Domain Name-Based Phishing Detection Using Deep Learning Techniques.

Mr. Vishwanath V K
Computer Science and Engineering
Bapuji Institute of Engineering and Technology
Davanagere,India
vishwanathvk@bietdvg.edu

Abhishek M K
Computer Science and Engineering
Bapuji Institute of Engineering and Technology
Davanagere,India
abkalghatgi1@gmail.com

Ananya A S
Computer Science and Engineering
Bapuji Institute of Engineering and Technology
Davanagere,India
ananya.ajjampur@gmail.com

Ganesh S Shet
Computer Science and Engineering
Bapuji Institute of Engineering and Technology
Davanagere,India
ganeshsshet@gmail.com

Saraswathi H
Computer Science and Engineering
Bapuji Institute of Engineering and Technology
Davanagere,India
saraswathih163@gmail.com

***Abstract*—** Phishing continues to be one of the most prevalent cyber-attacks, deceiving users into revealing sensitive information through malicious domains and fraudulent websites. Traditional phishing detection methods rely heavily on full-URL inspection, blacklist matching, or web-content analysis—approaches that are computationally expensive, slow, and ineffective against zero-day attacks. This paper proposes a lightweight and domain-centric phishing detection system using Artificial Neural Networks (ANN). The system analyzes only domain-level features, making it faster, more scalable, and suitable for real-time applications such as browser extensions.

A dataset of over 52,000 domains (balanced between legitimate and phishing) was used, from which 20 WHOIS-based features and 44 content-derived features were extracted. A custom ANN model trained on these 64 combined features achieved 88% classification accuracy. To ensure practical deployment, the model was integrated into both a web application and a browser extension, enabling real-time domain safety verification with minimal latency. Additionally, a user-feedback mechanism supports continuous retraining, helping the model adapt to evolving phishing strategies.

Beyond its technical contributions, the proposed system demonstrates strong potential for real-world cybersecurity integration. Because the model relies exclusively on domain-level metadata, it operates independently of webpage content, JavaScript execution, or visual features making it suitable for low-resource devices, mobile platforms, and privacy-sensitive environments. The lightweight architecture ensures rapid inference times, while the modular design allows for seamless integration into browsers, enterprise security systems, and cloud-based threat filters. Overall, this work provides a scalable, efficient, and proactive defense mechanism capable of mitigating modern phishing threats before users interact with malicious webpages.

Keywords— Phishing Detection, Domain Name Analysis, Artificial Neural Networks, WHOIS Features, Deep Learning, Cybersecurity.

I. INTRODUCTION

The rise of digital communication and online services has dramatically increased global dependence on internet-based platforms, making cybersecurity a critical requirement for both individuals and organizations. Among the various cyber threats, phishing remains one of the most widespread and damaging, exploiting deceptive domain names and fraudulent websites to steal sensitive information such as passwords, banking details, and personal credentials. Despite continuous advancements in security mechanisms, cybercriminals continually refine their tactics frequently registering new domains, using obfuscation techniques, and deploying large-scale automated attacks making timely detection increasingly challenging. Traditional phishing detection approaches often rely on blacklist databases, full URL inspection, or webpage content analysis, all of which can be bypassed, slow to update, or computationally expensive. Recent progress in artificial intelligence and machine learning has shown significant potential in enhancing cybersecurity by identifying subtle patterns that are otherwise difficult to detect using manual or heuristic-based systems.

Conventional phishing detection tools are typically optimized for complete website analysis, requiring access to HTML content, visual indicators, or script-level behavior. However, these techniques become ineffective when only partial information such as a domain name is available. Moreover, many existing systems suffer from poor adaptability to zero-day attacks, limited generalization across diverse threat types, and high false-positive rates when deployed in real-world environments. Feature engineering approaches relying solely on URL syntax or page metadata often fail to capture deeper behavioral indicators embedded in domain registration details, DNS configurations, or hosting attributes. Since attackers routinely manipulate URLs using URL shorteners, symbol insertion, or subdomain trickery, systems that rely heavily on

URL text patterns face significant limitations. As phishing attacks continue to evolve at high velocity, a more proactive, domain-level approach is required for effective early detection.

