iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** I **Month of publication:** January 2025

DOI: https://doi.org/10.22214/ijraset.2025.65807

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

Real-Time Cyber Security Protection Tool

A. S. Mulla[1], Shreyash Dude[2], Atharva Pawar[3], Kunal Pharande[4], Shubham Suryawanshi[5]
Dept. Computer Science and Engineering of YSPM's YTC, Satara, Maharashtra, India

Abstract: ***This report aims to examine the evolving cybersecurity threats, including DeepFakes, phishing, social engineering, and malware, and analyze detection mechanisms to counter these threats. DeepFakes, generated using advanced AI techniques, pose risks such as identity theft and disinformation, with detection models like CNNs and RNNs showing promise, albeit with reduced effectiveness against high-quality manipulations. Tools like Face Forensics++ are instrumental for training such models. Phishing, which employs deceptive techniques to steal sensitive information, is addressed through URL-based detection systems and datasets such as Phish-Tank. Social engineering, leveraging tactics like pretexting and baiting, highlights the importance of NLP models for detecting manipulation in communications. Malware, encompassing threats like ransomware and spyware, continues to challenge cybersecurity efforts, with machine learning and deep learning approaches proving effective for detection. Tools like Virus Total and Cuckoo Sandbox enhance detection through multi-engine scanning and dynamic analysis. While detection technologies show significant potential, challenges such as real-time threat identification and user awareness underscore the need for integrated, adaptive cybersecurity solutions.***

Keywords: Natural Language Processing (NLP), Convolutional Neural Networks (CNNs), Artificial Neural Networks (RNNs), Uniform Resource Locator (URLs)

I. INTRODUCTION

The rapid advancement of digital technologies has brought transformative benefits, but it has also exposed individuals and organizations to increasingly sophisticated cyber threats. Traditional cybersecurity measures struggle to keep pace with the evolving tactics of malicious actors, who exploit vulnerabilities across diverse attack vectors. From Deep-Fakes that manipulate audio and video to phishing and social engineering schemes that prey on human psychology, modern threats have grown more pervasive and complex.

Despite the availability of specialized tools for detecting specific threats such as malware or phishing, the fragmented nature of these solutions often leaves critical security gaps. Additionally, many detection tools are reactive rather than proactive, making it difficult to prevent threats in real time. This challenge is compounded by a lack of user awareness and education, which undermines the effectiveness of even the most advanced security systems.

To address these issues, there is an urgent need for an integrated cybersecurity protection tool that consolidates multiple detection mechanisms into a single, comprehensive platform. Such a solution must not only provide real-time detection of threats like DeepFakes, phishing, social engineering, and malware but also educate users to strengthen their overall security posture. This project seeks to bridge the gaps in current cybersecurity approaches by developing a robust, unified system capable of safeguarding against the diverse and evolving landscape of cyber risks.

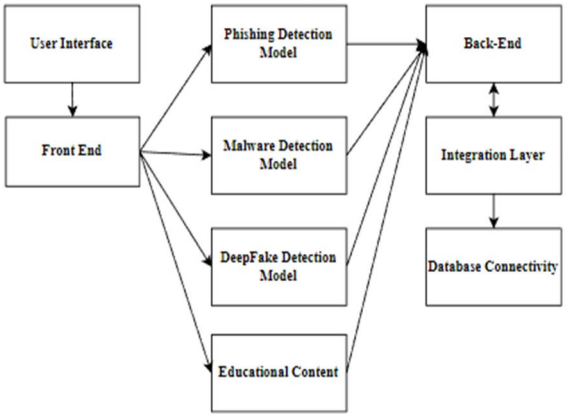


Figure 1: Functional pattern of the Cyber-Security Protection Tool

This diagram represents a software system architecture with distinct components interacting to provide functionality. The User Interface and Front End serve as the interaction point for users. The front end interacts with three detection models: Phishing Detection Model, Malware Detection Model, and DeepFake Detection Model, which analyze and detect threats. The Educational Content module is connected to these models, likely to provide relevant training or awareness to users. These components communicate with the Backend, which manages core processing and connects to the Integration Layer for streamlined operations. The Integration Layer ensures efficient Database Connectivity for data storage and retrieval.

II. LITERATURE SURVEY

This Paper [1] Explores cybersecurity research trends and issues, focusing on countering malware attacks and rootkits, hidden and persistent malware that lives at the operating system's base. Rootkits cause serious problems due to their ability to evade detection and compromise integrity. The research delves into the distribution of rootkits, their working mechanisms, and their impact on system security. The study also evaluated various rootkit protection tools, including Spy DLL Remover, Sanity Check, and Root Repeal, comparing performance-based analysis.

