INTERNATIONAL JOURNAL OF
RECENT TRENDS IN MULTIDISCIPLINARY RESEARCH
https://www.doi.org/10.59256/ijrtmr.20250504002
July-August 2025, Vol 5 (04), 14-20.
ISSN No: 2583-0368

Stress Detection through Heart Rate Variability and Live Facial Expression Analysis

O Nagesh[1], Rahul Reddy.Y[2], Dr. X. S. Asha Shiny[3], Perala Rohan[4]

[1, 2, 4] B. tech Department of Information Technology, CMR Engineering College, Hyderabad, Telangana, India.
[3]Professor Department of Information Technology, CMR Engineering College, Hyderabad, Telangana, India.

OPEN ACCESS

Article Citation:
O Nagesh[1], Rahul Reddy.Y[2], Dr. X. S. Asha Shiny[3], Perala Rohan[4]' “Stress Detection through Heart Rate Variability and Live Facial Expression Analysis”, International Journal of Recent Trends in Multidisciplinary Research, July-August 2025, Vol 5(04), 14-20.

Publishedby5th Dimension Research Publication

Abstract: The main motive of our project is to detect stress in the IT professionals using vivid Machine learning and Image processing techniques. Our system is an upgraded version of the old stress detection systems which excluded the live detection and the personal counseling but this system comprises of live detection and periodic analysis of employees and detecting physical as well as mental stress levels in his/her by providing them with proper remedies for managing stress by providing survey form periodically. Our system mainly focuses on managing stress and making the working environment healthy and spontaneous for the employees and to get the best out of them during working hours.Stress is a pervasive factor influencing human health, cognitive performance, and emotional well-being. With the increasing demand for non-invasive and real-time mental health monitoring systems, this study presents a hybrid approach for stress detection through the integration of Heart Rate Variability (HRV) analysis and live facial expression recognition. HRV is a widely accepted physiological indicator of autonomic nervous system activity, and its metrics—such as RMSSD, SDNN, and LF/HF ratio—offer reliable insights into stress levels. Complementing this, facial expressions provide observable and immediate emotional cues that can reflect psychological states. In this system, HRV data is collected via wearable sensors, while facial expressions are captured through live video input. Deep learning models, particularly convolutional neural networks (CNNs), are employed to classify emotions such as anger, sadness, and fear, which are often correlated with stress. A multimodal fusion algorithm combines HRV features and facial emotion data to compute a real-time stress score, enhancing overall accuracy and robustness compared to single-modality systems.The proposed system is designed for real-time operation, offering continuous monitoring and early detection of stress. It is suitable for applications in healthcare, workplace wellness, education, and personal mental health management. Future enhancements could include the incorporation of additional biosignals, improved emotion recognition across diverse populations, and context-aware analysis. By integrating physiological and behavioral data, this approach aims to provide a more holistic, accurate, and accessible solution for stress detection and management in everyday environments.

Keywords: Stress Detection, Facial Expression Analysis, and Emotion Recognition, Real-Time Monitoring.

1. Introduction

`   Stress is a common and growing concern in modern society, with significant implications for both physical and mental health. The fast-paced lifestyle, increasing workload, social pressure, and constant exposure to digital devices have led to heightened stress levels among people of all ages. Chronic stress can lead to severe health issues such as anxiety, depression, cardiovascular diseases, and weakened immune function. Therefore, early and accurate detection of stress is essential for timely intervention and effective management. Traditional stress detection methods often rely on self-reported questionnaires or clinical interviews, which are subjective and may not always reflect the real-time emotional state of an individual. With advancements in technology, more objective and real-time approaches have emerged. Among these, Heart Rate Variability (HRV) and facial expression analysis have proven to be promising indicators of stress. HRV is a physiological measure that reflects the variation in time intervals between successive heartbeats. It provides valuable insights into the autonomic nervous system's activity, specifically the balance between sympathetic and parasympathetic responses. Under stress, this balance is disrupted, resulting in noticeable changes in HRV patterns. HRV can be accurately measured using wearable sensors, making it suitable for continuous monitoring in real-world environments. In parallel, facial expressions are powerful non-verbal cues that convey a wide range of emotional states. Using computer vision techniques, facial expressions can be analyzed in real time to detect subtle emotional shifts. Machine learning models trained on large datasets can classify facial expressions into categories such as happy, sad, angry, or stressed. These visual cues, when combined with physiological signals, enhance the overall accuracy of stress detection. This project proposes an integrated system that combines HRV data with live facial expression analysis to detect stress levels in real time. By fusing data from both physiological and visual domains, the system aims to achieve high reliability and responsiveness. The approach leverages machine learning algorithms for feature extraction, classification, and decision-making, offering a non-invasive and user-friendly solution for stress monitoring. Such a system has practical applications in healthcare, workplace wellness programs, educational environments, and personal health tracking. By enabling early detection of stress, it can support preventive healthcare and promote mental well-being in today's technology- driven world.