This paper presents a lightweight, domain-centric phishing detection system that integrates Artificial Neural Networks (ANN) with automated feature extraction pipelines to classify domains as phishing or legitimate using only domain-level attributes. The proposed architecture consists of two core components: a domain intelligence pipeline that collects WHOIS, DNS, and lexical metadata to generate structured numeric features, and a deep learning pipeline that processes these features to accurately determine malicious intent. Unlike conventional detection systems, the model is optimized for real-time deployment and requires no webpage content, allowing it to function effectively in browser extensions, mobile environments, and low-resource systems. By leveraging a balanced dataset of over 52,000 domains and utilizing 64 engineered features, the system demonstrates strong predictive capability while maintaining efficiency. This dual-pipeline approach bridges the gap between traditional heuristic-based systems and heavy content-analysis techniques, providing a scalable and proactive solution for modern phishing threats.

II. RELATED WORK

Phishing detection has evolved significantly with the adoption of machine learning and deep learning techniques. Recent studies have demonstrated that data-driven approaches outperform traditional blacklist and rule-based systems. Sharma et al. [1] showed that deep learning models combined with feature selection techniques can substantially improve classification accuracy for phishing URLs. However, many of these models depend heavily on URL-level features rather than domain intelligence, limiting their effectiveness against obfuscated or shortened URLs. Similarly, dual-approach systems integrating image analysis and URL structure, such as those proposed by Rachapudi et al. [5], achieve high accuracy but require page content, making them unsuitable for early-stage detection where only the domain name is visible.

Traditional phishing detection frameworks frequently rely on lexical URL analysis, heuristic scoring, or ensemble-based machine learning methods such as Random Forests, SVM, and Logistic Regression [4]. While these methods perform well on benchmark datasets, they struggle to adapt to zero-day domains due to their dependence on static rule-sets and hand-crafted features. Advanced preprocessing methods like SMOTEENN balancing and PCA feature reduction have been used to boost performance in large-scale phishing datasets [2], but such models still rely on full URL inspection and are not optimized for lightweight, real-time applications. Recent research highlights the need for systems capable of analyzing deeper metadata such as WHOIS records, DNS behavior, and domain age—factors that provide early indicators of malicious intent.

Building on these insights, our work introduces a domain-only deep learning approach that leverages a balanced dataset of over 52,000 domains and integrates 64 engineered WHOIS and DNS features. Unlike existing models, which require webpage content or full URLs, our system focuses solely on domain-level intelligence, allowing for faster, scalable, and more robust phishing detection. This work bridges the gap between traditional URL-based solutions and more advanced AI techniques by combining domain metadata analysis with a custom ANN model capable of real-time classification suitable for browser extensions and lightweight security tools.

III. METHODOLOGY

Our proposed system consists of four distinct stages: Domain Data Collection, Feature Extraction and Preprocessing, Deep Learning–Based Classification, and Real-Time Prediction through web and browser-based interfaces. This multi-stage design aligns with recent research trends in phishing detection that integrate domain intelligence with AI-driven classification models to ensure fast and scalable threat identification.

