improving the robustness of these models to novel phishing techniques and the integration of unsupervised learning methods, which can help detect previously unknown phishing threats.

III. COMPARISON

The comparison table below provides a comprehensive analysis of various phishing detection methods, highlighting their advantages and disadvantages. It serves as a valuable reference for understanding the strengths and limitations of traditional, machine learning, and deep learning-based approaches to combat phishing attacks.This evaluation aims to guide researchers and cybersecurity professionals in selecting and optimizing techniques for more effective phishing detection.

TABLE I
COMPARISON TABLE

Reference	Description	Advantages	Disadvantages
[3]	Phishing is a type of cybercrime where attackers cre- ate fake websites to steal sensitive information like usernames, passwords, and credit card details. Various techniques are used, such as link manipulation, website forgery, and social engineering. Machine learning has proven to be an effective method for detecting phishing attempts by identifying common characteristics in phish- ing website	- High Accuracy: Machine learning models, especially ensemble methods like Random Forest and XGBoost, provide high accuracy in detecting phishing websites. - Automation: Unlike manual detection methods, machine learning can auto- matically analyze large datasets and detect phishing attempts in real time.	- Data Dependency:The accuracy of machine learning models depends on the quality and size of the training dataset. - Computational Cost: Some models, such as deep learning and neural net- works, require significant computa- tional power and time for training.
[8]	Phishing websites are fake websites designed to trick users into giving away personal information, such as passwords and credit card details.	- High Accuracy: Advanced models like XGBoost and neural networks can improve detection rate - Fast Detection: Machine learning al- gorithms can quickly analyze large amounts of data to detect phishing sites.	- Data Dependency: The accuracy of machine learning models depends on having a high-quality dataset - Computational Cost:Some methods require high processing power, mak- ing them slower on large-scale data.
[6]	phishing is a type of cyberattack where fake websites trick users into sharing personal information like pass- words and credit card details. These attacks are increasing rapidly, making online security a big concern.	- Machine learning can identify phish- ing websites with high precision - Automated detection speeds up web- site verification compared to manual methods	- Depends on Data Quality: The accu- racy of ML models relies on high- quality training data. - Computationally Expensive: Some models require significant processing power.
[5]	Traditional methods like blacklists are not enough to stop new phishing sites. Machine learning provides a smart way to detect phishing by analyzing website features and patterns to differentiate between real and fake sites.	- Machine learning can identify phish- ing websites with high precision - Fast Processing: Automated detection speeds up website verification com- pared to manual methods.	- Depends on Data Quality:* The ac- curacy of ML models relies on high- quality training data. - Computationally Expensive:* Some models require significant processing power.
[7]	Machine learning offers a powerful way to detect phish- ing attacks, but each method has trade-offs. Random Forest and Neural Networks perform well in accuracy but require more resources.	- Simple and easy to interpret. - Works well with both numerical and categorical data.	- Prone to overfitting if not properly pruned. - Can be sensitive to small changes in data.
[10]	Each machine learning method has strengths and weak- nesses. Simple models like Decision Trees and Na¨ıve Bayes are fast but may struggle with complex attacks.	- Easy to understand and interpret. - Works well for small to medium- sized datasets.	- Some classifiers, like Random Forest, may be too computationally expen- sive for real-time systems. - Works well for small to medium- sized datasets.
[2]	The document provides a detailed analysis of different phishing detection methods, including their advantages and disadvantages. Below is a simplified summary of these methods:	- Simple and fast to implement.	- Cannot detect new (zero-hour) phish- ing attacks. - Blacklists need constant updating.
[4]	This paper reviews techniques for detecting malicious URLs, categorizing them into blacklist-based, rules- based, machine learning, and deep learning methods.	- Offers a detailed review of current malicious URL detection methods, beneficial for researchers. - In-depth look at features that help identify malicious URLs	- No case studies or real-world experi- ments to back up the methods. - Doesn't provide enough details on how to implement the techniques in real-world scenarios.
[9]	Phish Fighter is a system designed to detect phishing websites by analyzing their HTML structure. It identifies repeated code patterns used in phishing kits, which are pre-made tools that help attackers create fake websites.	- Detects phishing websites by recog- nizing common HTML code struc- tures . - Can identify new phishing threats by analyzing as few as three pages from an unknown phishing kit.	- Machine learning-based detection re- quires significant processing power, making it more resource- demanding. - Attackers can modify their phishing kits to change HTML structures, po- tentially reducing detection accuracy.