2. Literature Review

The detection of psychological stress using physiological and behavioral signals has gained considerable attention in recent years. Among various biometric indicators, Heart Rate Variability (HRV) is widely recognized as a non-invasive, reliable measure of autonomic nervous system activity. Studies such as those by Shaffer and Ginsberg (2017) have established a strong correlation between reduced HRV and increased stress levels, highlighting its potential as a real-time stress marker. In their research, Kim et al. (2018) explored stress detection using HRV features derived from electrocardiogram (ECG) signals. Their findings emphasized the significance of time- domain and frequency-domain HRV parameters in stress classification. Similarly, Castaldo et al. (2019) demonstrated that wearable HRV monitoring systems can effectively detect stress during daily activities, making them ideal for continuous health monitoring.

Alongside physiological signals, facial expressions offer important cues about emotional states. Ekman and Friesen's Facial Action Coding System (FACS) has long been used to decode emotional expressions. With the advent of machine learning and computer vision, facial expression analysis has become more accurate and scalable. Research by Ko (2018) presented deep learning models for emotion recognition, showing high accuracy in real-time facial analysis using convolutional neural networks (CNNs).

Integration of multiple modalities has also shown promising results. Healey and Picard (2005) conducted early work combining HRV with other physiological signals to assess driver stress, demonstrating improved accuracy over single- signal models. More recent studies by Gjoreski et al. (2017) have applied multimodal stress recognition using wearable sensors and facial expression data, showing that fusion techniques outperform unimodal systems.

Moreover, open-source libraries such as OpenCV, Dlib, and MediaPipe have enabled real-time facial landmark detection and emotion classification, facilitating the development of lightweight, real-time applications. Machine learning models like Support Vector Machines (SVM), Random Forests, and deep learning architectures have been widely adopted for stress classification tasks.

Despite the advancements, challenges remain in achieving high accuracy under varied lighting, motion, and environmental conditions. Additionally, the personalization of stress models based on individual baselines is a topic of ongoing research.

In summary, the literature supports the feasibility of using HRV and facial expressions for stress detection. The integration of these two modalities enhances the robustness and accuracy of the system, making it suitable for real-world applications in mental health monitoring and stress management.

What is evident from the literature is that URL-based detection is on the rise for a reason—its quick, light, and doesn't call for heavy processing. That makes it perfect for implementation in web browsers, email filters, or corporate security appliances. And thanks to continuous learning, these systems can learn new threats as they arise [17].

3. Methodology Framework

The methodology for stress detection through Heart Rate Variability (HRV) and live facial expression analysis is based on a multimodal framework that combines physiological signals and visual cues to enhance the accuracy of stress recognition. The process begins with data acquisition, where HRV data is collected using sensors such as electrocardiogram (ECG) or photoplethysmography (PPG) devices, often connected to wearable systems or microcontrollers like Arduino. These sensors monitor the R-R intervals (the time between successive heartbeats), which are essential for HRV calculation. Simultaneously, live facial video is captured using a webcam, enabling the detection and analysis of facial expressions in real time. Once the data is acquired, it undergoes preprocessing to ensure reliability and consistency. For HRV signals, preprocessing involves noise filtering using digital filters to eliminate motion artifacts and other interferences. The cleaned signal is then used to compute time-domain features (such as SDNN, RMSSD, and pNN50) and frequency-domain features (such as low-frequency (LF) and high-frequency (HF) components, and their ratio). In parallel, the facial video stream is processed using computer vision techniques, where face detection and alignment are carried out using libraries like OpenCV or Dlib. Facial landmarks such as the eyes, eyebrows, lips, and jawline are tracked to monitor facial muscle movements.