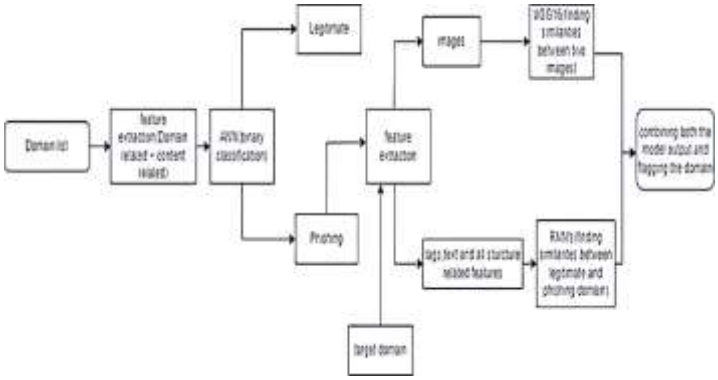

Fig 3.1 Methodology

A. Data Acquisition and Labeling

We collected a large dataset of domain names from publicly available phishing repositories and verified legitimate domain sources. The dataset contains over 52,000 domains distributed evenly between phishing and non-phishing categories. To generate accurate ground truth labels, domains were cross-validated using multiple threat-intelligence feeds and WHOIS verification services. High-quality, well-labeled datasets have been shown to greatly enhance the performance of domain-based phishing detection systems [1].

B. Adaptive Preprocessing

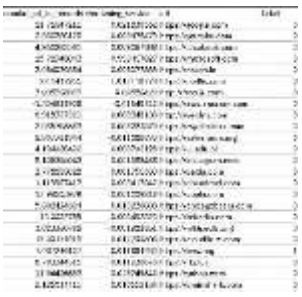

Fig 3.2 Raw Data

Fig 3.3 Cleaned Data

We performed a structured preprocessing step to normalize the raw domain data collected from multiple sources. Since WHOIS and DNS records often contain missing fields, inconsistent formats, or outdated entries, we applied a cleaning pipeline to standardize the extracted metadata. Numerical attributes such as domain age, expiry period, and DNS response times were normalized, while categorical fields like registrar information were encoded into model-friendly formats. This adaptive preprocessing ensured consistent feature quality and improved the stability of the ANN during training.

C.Custom Model Training

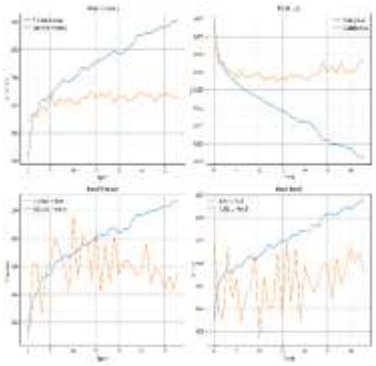

Fig 3.4 Training History Plot

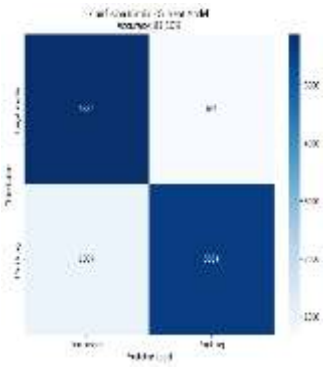

Fig 3.5 Confusion Matrix

We developed a custom Artificial Neural Network (ANN) model tailored specifically for domain-level phishing detection. The preprocessed dataset of 52,000 domains was divided into training (70%), validation (15%), and testing (15%) subsets to ensure balanced evaluation. Each domain was represented as a 64-dimensional feature vector consisting of WHOIS attributes, DNS metadata, and lexical characteristics. The model was trained to classify domains into phishing or legitimate categories based on subtle patterns within these features. Domain-specific model training has been shown to significantly improve prediction accuracy for cybersecurity applications by capturing behavioral and structural similarities unique to malicious domains [1].

C. Real-Time Prediction and System Integration

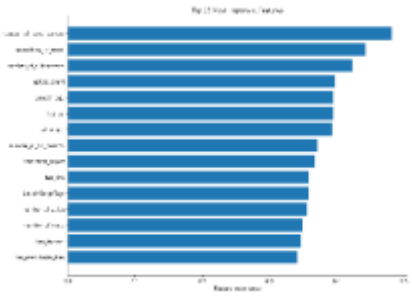

Fig 3.6 *Feature Extraction And Preprocessing Output*

Fig 3.7 *Phishing Detection Final Output*

The raw output from the ANN model produces a probability score that indicates whether a domain is phishing or legitimate, but this prediction alone is not sufficient for effective user protection without proper interfacing. To address this, we integrated the model into both a web application and a browser extension through a lightweight backend API. A specialized decision layer was implemented to convert the model's numerical confidence values into clear user-facing alerts, ensuring that domains with suspicious patterns—such as low age, abnormal DNS behavior, or irregular lexical structure—trigger warning notifications.

