Archives available at journals.mriindia.com

International Journal of Recent Advances in Engineering and Technology

ISSN: 2347 - 2812

Volume 14 Issue 02s, 2025

AI-Powered Cyber Security Protection Tool

[1]Asma Mulla, [2]Shreyash Dude, [3]Atharva Pawar, [4]Kunal Pharande, [5]Shubham Suryawanshi

[1,2,3,4,5]Dept. Computer Science and Engineering YSPM's YTC, Satara, Maharashtra, India

Email: [1]asmamulla_engg@yes.edu.in, [2]shreyashdude9@gmail.com, [3]atharvapaw123@gmail.com, [4]kunalpharande21@gmail.com, [5]Shubhamsuryawanshi6897@gmail.com

Peer Review Information

Submission: 21 Oct 2025

Revision: 18 Nov 2025

Acceptance: 05 Dec 2025

Keywords

Natural Language Processing (NLP), Convolutional Neural Networks (CNNs), Artificial Neural Networks (RNNs), Uniform Resource Locator (URLs) Introduction (Heading 1)

Abstract

This report delves into the landscape of contemporary cybersecurity threats, with a focus on the dynamic nature of DeepFakes, phishing schemes, social engineering ploys, and the persistent issue of malware. It underscores the challenges posed by DeepFakes, which utilize sophisticated AI to create convincing but false content, leading to risks like identity fraud and the spread of misinformation. The report also examines the role of detection technologies, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), in identifying these threats, while noting the ongoing challenge of detecting high-fidelity DeepFakes. It mentions the utility of tools like Face Forensics++ in training detection models to improve their accuracy.

Phishing, a method of acquiring sensitive information through deceit, is another area of concern highlighted in the report. It discusses the use of URL analysis and resources like Phish-Tank to detect and prevent phishing attacks. The report also addresses social engineering, which manipulates individuals into divulging confidential information, and emphasizes the need for Natural Language Processing (NLP) models to detect such manipulations in communication channels.

Furthermore, the report explores the realm of malware, including dangerous forms like ransomware and spyware, and how they pose ongoing challenges to cybersecurity. It details the application of machine learning and deep learning in malware detection and the use of tools such as Virus Total and Cuckoo Sandbox to enhance detection capabilities through comprehensive scanning and behavioral analysis.

The report concludes by recognizing the potential of current detection technologies while also pointing out the challenges that remain, such as the need for real-time threat detection and raising user awareness. It stresses the importance of developing integrated and adaptive cybersecurity solutions that can evolve in response to the ever- changing threat landscape.

Introduction

The rapid progression of digital innovation has ushered in a new era of connectivity and performance, but it has simultaneously opened the door to a myriad of cyber threats, which are becoming more problematic and harder to predict. The panorama of cybersecurity is under constant strain as malicious entities devise novel strategies to take advantage of device weaknesses. The threats vary from the introduction of DeepFakes, which can convincingly mimic actual audio and visual

© 2025 The Authors. Published by MRI INDIA.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

content, to the use of phishing and social engineering strategies that take advantage of human behavior and trust.

Even as there are committed tools designed to fight precise kinds of threats, inclusive of malware or phishing, these are often remote answers that do not provide a cohesive defense in opposition to the vast spectrum of cyber dangers. The contemporary crop of detection mechanisms is often reactive, lacking the capability to preemptively thwart attacks, which is similarly complex through a well-known deficiency in user schooling on cybersecurity best practices. This gap in awareness can render even the most state-of- the-art security measures much less effective.

To counter those challenges, there is a vital need for a unified cybersecurity framework that amalgamates diverse detection abilities into one holistic platform. This included tool might be designed to provide instant chance detection throughout the board, including but not restricted to DeepFakes, phishing attempts, social engineering ploys, and malware incursions. Furthermore, it'd place a robust emphasis on person schooling to bolster the human element of cybersecurity, noting that knowledgeable users are a vital line of defense.

The purpose of this initiative is to create a comprehensive device that not best shields in opposition to the multifaceted nature of modern cyber risks but also evolves in tandem with the chance landscape, making sure sustained protection in an increasingly digital world.