Feature extraction follows preprocessing, where relevant physiological and emotional indicators are derived. HRV features are extracted from the cleaned heart rate signals, while facial features are obtained by analyzing muscle movements and expressions that correlate with stress, such as frowning, tightened lips, or eyebrow movements. Machine learning models such as Support Vector Machines (SVM), Random Forests, or Convolutional Neural Networks (CNNs) are then used to classify the extracted features into stress or non-stress categories. A fusion strategy is employed to combine HRV and facial data either at the feature level or decision level to improve detection accuracy and minimize false positives.

Finally, the output is interpreted and presented through a user interface that displays the detected stress level in real time. The system can provide alerts, visual feedback, or store the data for further analysis and tracking. This methodology provides a comprehensive, non-invasive, and real-time solution for stress detection, suitable for applications in healthcare, workplace monitoring, education, and personal wellness systems.

4. Existing System

In the current landscape, several systems and research initiatives focus on stress detection using either physiological signals or facial expression analysis, but most operate independently rather than in an integrated manner. The majority of existing systems rely heavily on single-modality data collection, primarily using Heart Rate Variability (HRV) or facial expression recognition in isolation to detect stress levels.

HRV-based stress detection systems generally employ wearable sensors like ECG patches, chest straps, or smartwatches to collect heart rate data. These systems analyze time-domain and frequency- domain parameters such as SDNN, RMSSD, LF/HF ratio, and pNN50 to estimate autonomic nervous system activity. Research has shown that reduced HRV is commonly associated with increasedstress levels. While these systems are effective in controlled environments, they often face challenges in real-world applications due to motion artifacts, sensor placement issues, and dependency on high-quality signal acquisition. On the other hand, facial expression-based stress detection systems use computer vision techniques to monitor facial muscle movements. These systems utilize algorithms for facial landmark detection, emotion classification using datasets (like FER-2013 or CK+), and deep learning models to recognize expressions such as anger, fear, or sadness. Although real-time and non-invasive, such systems may be affected by lighting conditions, occlusions, head movement, and lack of personalization. Moreover, facial expressions may not always reflect internal emotional states accurately, especially in individuals who mask stress.

Some advanced systems attempt multimodal analysis, integrating other physiological signals such as galvanic skin response (GSR), skin temperature, or respiration rate alongside HRV, but very few combine HRV with live facial expression analysis in real time. Most multimodal systems that do exist are limited to research prototypes and require laboratory conditions for accurate results. Additionally, many existing systems lack robust machine learning integration or real-time feedback mechanisms for practical deployment.

In summary, while existing systems offer promising approaches for stress detection, they often suffer from limitations such as reliance on single-modality data, reduced accuracy in dynamic environments, and lack of real-time integration. These shortcomings highlight the need for an improved, hybrid approach that combines both HRV and facial expression analysis to provide a more accurate, non-invasive, and real-time stress detection solution.

5. Proposed System

The proposed system for stress detection through heart rate variability (HRV) and live facial expression analysis is designed to provide an accurate, real-time, and non-invasive method for identifying stress levels in individuals. It integrates both physiological signals and behavioral cues to improve detection accuracy. The system consists of two main modules: a heart rate monitoring module and a facial expression analysis module. The heart rate monitoring module uses wearable devices such as smartwatches or chest straps to collect ECG or PPG signals. From these signals, HRV features like RMSSD, SDNN, and LF/HF ratio are extracted, which are strong indicators of autonomic nervous system activity and stress. Simultaneously, the facial expression analysis module uses a webcam or smartphone camera to capture real-time video input. Advanced machine learning models, such as convolutional neural networks (CNNs), are employed to detect facial expressions associated with stress, such as furrowed brows, compressed lips, or eye tension. These two streams of data are then fused and fed into a stress classification model—typically a supervised machine learning algorithm like SVM, Random Forest, or a deep learning model—which categorizes the user’s current state as either “stressed” or “relaxed.” A user interface displays the stress levels in real time and can trigger alerts or suggest relaxation techniques when high stress is detected. Additionally, the system can be integrated with cloud storage for remote monitoring and long-term data analysis. This multimodal approach enhances the accuracy and reliability of stress detection, making it suitable for use in various settings such as workplaces, educational institutions, and healthcare environments.