IV. CONCLUSION

Phishing attacks remain a significant cybersecurity threat, with attackers continuously evolving their tactics to bypass detection systems. As traditional methods fall short in addressing new and increasingly sophisticated phishing schemes, deep learning models offer a promising solution for more accurate and efficient phishing detection. This paper has reviewed URL-based and hybrid deep learning techniques, emphasizing their effectiveness in automating feature extraction and improving detection accuracy. However, challenges remain, particularly in the areas of data preprocessing, model scalability, and the detection of novel phishing tactics. The study highlights the need for more efficient models that require less computational power while maintaining high detection performance. Moving forward, research should focus on improving data handling techniques, enhancing model adaptability to new phishing strategies, and developing robust datasets to strengthen phishing detection systems.

V. FUTURE SCOPE

Phishing attacks, leveraging social engineering tactics, remain one of the most prevalent forms of cybercrime, posing significant threats to sensitive information and system security. As attackers continuously evolve their strategies, the need for advanced, automated phishing detection methods grows. Deep learning (DL) models, particularly those leveraging URL-based and hybrid approaches, have emerged as powerful tools to enhance detection capabilities. These models, capable of automatic feature extraction and pattern recognition, offer a promising solution to the limitations of traditional methods like blacklisting. However, challenges remain in data preprocessing, model scalability, real-time detection, and adaptability to novel phishing techniques. Future research in phishing detection should focus on advancing deep learning architectures, such as Transformer-based models, to improve accuracy and robustness. Incorporating unsupervised and semi-supervised learning methods can help detect emerging phishing tactics with minimal labeled data, while the integration of Explainable AI (XAI) will provide transparency and foster trust in automated systems. Real-time detection models optimized for low-latency responses and cross-platform functionality are crucial as phishing continues to target diverse digital environments. Additionally, federated learning could promote decentralized detection systems that ensure privacy without compromising efficiency. Creating robust, diverse datasets through data augmentation techniques will help models generalize better, while privacy-preserving methods like differential privacy will address ethical concerns surrounding user data. Ultimately, the future of phishing detection lies in developing efficient, adaptable, and scalable models that can address the evolving landscape of cyber threats, while ensuring privacy and trust in automated security systems.

REFERENCES

[1] Sultan Asiri, Yang Xiao, Saleh Alzahrani, Shuhui Li, and Tieshan Li. A survey of intelligent detection designs of html url phishing attacks. *IEEE Access*, 11:6421–6443, 2023.

[2] Gabriela Brezeanu, Alexandru Archip, and Codru-Georgian Artene. Phish fighter: Self updating machine learning shield against phishing kits based on html code analysis. *IEEE Access*, 13:4460–4486, 2025.

[3] Chenyu Gu. A lightweight phishing website detection algorithm by machine learning. In *2021 International Conference on Signal Processing and Machine Learning (CONF-SPML)*, pages 245–249, 2021.

[4] Rizka Widyarini Purwanto, Arindam Pal, Alan Blair, and Sanjay Jha. Phishsim: Aiding phishing website detection with a feature-free tool. *IEEE Transactions on Information Forensics and Security*, 17:1497–1512, 2022.

[5] Sita Rani, Aman Kataria, Sachin Kumar, and Vinod Karar. A new generation cyber-physical system: A comprehensive review from security perspective. *Computers Security*, 148:104095, 2025.

[6] Junaid Rashid, Toqeer Mahmood, Muhammad Wasif Nisar, and Tahira Nazir. Phishing detection using machine learning technique. In *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, pages 43–46, 2020.

[7] Ozgur Koray Sahingoz, Ebubekir Buber, Onder Demir, and Banu Diri. Machine learning based phishing detection from urls. *Expert Systems with Applications*, 117:345–357, 2019.

[8] Vahid Shahrivari, Mohammad Mahdi Darabi, and Mohammad Izadi. Phishing detection using machine learning techniques, 2020.

[9] Yi Wei and Yuji Sekiya. Sufficiency of ensemble machine learning methods for phishing websites detection. *IEEE Access*, 10:124103–124113, 2022.

[10] Rasha Zieni, Luisa Massari, and Maria Carla Calzarossa. Phishing or not phishing? a survey on the detection of phishing websites. *IEEE Access*, 11:18499–18519, 2023.