System Architecture

The device structure integrates a user-friendly interface for interaction, linked to a strong front give up that communicates with specialised detection methods for phishing, malware, and deepfake threats. Those models leverage superior device getting to know strategies to research and classify protection dangers as it should be. The returned end guarantees seamless integration and operation, supported via an integration layer that enables communication between components and database connectivity for information storage and retrieval.

This architecture is designed to offer comprehensive safety by detecting and mitigating numerous cyber threats while also teaching users on cybersecurity practices, hence enhancing common gadget resilience against evolving digital risks.

Proposed Work

Addressing the escalating complexity of cyber threats, this initiative outlines the creation of a cohesive cybersecurity platform that integrates five essential components: modules for detecting Malware, Phishing, DeepFakes, Social Engineering, and a dedicated focus on User Education. The objective is to establish an all-encompassing system that actively identifies and counteracts an array of cyber threats while also enhancing user knowledge to bolster cybersecurity resilience.

The Malware Detection component is designed to recognize and neutralize a spectrum of malicious software, like viruses and ransomware. It will apply machine learning and signature-based methods to scrutinize system activities, files, and processes, thereby safeguarding against potential breaches.

The Phishing Detection component addresses the issue of phishing, which deceives users into disclosing sensitive data. It will employ URL analysis, email scrutiny, and machine learning to spot and thwart phishing endeavors in real time, utilizing resources like Phish-Tank to improve detection precision.

The DeepFake Detection component tackles the emerging challenge of AI-generated media that can spread misinformation and facilitate identity theft. It will use sophisticated AI techniques, including CNNs and RNNs, to scrutinize audiovisual content for signs of manipulation, aiming to detect and prevent the harmful impact of DeepFakes.

The Social Engineering Detection component focuses on the human element of cybersecurity, countering attacks that exploit psychological weaknesses. It will deploy NLP models to identify language patterns indicative of social engineering ploys in textual communications.

The User Education component underscores the significance of an informed user base in cybersecurity. It will offer a range of educational materials, such as tutorials and advisories on prevalent cyber threats, to diminish the success rate of attacks that capitalize on human error.

By amalgamating these components into a single platform, the system will provide instantaneous threat detection and mitigation, presenting a versatile defense mechanism for users and organizations. The educational aspect will keep users apprised and ready to confront novel and evolving threats. The system's architecture will feature a User Interface and Front End to engage with the detection modules, supported by a robust Backend and Integration Layer for efficient data management.

In essence, this endeavor strives to deliver a comprehensive, preemptive, and user-centric cybersecurity strategy, filling the void in existing piecemeal digital security measures.

Design

The login page for the Cybersecurity safety tool is characterized by means of a graceful and modern design that employs a dark color scheme for a modern appearance. This web page is crafted to deliver a sincere user experience, providing awesome radio button choices for customers to either log in to their existing account or to sign up for a brand new one. The interface consists of fields for users to enter their username and password, greater by a convenient toggle characteristic that allows users to reveal their password for verification purposes. A putting orange Login button is designed to stand out, guiding users through the authentication process. This thoughtful layout preference is no longer the most effective aid in navigation, however additionally reinforces a feel of visual hierarchy, making the login method intuitive and available.

The educational page inside the Cybersecurity safety tool is designed to be an informative and tasty aid for users, presenting them with vital expertise about keeping virtual protection. It functions as a warm welcome message and emphasizes the importance of secure online conduct through a visually appealing "live safe online" button, which probably leads to further educational content material or security capabilities. Moreover, the web page consists of a cybersecurity consciousness video from YouTube, indicating a focal point on multimedia training to assist customers understand and observe cybersecurity best practices effectively. The overall layout is person-friendly, making sure that the content material is on the market and attractive to a huge audience, thereby promoting a proactive approach to cybersecurity.