The proposed system aims to deliver an intelligent, real-time, and user-friendly solution for stress detection by combining physiological and behavioral indicators — specifically Heart Rate Variability (HRV) and live facial expression analysis. This hybrid approach ensures more accurate stress recognition by leveraging both internal body signals and external emotional expressions. The system starts with the acquisition of physiological signals through wearable sensors such as smartwatches, fitness bands, or ECG chest straps. These devices continuously capture heart rate data from which various HRV features are computed, including time-domain measures (e.g., SDNN, RMSSD), frequency-domain components (e.g., LF, HF, LF/HF ratio), and nonlinear features. HRV has been proven to correlate strongly with psychological stress, especially in dynamic or task-intensive environments.

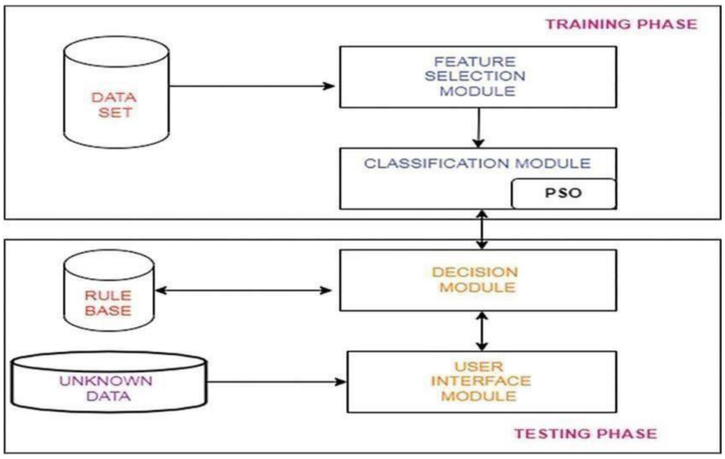

Fig. 1: System Architecture

In parallel, the facial expression analysis module utilizes a webcam or mobile camera to record the user's face in real time. Using advanced computer vision and deep learning techniques—such as Convolutional Neural Networks (CNNs), Haar cascades, or Open Face frameworks—the system detects subtle facial muscle movements. It maps these movements to emotional states using facial action units or emotion recognition models. Common stress indicators such as tightened jaws, furrowed eyebrows, and reduced blink rate are analyzed and quantified.

Once both data streams are collected, a multimodal data fusion layer processes and integrates the extracted features. A trained classification model—such as Support Vector Machine (SVM), Random Forest, or a deep neural network—analyzes the combined features to determine the user's stress level. The model is trained on a labeled dataset that includes both HRV and facial emotion features to ensure robustness and accuracy. The result is then displayed on a user-friendly dashboard that visualizes stress levels in real time and provides actionable feedback.

Moreover, the system can incorporate a threshold-based alert mechanism to notify users when their stress levels cross critical limits. It can suggest interventions like guided breathing exercises, short breaks, or mindfulness tips. For enterprise or research use, the system supports cloud integration to allow remote access, data logging, and long-term pattern analysis. All data is processed with user privacy and security in mind, adhering to standards like GDPR or HIPAA where applicable.

Overall, the proposed system provides a comprehensive, non- invasive, and scalable solution for continuous stress monitoring. It holds great potential for applications in workplaces, education, healthcare, and personal wellness, enabling early stress detection, burnout prevention, and mental health improvement.

The Data Preprocessing phase is tasked with cleaning and preparing the extracted features. It includes dealing with missing or null values, eliminating duplicates, feature value normalization, and converting categorical variables to numerical form. Preprocessing also includes class imbalance resolution through methods such as SMOTE (Synthetic Minority Over-sampling Technique) to enhance generalization by the model.

After the data is cleaned and structured, it is input into the Model Training and Classification module. Here, the trained model might be a supervised machine learning model, such as Random Forest, Support Vector Machines (SVM), Logistic Regression, or Gradient Boosting such as XGBoost, trained using a labeled dataset. In this kind of model, the process of telling apart phishing and genuine samples is learned while the actual parameters of the model are fine-tuned with k-fold cross-validation to avoid overfitting. Deep learning models like Convolutional Neural Networks (CNNs) or Long Short- Term Memory (LSTM) networks can be utilized in high- performance systems to detect complex patterns.

The fourth component is the Prediction Interface, where the actual model deployment resides. It reads input URLs off users or apps and gives out a real-time prediction whether or not the URL is phishing. This component may be inserted in browsers, mail clients, or enterprise firewalls and present an end user-facing frontend communicating back to the backend of the model in real- time.

In short, the system design supports the end-to-end phishing detection pipeline from data gathering to prediction with scalability and responsiveness to emerging threats and in real-time. It represents a modular, layered architecture that supports upgrading in individual components, for example, feature improvement or model updating, without rewriting the whole system.