The goal is to find the most effective tools for new users and IT professionals, provide insight into rootkit threat mitigation, and strengthen cybersecurity protection.

This paper [2] proposes a solution to the growing problem of detecting Deepfake videos, which are created using Generative Adversarial Networks (GANs) to swap faces in videos. To aid in detection research, the authors generated a publicly available dataset using the VidTIMIT database, consisting of 640 Deepfake videos with varied quality (320 low-quality and 320 high-quality) produced using open-source GAN-based tools. The study highlights the vulnerability of state-of-the-art face recognition systems, with VGG and Facenet models demonstrating false acceptance rates of 85.62% and 95.00%, respectively. Several detection approaches were evaluated, including audio-visual lip-sync detection, which failed to distinguish Deepfakes effectively, and visual quality metrics, a method adapted from presentation attack detection, which performed best with an equal error rate (EER) of 8.97% on high-quality Deepfakes. The authors emphasize that the training and blending parameters used during GAN-based Deepfake generation significantly influence video quality, making high-quality Deepfakes harder to detect. The paper concludes that Deepfake technology will continue challenging current detection systems, urging the development of advanced multi-modal detection techniques that combine visual, audio, and temporal data. This study lays the foundation for future advancements in Deepfake detection research by offering a benchmark dataset and key insights.

This paper [3] proposes to explore the critical role of cybersecurity in safeguarding sensitive data and ensuring the resilience of modern systems against evolving cyber threats. It aims to highlight the importance of adopting advanced security measures and adaptive frameworks to combat increasingly sophisticated hacking techniques targeting organizations across industries. Additionally, the paper examines emerging technologies like artificial intelligence, machine learning, and blockchain as innovative solutions for enhancing security protocols. By addressing both technological advancements and the human factor, this research seeks to provide a comprehensive understanding of how organizations can effectively mitigate risks, protect valuable assets, and maintain operational integrity in a highly connected world.

This paper [4] examines the rapid advancements in artificial intelligence (AI), machine learning, and deep learning, which have led to both beneficial applications and malicious uses, particularly through Deepfakes—highly realistic fake videos, images, and audio that spread misinformation, provoke political discord, and enable harassment. To address these issues, the paper presents a systematic literature review (SLR) of 112 studies published between 2018 and 2020, categorizing detection methods into four groups: deep learning-based techniques, classical machine learning methods, statistical approaches, and blockchain-based solutions. The findings reveal that deep learning-based methods are the most effective in detecting Deepfakes across various datasets, providing a thorough overview of current strategies to mitigate the risks posed by this emerging threat.

This paper [5] addresses the growing concern regarding high-quality face editing in videos, which can undermine trust in video content. Many face editing algorithms introduce artifacts due to traditional challenges in computer vision, particularly in face tracking and editing.

The paper reviews current facial editing methods, identifies characteristic artifacts in their processing pipelines, and demonstrates that relatively simple visual features can effectively reveal manipulations, such as Deepfakes and Face2Face. These artifact-based methods are intuitive and easily understandable for non-technical audiences, simple to implement, and adaptable to new types of manipulations with minimal data requirements. Despite their simplicity, these methods achieve promising results, with Area Under the Curve (AUC) values reaching as high as 0.866.

This paper [6] focuses on phishing attacks, which are among the simplest and most effective methods for acquiring sensitive user information, such as usernames, passwords, and bank details. As cybercriminals increasingly exploit phishing websites, cybersecurity professionals are seeking reliable detection techniques. The study investigates the use of machine learning for detecting phishing URLs by analyzing the features of both legitimate and phishing URLs. It utilizes algorithms such as Decision Tree, Random Forest, and Support Vector Machine (SVM) to identify phishing websites, comparing their performance based on accuracy, false positive rate, and false negative rate. The ultimate goal is to effectively detect phishing URLs while identifying the most accurate algorithm for this task.

This paper [7] examines phishing, a common internet scam in which attackers impersonate trusted sources to steal personal information or deploy malware via deceptive URLs or files. Traditionally, phishing attacks were carried out through mass spam campaigns targeting a broad audience. However, modern detection methods now utilize machine learning. In this approach, URLs received by users are analyzed using machine learning models to classify them as either phishing or legitimate. Common algorithms employed for this purpose include Support Vector Machines (SVM), Neural Networks, Random Forests, Decision Trees, and XGBoost. The study focuses on the Random Forest and Decision Tree classifiers, which achieved classification accuracies of 87.0% and 82.4%, respectively. These results demonstrate the effectiveness of machine learning in mitigating phishing threats.

