**INTELLIGENT SYSTEM FOR IDENTIFICATION OF PHISHING EMAILS, FAKE WEBSITES AND SAND-BOXING TARGETED ENTITY**

**Sowmiya P1, SaravanaKumar M2**

1Student, Department of Computer Science, Rathinam College of Arts and Science, Tamil Nadu, India.

2Associate Professor, Department of Computer Science, Rathinam College of Arts and Science, Tamil Nadu, India.

**ABSTRACT**

An intelligent system designed to identify phishing emails, detect fake websites, and sandbox targeted entities to enhanceThe proposed system leverages machine learning algorithms and natural language processing techniques to analyze the content, structure, and behavior ofA comprehensive dataset comprising legitimate and malicious samples was used to train and validate the detection models.The system integrates a sandboxing module to execute and observe potentially harmful elements in a controlled environment, thereby aiding inExperimental results indicate a high detection accuracy and low false-positive rate, demonstrating the system’s effectiveness in real-time threat identification.The proposed solution contributes to reducing human error in phishing detection, automating threat response, and improving organizational security posture.This research highlights the significance of a multi-layered approach combining static and dynamic analysis to combat evolving cyber threats efficiently.

**Keywords:**Phishing Detection, Fake Website Identification, Sandboxing, Machine Learning, Cybersecurity, Real-time Analysis

1. **INTRODUCTION**

In today’s digital era, cyber threats such as phishing attacks and fake websites have become increasingly sophisticated and widespread, posingPhishing is a deceptive attempt to obtain sensitive information by masquerading as a trustworthy entity through emails or fraudulent websites.These attacks often lead to financial losses, data breaches, and compromised systems.Traditional security measures often fall short in identifying novel or cleverly disguised threats, making it essential to develop intelligent, adaptive solutions.Recent advancements in artificial intelligence (AI) and machine learning have opened new avenues in cybersecurity, especially in the automated detectionCurrent research focuses on utilizing natural language processing, URL analysis, and behavioral profiling to improve threat detection capabilities.However, most systems lack an integrated approach that not only detects phishing emails and fake websites but also provides real-time analysis of suspicious elements using sandboxing techniques.This paper addresses the subject by proposing an intelligent system that combines phishing email detection, fake website identification, and sandboxing of targeted entities.The study aims to enhance detection accuracy, reduce false positives, and provide comprehensive threat analysis, thereby contributing to the development.

1. **METHODOLOGY**

The proposed research work focuses on designing an intelligent system for the identification of phishing emails, fake websites, and sandboxingThe methodology integrates machine learning, keyword analysis, and static script evaluation to build a comprehensive threat detection framework.The system development was divided into three core modules: phishing email detection, fake website identification, and sandboxing for suspicious behavior analysis.For phishing email detection, a keyword-based scoring model was implemented.Frequently occurring terms in phishing attempts such as “urgent”, “account”, “verify”, and “login” were selected based on literature review andEmails were parsed and evaluated against these keywords, and a score-based threshold was used to classify them as phishing or legitimate.To identify fake websites, feature extraction was applied to URLs.Features such as URL length, use of symbols (e.g., '@', '-'), and presence of IP addresses were extracted.These features were used to train a Random Forest Classifier, which demonstrated high accuracy in distinguishing phishing websites from legitimate ones.Sandboxing was conducted by statically analyzing the HTML and JavaScript content of websites.Scripts containing potentially dangerous functions like eval() and document.write() were flagged as suspicious.This multi-module approach ensures a layered, intelligent detection system with effective real-time applicability.

**2.1 Email Phishing Detection**

Phishing emails were identified using keyword-based text classification.Common phishing terms such as "urgent", "account", "verify", and "password" were extracted from a corpus of legitimate and malicious emails.Each email was analyzed by counting the frequency of these keywords and scoring the content.If the score exceeded a defined threshold, the email was flagged as phishing.This approach was lightweight and effective for real-time scanning.

**2.2 Fake Website Detection**

To detect fake or malicious websites, URL-based feature extraction was employed.Features such as:

* URL length,
* presence of special characters (@, -),
* and the use of IP addresses in domain names,

were extracted and used to train a supervised machine learning model (Random Forest Classifier).The model was trained using a labeled dataset of legitimate and phishing URLs, achieving accurate classification of unknown URLs.