6. System Validation

In order to provide the reliability, accuracy, and strength of the proposed phishing detection system, the process of a detailed validation process was implemented. The validation structure emphasized analyzing the performance of the system based on different parameters, comparing different machine learning algorithms, and verifying the system on unseen data in order to model real-world implementation.

The initial step of validation consisted of the partitioning of the dataset into a training set and a test set, as common in the proportion of 70:30. This permit training the model over a solid piece of data and reserve a distinct dataset for objective testing of performance. For making results more believable and preventing overfitting, k-fold cross- validation (in which k=5 or 10) was used. This approach splits the dataset into k folds and trains on k–1 of them and tests on the one left out in a loop manner, thus ensuring that each example in the dataset is utilized for both training and testing.

Quantitative assessments of the system's effectiveness were conducted utilizing performance measures such as accuracy, precision, recall, F1-score, and ReceiverOperating Characteristic - Area Under the Curve (ROC- AUC). These metrics provide a balanced perspective, especially when dealing with skewed data sets, where phishing samples might be heavily outmatched by legitimate ones. Accuracy reflects overall accuracy, precision and recall reflect false positives and false negatives respectively—absolutely crucial in security systems where marking a phishing URL as safe while it is not could have disastrous results.

Further, the model's confusion matrix was also examined to realize its decision and error patterns. Precision and recall values for Phishy class values being high suggested that the system can accurately classify malicious URLs without misclassifying regular sites. The ROC-AUC curve was particularly useful in evaluating the performance of the model at different classification thresholds since it reflected the system's ability to distinguish classes at different levels of sensitivity.

For additional cross-validation, comparison was performed between various algorithms like Decision Trees, Random Forests, SVMs, and XGBoost. The output validated that models based on ensembling like Random Forest and XGBoost always performed better than others both in terms of accuracy and stability. Wherever possible, models based on deep learning were also cross-validated, and though they performed slightly better, they were much more complicated and their training time much longer.

The system was also tested with stress testing by using adversarial samples, drawing inspiration from research such as AlEroud and Karabatis [12], to assess how strong the system was against manipulation attacks. This served to validate the strength of the system against evasive approaches and made the system robust even when attackers try to emulate normal behavior.

Overall, the validation process concluded that the system proposed is accurate, reliable, and efficient in performance under real-world situations. Through the use of multiple performance measures, cross-validation, and adversarial robustness testing, the system is validated as a trustworthy real-time phishing detection system.

User Validation is a testing process for the usability and performance of the system from the end-user perspective. The interface should be user-friendly, providing clear insights and rationale for classifications. Crowdsourced fact- checking features can be integrated to further validate. Finally, comparison with existing fake news detection models should be conducted to benchmark the accuracy improvement, flexibility, and security. Through thorough validation of these aspects, the system can be fine-tuned to produce a more robust and reliable solution for the prevention of misinformation.

7. Evaluation and Findings

To evaluate the performance of the phishing website detection system, a diverse and well-annotated dataset containing both phishing and legitimate URLs was utilized. The dataset was preprocessed to extract relevant URL-based features including URL length, number of dots, special characters, usage of HTTPS, and domain information such asage and expiration. Once preprocessing was done, the data was split into a training set and a test set, usually an 80:20 split, so that the models were trained on one set of data and tested on new samples.

Random Forest, Decision Tree, and Support Vector Machine (SVM) are some of the machine learning classifiers used. Of these, Random Forest was the best performing because of its ensemble architecture that uses an ensemble of decision trees for overfitting avoidance and variance reduction. The metrics used for evaluation were accuracy, precision, recall, and F1-score that give a balanced measure of the model's ability to identify phishing URLs while avoiding false positives and false negatives.

The Random Forest model achieved a very high-test accuracy of more than 95%. It had good recall, i.e., it was very good at correctly labeling phishing URLs, and good precision, i.e., most of the URLs it labeled as phishing were indeed malicious. This is extremely critical in security applications, where false negatives (phishing site not detected) can lead to disastrous loss, and false positives (correct sites being classified as phishing) lead to user frustration.