The network visitors Analyzer is an important tool for real-time monitoring of the community overall performance and protection. It offers

functions such as tracking live connections, fact transfer, and response time, which are critical for preserving network performance. The analyzer additionally consists of a network health assessment feature, which helps in identifying capability problems earlier than they impact customers. This tool is designed to offer IT experts the insights needed to control community sources effectively and ensure a dependable and at-ease community environment.

The safety rating Dashboard serves as a complete evaluation of a device's safety fitness, highlighting the general security score, risk blocking off skills, and the reputation of security updates. It emphasizes the significance of proactive security measures through a listing of prioritized guidelines, which include permitting issue authentication, updating passwords, and performing security scans. Moreover, the dashboard tracks recent protection sports, ensuring that each actions, which include password adjustments and logins from new devices, are accounted for and completed, thus providing a clean audit path of protection-related tasks.

The picture shows a person interface for a safety report Generator, designed to supply certain security reviews. This tool permits users to customise their reviews by choosing from diverse options. The 'report alternatives' phase enables users to choose the form of record they need, which includes a security evaluation, and to specify a date range for the document's facts. The 'record Sections' characteristic gives checkboxes for along with different elements in the record, which include the safety rating, threats detected, user activity, and suggestions. as soon as the alternatives are selected, customers can generate the document with the press of a button, imparting a complete evaluate of their machine's protection status.

Development Environment

Programming Language: Python Frameworks: Flask, TensorFlow / PyTorch Libraries: OpenCV, spaCy, Scikit-learn APIs: Virus Total API Database: MySQL

Conclusion

The Cybersecurity protection device affords an included, multi- layered method to fight the evolving form of cyber threats in the latest virtual landscape. With the aid of combining modules for detecting Malware, Phishing, DeepFakes, Social Engineering, and consumer education, the device addresses each technological and human vulnerability. The device no longer handiest identifies and mitigates capability risks in real- time but also educates customers, empowering them to make informed decisions and comprehend threats successfully. As cyber threats continue to evolve in sophistication, the device's proactive detection and prevention mechanisms, at the side of its instructional features, provide a sturdy defense against a wide range of attacks. This integrated technique, coupled with non-stop updates and consumer focus, ensures more suitable cybersecurity resilience for each individual and businesses. In the long run, the device aims to bridge the space between reactive security measures and proactive, person- knowledgeable cybersecurity, fostering a more secure digital environment for all.

Acknowledgments

We amplify our deepest appreciation to all of us who contributed substantially to the successful development of this widespread undertaking report. Their unwavering support, insightful steerage, and precious help had been instrumental in bringing this enterprise to fruition.

Our heartfelt gratitude goes to our mentor, A. S. Mulla, whose understanding, encouragement, and advice were pivotal during this adventure. The steadfast support and route provided with the aid of our mentor have been essential in shaping this venture into a reality.

We are also immensely thankful to Dr. S. V. Balshetwar, Head of the Department of laptop technology and Engineering at YSPM's YTC, Satara, for his management and the conducive environment he fostered. Moreover, our sincere thanks go to Dr. Vikram Patil for the terrific opportunities and aid that substantially benefited our mission.

Furthermore, we make our way bigger to our pals and own family, whose continuous support and encouragement have been a constant supply of motivation. Their perception of our talents and their assistance in overcoming challenges have been critical throughout the timely of entirety of this challenge.

References

Ashwini D. Mate, Dr. D. R. Ingle, "Cybersecurity Tools and Methods,". © 2017 IJCRT | International Conference Proceeding ICGTETM Dec 2017 | ISSN: 2320

Korshunov, P., & Marcel, S. (2018), "DeepFakes: A New Threat to Face Recognition?"

International Conference on Biometrics (ICB).

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

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

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

Rishikesh Mahajan, Irfan Siddavatam, "Phishing Website Detection using Machine Learning Algorithms," International Journal of Computer Applications (0975 – 8887) Volume 181

No. 23, October 2018

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

Fatima Salahdine, Zakaria El Mrabet, Naima Kaabouch, "Phishing Attacks Detection A Machine Learning-Based Approach," https://arxiv.org/pdf/2201.10752

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