**2.3 Sandboxing Targeted Entities**

A sandboxing mechanism was developed to analyze the content of websites without executing them in a live environment.This module fetched the raw HTML and JavaScript of a webpage and parsed it using BeautifulSoup.It searched for malicious script patterns like:

* eval()
* document.write()
* suspicious

1. **MODELING AND ANALYSIS**

The intelligent system developed in this research comprises three interconnected modules, each modeled to address a specific aspect of phishingThe first module targets phishing emails through a text classification model.A keyword-based heuristic approach was adopted wherein a predefined list of phishing-related keywords was used to calculate a threat scoreEmails exceeding a certain threshold were flagged as phishing.This model was lightweight, interpretable, and suitable for integration into real-time email filtering systems.The second module focuses on identifying fakeA machine learning model—specifically, a Random Forest Classifier—was used for URL classification.URLs were pre-processed and converted into feature vectors using parameters such as URL length, presence of special characters (like '@'The model was trained on a balanced dataset of phishing and legitimate URLs, resulting in reliable predictive performance.The third moduleInstead of executing potentially dangerous code, this module performs static analysis of the website content.Using BeautifulSoup, it parses the HTML and JavaScript code, identifying red flags such as the presence of eval(), document.write(), hidden iframes, which are often indicative of malicious behavior.This multi-tiered modeling approach enhances detection accuracy and ensures the system is capable of handling evolving phishing techniques.

1. **RESULTS AND DISCUSSION**

The intelligent system developed in this research was evaluated based on its ability to accurately classify phishing emails, detect fakeThe results are discussed below for each module, followed by an overall system evaluation.

**4.1Phishing Email Detection**

The phishing email detection module was tested using a diverse dataset containing both legitimate and phishing email samples.The system successfully identified phishing emails with a high degree of accuracy, achieving an accuracy rate of approximately 92%.The keyword-based scoring model performed well in identifying commonly used phishing phrases and tactics, such as "urgent," "verify," and "account."However, some edge cases, where phishing emails did not contain typical keywords, were missed, highlighting the potential benefit of integrating more advanced NLP models for deeper contextual understanding.

**4.2 Fake Website Detection**

The website analysis module utilized a Random Forest Classifier to evaluate URLs based on extracted features such asThe model showed excellent performance with an accuracy of 89%, distinguishing between legitimate and phishing sites based on common patternsFalse positives occurred when legitimate websites with unusual URL structures were misclassified, indicating the need for further fine-tuning and additional feature selection.

**4.3 Sandboxing of Suspicious Entities**

The sandboxing module was designed to analyze the behavior of web pages by inspecting their HTML andThe system successfully flagged malicious websites containing suspicious code patterns, such as the use of eval() and document.write(), with aSome websites that used legitimate scripts or obfuscated JavaScript went undetected, emphasizing the challenge of distinguishing between malicious and harmless web content in complex scenarios.

**Overall System Performance**

The system demonstrated solid overall performance, effectively detecting phishing threats with a combination ofHowever, it also revealed limitations when faced with more sophisticated attacks.Combining multiple detection techniques, such as machine learning with deeper context analysis, could improve the system's ability to identify more

1. **CONCLUSION**

This research aimed at developing an intelligent system for identifying phishing emails, fake websites, and sandboxing targeted entities.The system incorporated a multi-faceted approach to tackle phishing threats, utilizing machine learning models, keyword-based text analysis, and static content analysis for website behavior monitoring.The phishing email detection module effectively identified suspicious emails based on the frequency of phishing-related keywords,The website analysis module, using a Random Forest Classifier, demonstrated strong performance in detecting fraudulent websites, with a classification accuracyThe sandboxing module showed promising results in identifying malicious scripts, with an 85% detection rate.While the system proved effective in most scenarios, certain limitations were observed, particularly with more sophisticated phishing attempts and websites using complex JavaScript code.False positives and missed detections, especially with legitimate sites having unusual URL structures or obfuscated scripts, were challenges that need further refinement.

Overall, this research provides a solid foundation for building real-time phishing detection systems.The integration of multiple detection techniques, combined with machine learning, offers a scalable and adaptive approach to combating phishing andFuture work could focus on enhancing the accuracy of the system by incorporating advanced Natural Language Processing (NLP) techniques for email analysis and improving the sandboxing functionality for more complex threats.

1. **REFERENCES**

[1. ] Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006). Phishing email detection using structural properties.NYS Cyber Security Conference.

[2.] Basnet, R. et al. (2012). Detection of phishing attacks: A machine learning approach. IEEE Int. Conf. on Big Data.

[3.] Bergholz, A. et al. (2010). Improved phishing detection using model-based features. CEAS.

[4.] Verma, R., & Hossain, N. (2017). Semantic feature selection for phishing email detection. eCrime Researchers Summit.

[5.] Marchal, S. et al. (2016). PhishStorm: Detecting phishing with streaming analytics. IEEE Trans. on Computers.

[6.] Mohammad, R.M., Thabtah, F., & McCluskey, L. (2015). Intelligent phishing detection system using URL features. IET Information Security.

[7.] Xiang, G. et al. (2011). Content-based phishing detection with machine learning. ACM TIST.