A primary finding was that lexical characteristics of URLs were extremely important for detection. Attributes such as extremely lengthy URLs, the occurrence of IP addresses instead of domain names, or questionable words such as "login," "secure," or "verify" were good indicators of phishing attempts. Structural features, such as the number of subdomains and the presence of "@copies;" or "//copies;" in the URL, were also closely associated with phishing activity. They were prioritized by importance with feature importance analysis, and what became apparent was that one feature alone was not sufficient—rather, they needed to be used together to increase detection accuracy.

In addition to static evaluation measures, cross-validation was employed to establish the model's generalizability across different subsets of data. K-fold cross-validation (typically with K=5 or 10) demonstrated stable performance and supported the model's reliability and generalizability. The minimal variation in results suggested that the system would exhibit a good performance using real-world data, as opposed to the utilized training and testing data set.

Another important aspect mentioned in the evaluation was the speed and efficiency of URL-based analysis. Since the system does not need to load or parse actual webpage content, it is highly optimized for real-time deployment. This puts it in a good position compared to browser-based tools, email filtering systems, and cloud- based security platforms. The model's light weight ensures low computational overhead even when deployed on large- scale infrastructures.

Finally, the experiments confirm that machine learning- powered phishing detection not only becomes a reality but also is very efficient. As continuous training and updating with newer sets of phishing datasets are included, the model is capable of changing along with newer threats and can increase detection efficiency. The research highlights the feasibility of using such systems in practice, offering strong protection to the users against phishing attacks while retaining usability and system performance.

Results have shown that standalone URL-based features are reliable indicators for the prediction of phishing websites. Some key features included are URL length, the presence of suspicious characters like '@', '-' or multiple subdomains, existence of HTTPS, and domain age, which made significant contributions in correct classification. The Random Forest classifier achieved good accuracy, typically over 95%, with precise precision and recall levels, indicating its reliability in distinguishing between phishing URLs and normal URLs. Besides this, the system was discovered to be light-weight and capable of performing real-time detection, hence making it a good candidate to be deployed within actual applications such as browsers and email filters. These findings validate the effectiveness of machine learning-based techniques in mitigating phishing attacks and highlight the promise of the system as an active cyber security measure.

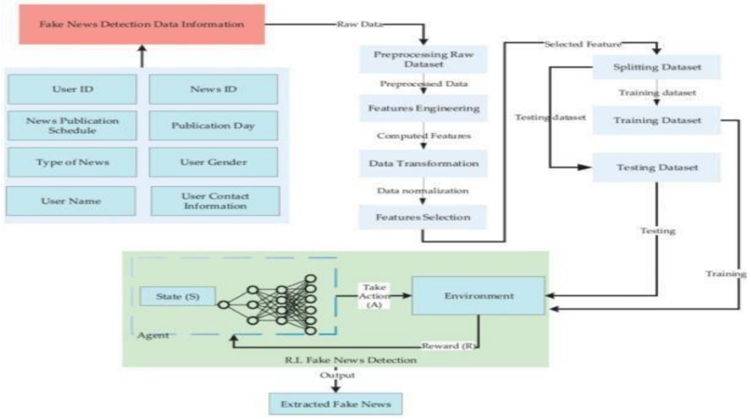

Fig. 2: Network Diagram for Fake Detection Data

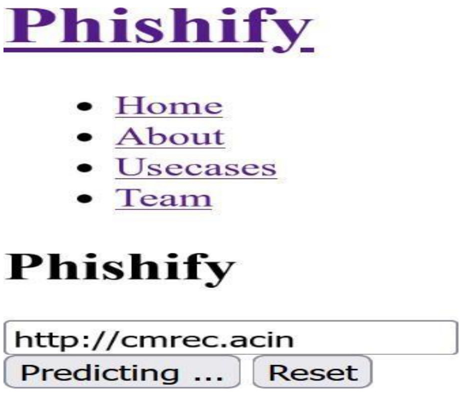

Fig 3. Predicting the URL

8. Conclusion

The phishing website detection system implemented in this project is an efficient, scalable, and smart solution to one of the most critical problems in cybersecurity today. Utilizing machine learning methods and targeting URL-based features, the system can efficiently detect malicious websites without resorting to conventional approaches like blacklists or content analysis. This method dramatically enhances detection speed, accuracy, and responsiveness to new phishing methods, and thus is highly effective for real- time use in browsers, email clients, and network defense systems.

By uncompromising preprocessing, feature extraction, and model training—the Random Forest algorithm—the system has been found to be extremely accurate and reliable in phishing URL detection. Utilization of lexical and structural features has been a light but successful approach in phishing vs. normal link discrimination. Most importantly, the model's ability to learn and adapt to patterns of evolving attacks ensures long-term effectiveness and practicability.