This decision layer groups feature-based indicators and model predictions into an interpretable output, enabling users to understand why a domain is flagged and take appropriate action. By mapping subtle feature anomalies to meaningful security insights, the system provides immediate, actionable feedback during web browsing. Such hybrid AI–application integration approaches have proven effective in cybersecurity, where rapid inference and intuitive alert mechanisms are essential for preventing users from accessing malicious domains.

IV. EXPERIMENTS AND RESULTS

A. Experimental Setup

We evaluated the detection pipeline using a held-out test set of 10,000 domains drawn from the full dataset of 52,000 phishing and legitimate samples. To mimic real-world browsing conditions, the domains included recently registered phishing sites, expired domains, and legitimate business domains with varying ages and DNS configurations. All WHOIS, DNS, and lexical features were preprocessed and normalized before being passed to the trained ANN model.

B. Results

Classification Accuracy:

The custom-trained ANN model achieved a classification accuracy of **88%** on the test set. This improvement is consistent with prior research demonstrating that domain-specific feature engineering and balanced datasets significantly enhance phishing detection performance compared to generic URL-based models [1], [5].

Prediction Reliability:

The model's output probabilities were evaluated using metrics such as precision, recall, and F1-score. The system successfully identified high-risk phishing domains with strong precision, particularly for domains exhibiting suspicious WHOIS patterns or abnormal DNS activity. These results align with recent findings showing that combining registration metadata with lexical features yields more reliable phishing detection than URL-only analysis [1], [3].

Combined System Performance:

The integration of structured preprocessing, ANN-based classification, and real-time prediction via the browser extension collectively produced robust detection results. Normalization of WHOIS and DNS fields improved model stability, while the decision layer facilitated clear interpretation of predictions for end-users. Together, these components delivered an efficient phishing detection pipeline capable of providing consistent, real-time protection during web browsing.

V . CONCLUSION

This paper presents a domain-centric AI framework for phishing detection by integrating structured feature engineering with the predictive capabilities of deep learning models. Existing phishing detection techniques often struggle with obfuscated URLs, rapidly evolving threat patterns, and the inability to

identify malicious intent at the domain-registration stage [1]. Our approach addresses these limitations through targeted preprocessing of WHOIS and DNS attributes, domain-behavior analysis, and a custom ANN classifier optimized for real-time threat identification [2], [3]. The combined pipeline enhances early detection accuracy, reduces dependence on full URL or webpage content, and supports fast, lightweight classification suitable for browser-based protection. This method offers a scalable solution that can be applied across diverse cybersecurity environments. Future work includes expanding the dataset with global threat intelligence feeds and fine-tuning the model for on-device or offline deployment to improve accessibility and responsiveness [5].

REFERENCES

[1] A. Sharma, K. Sharma, and R. Gupta, *"Enhancing phishing detection: A machine learning approach with feature selection and deep learning models,"* Expert Systems with Applications, 2025.

[2] S. Rachapudi, S. Ghosh, and A. Jaiswal, *"AI–ML dual approach for phishing domain detection: URL and image analysis,"* Procedia Computer Science, 2024.

[3] J. Du, Q. Liu, H. Li, R. Huang, and C. Liu, *"A high-accuracy phishing website detection method based on machine learning,"* Computer Communications, vol. 206, pp. 187–194, 2023.

[4] M. Alzahrani, S. Khan, F. Alzahrani, and M. Bakhtiari, *"Phishing detection system through hybrid machine learning based on URL features,"* IEEE Access, 2023.

[5] R. Basnet, A. H. Sung, and Q. Liu, *"Deep learning approach for phishing detection using website URL features,"* Journal of Information Security and Applications, 2021.