This paper [8] examines phishing attacks, a common form of social engineering that targets users' emails to steal sensitive information and potentially lead to larger attacks on corporate or government networks. Despite the existence of various anti-phishing techniques, many are still inefficient and inaccurate. The authors propose a machine learning-based detection technique that utilizes a dataset of over 4,000 phishing emails collected from the University of North Dakota's email service. By selecting 10 relevant features, they constructed a comprehensive dataset for training, validating, and testing several machine learning algorithms. The performance of these algorithms is evaluated using four metrics: probability of detection, probability of miss-detection, probability of false alarm, and overall accuracy. The experimental results demonstrate that artificial neural networks provide superior detection performance compared to other methods.

This paper [9] presents a versatile framework designed to differentiate between malware and clean files using various machine learning algorithms, with a focus on minimizing false positives. The framework is initially tested with cascade one-sided perceptron’s and later with cascade kernelized one-sided perceptron’s. After achieving success on medium-sized datasets of malware and clean files, the framework is expanded to effectively handle larger datasets. This approach aims to enhance malware detection while maintaining high accuracy and reducing false alarms in large-scale applications.

This paper [10] addresses the increasing cybersecurity threat posed by malware, which continuously evolves to target computer systems, smart devices, and large networks, making detection more challenging. The paper conducts a systematic literature review (SLR) of 77 research studies focused on malware detection using machine learning techniques. It presents a comprehensive taxonomy that categorizes various machine learning methods for malware detection, analyzing their strengths and weaknesses in terms of performance accuracy and the ability to identify unexpected attacks. The research examines the classification of machine learning algorithms, identifies obstacles in malware detection, and suggests potential solutions. Additionally, an empirical study is presented to evaluate the performance of several machine learning algorithms, providing insights to guide future research aimed at improving malware detection methods.