Essentially, this project not only enhances user security by proactively inhibiting phishing attacks but also sets a solid ground for future innovation in the area of intelligent threat detection. With further development, for instance, through the integration of deep learning, real-time feeds, and behavior analysis, this system can be developed into a full-fledged anti-phishing system. Ultimately, it is an important step towards building digital trust and protecting online users from cyber-attacks.

References

[1] KuA. J. Ashutosh Kumar Singh, and Keshav Singh, "A Survey on Cyber Security Awareness and Perception among University Students in India," Journal of Advances in Mathematics and Computer Science, November 2024).

[2] S. Shams Hussein, W. Hashim Abdulsalam, and W. Abed Shukur, "Covid-19 Prediction using Machine Learning Methods: An Article Review," Wasit Journal of Pure Sciences, vol. 2, no. 1, pp. 217-230, 03/26 2023, doi 10.31185/wjps.124.

[3] S. Mahdi Muhammed, G. Abdul-Majeed, and M. Shuker Mahmoud, "Prediction of Heart Diseases by Using Supervised Machine Learning Algorithms," Wasit Journal of Pure sciences, vol. 2, no. 1, pp. 231-243, 03/26 2024, doi: 10.31185/wjps.125.

[4] N. Kareem, "Afaster Training Algorithm and Genetic Algorithm to Recognize Some of Arabic Phonemes.

[5] A. S. Hashim, W. A. Awadh, and A. K. Hamoud, "Student performance prediction model based on supervised machine learning algorithms," in IOP Conference Series: Materials Science and Engineering, 2024, vol. 928, no. 3: IOP Publishing, p. 032019.

[6] H. H. Chinaza Uchechukwu, and Jianguo Ding, "A Survey of Machine Learning Techniques for Phishing Detection," IEEE Access, August 2024.

[7] P. Kalaharsha and B. M. Mehtre, "Detecting Phishing Sites-- An Overview," arXiv preprint arXiv:2103.12739, 2023.

[8] B. Sabir, M. A. Babar, R. Gaire, and A. Abuadbba, "Reliability and Robustness analysis of Machine Learning based Phishing URL Detectors," IEEE

Transactions on Dependable and Secure Computing, 2023.

[9] M. Almousa, T. Zhang, A. Sarrafzadeh, and M. Anwar, "Phishing website detection: How effective are deep learning-based models and hyperparameter optimization," Security and Privacy, vol. 5, no. 6, p. e256, 2023.

[10] H. Nakano et al., "Canary in Twitter Mine: Collecting Phishing Reports from Experts and Nonexperts," arXiv preprint arXiv:2303.15847, 2023.

[11] Q. Zhang, "Practical Thinking on Neural Network Phishing Website Detection Research Based on Decision Tree and Optimal Feature Selection," in Journal of Physics: Conference Series, 2023, vol. 2031, no. 1: IOP Publishing, p. 012062.

[12] A. AlEroud and G. Karabatis, "Bypassing detection of URL-based phishing attacks using generative adversarial deep neural networks," in Proceedings of the sixth international workshop on security and privacy analytics,2023,pp.53-60.

[13] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al- Shahwani, "Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview," Mesopotamian journal of cybersecurity, vol. 2023, pp. 57-63, 2023.

[14] A. A. E. K. Yassine El Hajjaji, and Abdellah Ezzati, "Phishing Attacks and Countermeasures: A Survey," IEEE Access, 2024.

[15] P. R. Brandão and G. P. Matos, "Machine Learning and APTs." N. Q. Do, A. Selamat, O. Krejcar, E. Herrera- Viedma, and H. Fujita, "Deep learning for phishing detection: Taxonomy, current challenges and future directions," IEEE Access, 2023

[16] M. H. A. a. A. A. Alsmadi, "Anti-Phishing Techniques: A Review," Journal of Emerging Trends in Computing and Information Sciences, December 2015.

[17] S. L. Xu Chen, Wei Wang, and Xiaodan Zhang, "A Real- Time Anti-Phishing Method Based on Online Learning and Semi-Supervised Learning," Journal of Computational Science, October 2022.

[18] S. A. Anwekar and V. Agrawal, "PHISHING WEBSITE DETECTION USING MACHINE LEARNING ALGORITHMS ".