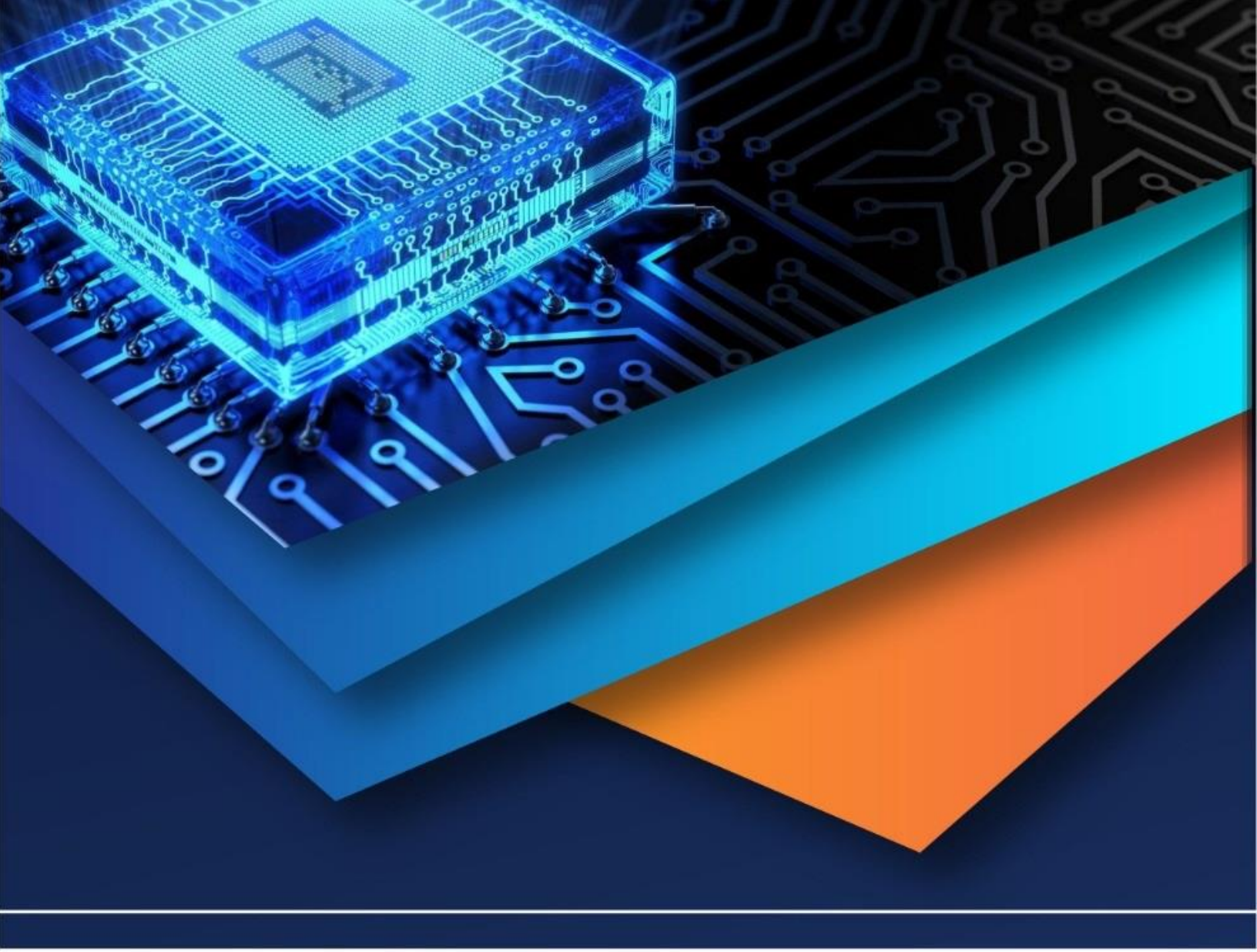
III. CONCLUSION

The Cybersecurity Protection Tool presents an integrated, multi-layered approach to combat the growing variety of cyber threats in today's digital landscape. By combining modules for detecting Malware, Phishing, DeepFakes, Social Engineering, and User Education, the tool addresses both technological and human vulnerabilities. The tool not only identifies and mitigates potential risks in real-time but also educates users, empowering them to make informed decisions and recognize threats effectively. As cyber threats continue to evolve in sophistication, the tool’s proactive detection and prevention mechanisms, along with its educational features, provide a robust defense against a wide range of attacks. This integrated approach, coupled with continuous updates and user awareness, ensures enhanced cybersecurity resilience for both individuals and organizations. Ultimately, the tool aims to bridge the gap between reactive security measures and proactive, user-informed cybersecurity, fostering a safer digital environment for all.

REFERENCES

[1] Ashwini D. Mate, Dr. D. R. Ingle, “Cybersecurity Tools and Methods,”. © 2017 IJCRT | International Conference Proceeding ICGTETM Dec 2017 | ISSN: 2320
[2] Korshunov, P., & Marcel, S. (2018), "DeepFakes: A New Threat to Face Recognition?,"International Conference on Biometrics (ICB).
[3] Mrs. Ashwini Sheth, Mr. Sachin Bhosale, Mr. Farish Kurupkar, “RESEARCH PAPER ON CYBER SECURITY,” CONTEMPORARY RESEARCH IN INDIA (ISSN 2231-2137): SPECIAL ISSUE: APRIL, 2021

[4] Md Shohel Rana, Mohammad Nur Nobi, Beddhu Murali, Andrew H. Sung, "Deepfake Detection: A Systematic Literature Review," IEEE Access (Volume: 10) **(ISSN:** 2169-3536) 10.1109/ACCESS.2022.3154404
[5] Falko Matern, Christian Riess, Marc Stamminger, "Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations," https://ieeexplore.ieee.org/xpl/conhome/8630326/proceeding10.1109/WACVW.2019.00020
[6] Rishikesh Mahajan, Irfan Siddavatam, "Phishing Website Detection using Machine Learning Algorithms," International Journal of Computer Applications (0975 – 8887) Volume 181 – No. 23, October 2018
[7] Saikiran Boppana, Vishnu Ravella, R Kavitha, "Phishing Website Detection Using Machine Learning," 2022 IEEE 7th International conference for Convergence in Technology (I2CT) 10.1109/I2CT54291.2022.9824801
[8] Fatima Salahdine, Zakaria El Mrabet, Naima Kaabouch, "Phishing Attacks Detection A Machine Learning-Based Approach," https://arxiv.org/pdf/2201.10752
[9] Dragos¸ Gavrilut¸ Mihai Cimpoes¸ Dan Anto, Liviu Ciortuz ,"Malware Detection Using Machine Learning," ISBN 978-83-60810-22-4 ISSN 1896-7094, PROCEEDINGS OF THE IMCSIT. VOLUME 4, 2009
[10] Nor Zakiah Gorment, Ali Selamat, Lim Kok Cheng, Ondrej Krejcar, "Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges, and Future Directions", IEEE Access (Volume: 11),10.1109/ACCESS.2023.325697



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY