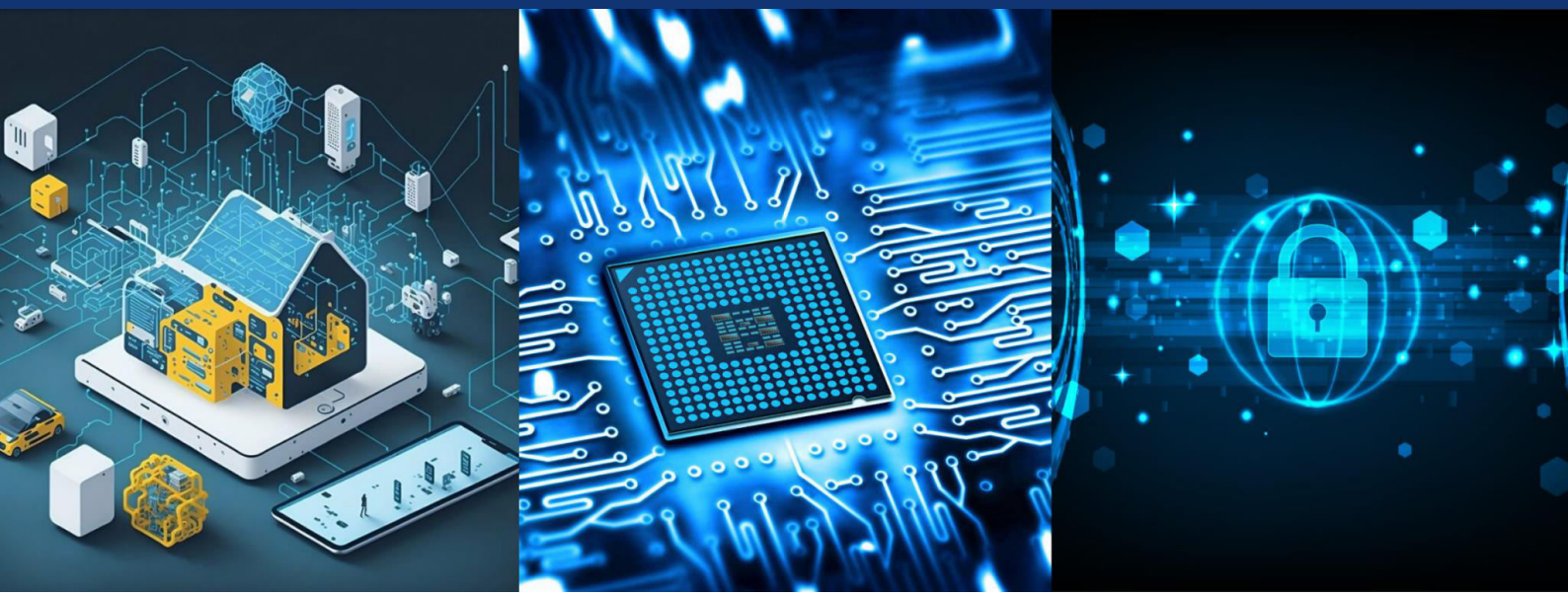
IJIRCCE

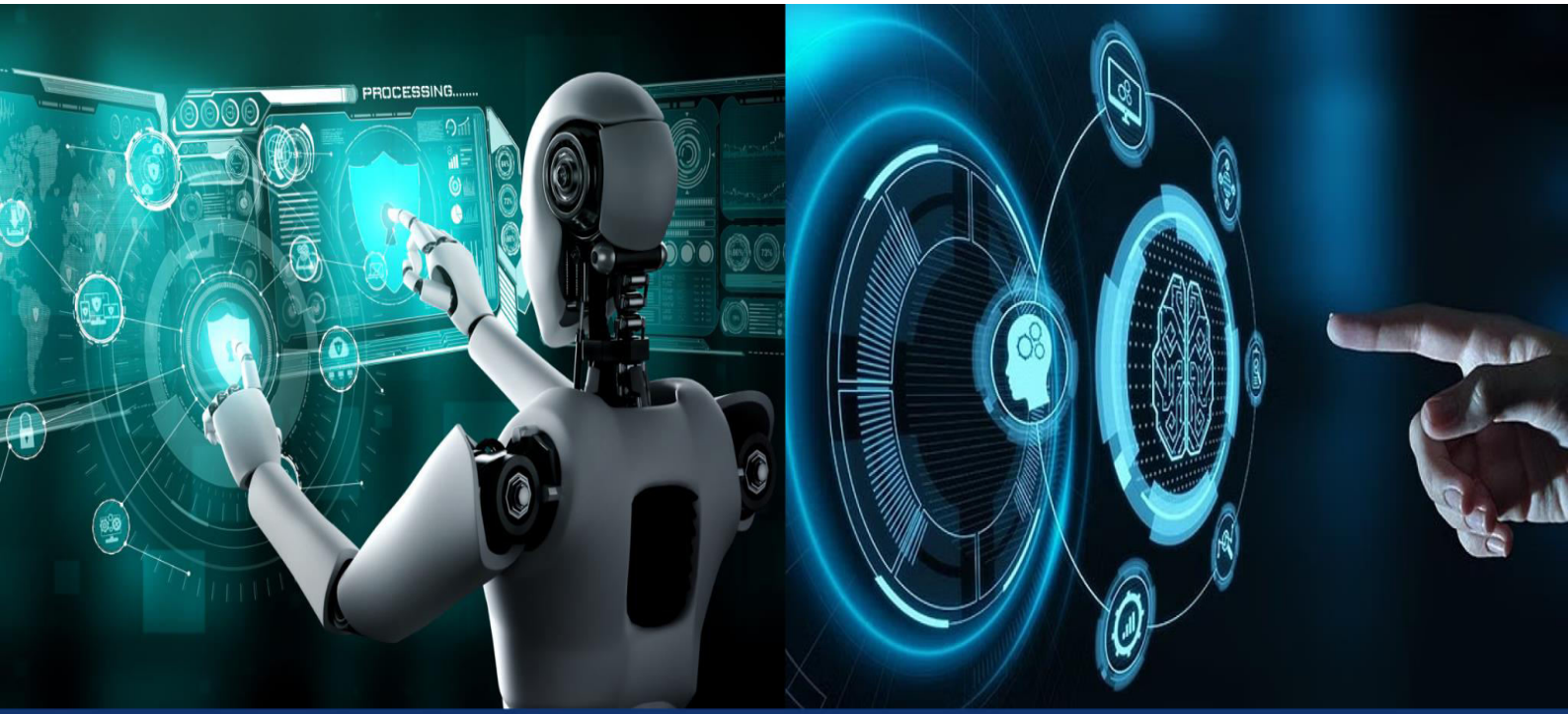
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 6, June 2026

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406083

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Cybersecurity Firmware for Malware Detection and Prevention Using Transformer Learning

Mr. S. Nijar Mohamed [1], Mrs. M. Vijayalakshmi[2]

PG Scholar, Department of Master of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India[1]

Assistant Professor, Department of Master of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India[2]

ABSTRACT: Malware detection plays a crucial role in cyber-security with the increase in malware growth and advancements in cyber-attacks. Malicious software applications, or malware, are the primary source of many security problems. These intentionally manipulative malicious applications intend to perform unauthorized activities on behalf of their originators on the host machines for various reasons such as stealing advanced technologies and intellectual properties, governmental acts of revenge, and tampering sensitive information, to name a few. More efficient mitigation methods are needed due to the fast expansion of malicious software on the internet and their self-modifying abilities, as in polymorphic and metamorphic malware.

This project proposes to develop the MalFree Sandbox with stacked bidirectional long short-term memory (Stacked BiLSTM) and generative pre-trained transformer based (GPT-2) deep learning language models for detecting malicious code offline. The proposed algorithms, namely the bidirectional long short-term memory (BiLSTM) model and the generative pre-trained transformer 2(GPT-2) detect malicious code pieces by examining assembly instructions obtained from static analysis results of Portable Executable (PE) Files. To understand malwares through MalFree Sandbox, care must be taken to sandbox the malwares in an environment that allows for a detailed and comprehensive analysis while also preventing it from being able to further spread.

KEYWORDS: Cybersecurity, Malware Detection, Transformer Learning, Deep Learning, BiLSTM, GPT-2, Malware Prevention, Machine Learning.

I. INTRODUCTION

To implement this system, we will need to develop software for image acquisition, processing, encryption, and transmission. We will also need to design and build hardware components such as biometric sensors and secure storage devices. The project will require collaboration between experts in various fields, including computer science, biomedical engineering, and cryptography. The resulting system will provide a high level of security for medical images, protecting patient privacy and ensuring the integrity of diagnostic information. The goal of this project is to develop a secure system for storing and transmitting medical images using biometric-inspired robust security techniques.

Medical images are critical for diagnosing and treating patients, and it is essential to ensure that they are protected against unauthorized access, modification, or disclosure. The system will use biometric techniques such as fingerprint or iris recognition to authenticate users and ensure that only authorized individuals can access the images. The security of the system will be enhanced through the use of robust encryption algorithms and steganography techniques, which will make it difficult for attackers to intercept and decrypt the images. The increasing use of technology in various aspects of our lives has brought with it the risk of cyber attacks and malware infections.

As a result, cybersecurity has become an essential component of any digital system or network. One important aspect of cybersecurity is the detection of malware, which are malicious software programs designed to infiltrate and damage computer systems. In recent years, there has been a growing interest in using machine learning algorithms for malware detection. One such approach is using transformer-based learning models that have shown promising results in various natural language processing tasks.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406083

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This project aims to develop a cybersecurity firmware system for malware detection using transformer-based learning models. The firmware will be designed to run on various devices such as routers, firewalls, and IoT devices, and will be able to detect and prevent malware attacks in real-time. The project will involve training and fine-tuning transformer-based models on large datasets of known malware to improve their detection accuracy.

II. TECHNOLOGY

The project titled "Cybersecurity Firmware for Malware Detection and Prevention Using Transformer Learning" utilizes advanced Deep Learning and Natural Language Processing (NLP) techniques to identify and prevent malware attacks. The system analyzes Portable Executable (PE) files through static analysis and extracts assembly instructions for feature generation. Malware detection is performed using Stacked BiLSTM and GPT-2 Transformer models, which learn malicious code patterns and classify files as benign or malicious. The system also incorporates feature extraction techniques such as Word2Vec and opcode analysis to improve detection accuracy. Furthermore, it provides real-time malware prevention, threat alerts, and detailed security reports, enabling users and administrators to monitor and protect systems from cyber threats effectively.

III. EXISTING SYSTEM

Anti-virus companies mainly use signature-based detection techniques (it is a technique in which detection of malware is done based on features extracted from previously known malware) to capture malware, but using this technique only known malware can be detected. Zero-day malware (new and unseen malware) can't be detected using this approach. Moreover, malware writers practice evasion techniques like encryption and obfuscation to prevent them from being detected at an early stage. After knowing the catastrophic effects of malware, it is necessary to protect systems from malware. The application of machine learning techniques to malware detection has been an active research area for about twenty years. Researchers have tried to apply various well-known techniques such as Neural Networks, Decision Trees, Support Vector Machines (SVM), ensemble methods and many other popular machine learning algorithms. Recent survey papers provide comprehensive information on malware detection techniques using machine learning algorithms.

Disadvantages

- Detects only known malware threats effectively.
- Cannot easily identify new or advanced malware attacks.
- May generate false positives by marking safe files as malicious.
- Can consume high system resources and reduce performance.
- Limited ability to prevent malware attacks before they occur.
- Depends on frequent signature database updates.
- Becomes vulnerable if updates are not applied regularly.
- Lacks flexibility across different platforms and environments.
- Shortage of skilled malware analysis professionals.
- Limited automation in malware analysis processes.
- Poor integration between different security tools.
- Malware analysis is often time-consuming.
- Manual analysis increases the chance of human errors.

IV. PROPOSED SYSTEM

The proposed system, MalFree, is a cybersecurity online firmware that uses advanced deep learning techniques, specifically stacked bidirectional long short-term memory (Stacked BiLSTM) and generative pre-trained transformer based (GPT-2) language models, to detect and prevent malware attacks. The proposed algorithms, namely proposes a stacked bidirectional long short-term memory (Stacked BiLSTM) and generative pre-trained transformer based (GPT-2) deep learning language models for detecting malicious code. Developed language models using assembly instructions extracted from .text sections of malicious and benign Portable Executable (PE) files. BiLSTM model processes a sequence of input elements across time to learn and analyze the patterns. In contrast, the transformers-based GPT-2 model enables modeling long dependencies between input sequence elements with parallel sequence processing

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406083

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

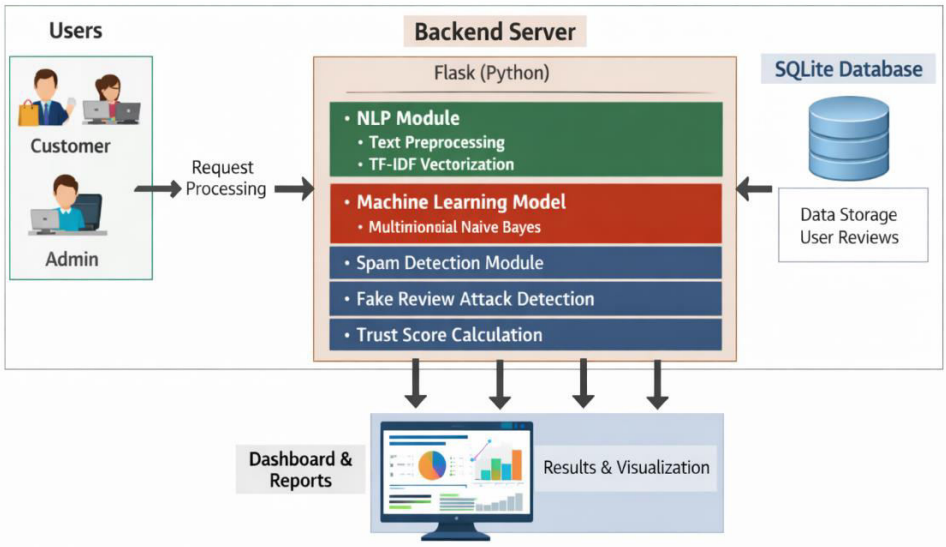
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

in which sequential data constituents can connect with others simultaneously. Then use the perspective of NLP modeling by DL to extract similar characteristics, i.e., syntactic and semantic characteristics of assembly instructions. This models were designed to effectively learn and extract the features and characteristics of assembly language and classify the polarity of files.

Advantages

- Provides real-time malware detection and prevention.
- Detects both known and unknown malware threats.
- Uses advanced deep learning techniques for improved threat analysis.
- Takes proactive measures to prevent malware attacks.
- Works across multiple platforms and environments.
- Highly adaptable and flexible to different system requirements.
- Improves detection accuracy.
- Reduces false positives and false negatives.
- Identifies potential attackers and threat sources.

V. SYSTEM ARCHITECTURE



VI. MODULE DESCRIPTIONS

1. MalFree Web Tool Module

- Provides an online malware analysis platform using Python and Flask
- Allows users to upload and scan executable files
- Generates malware detection reports and security alerts

2. Malware Classification Module

- Uses Deep Learning algorithms for malware detection
- Implements Stacked BiLSTM and GPT-2 models
- Analyzes assembly instructions extracted from PE files

3. Load Dataset Module

- Loads Byte and ASM malware files for analysis
- Collects opcode and assembly instruction information

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406083

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4. Pre-processing Module
- Separates Byte files and ASM files for analysis
- Converts byte files into text format for processing
- Removes unnecessary header information and addresses

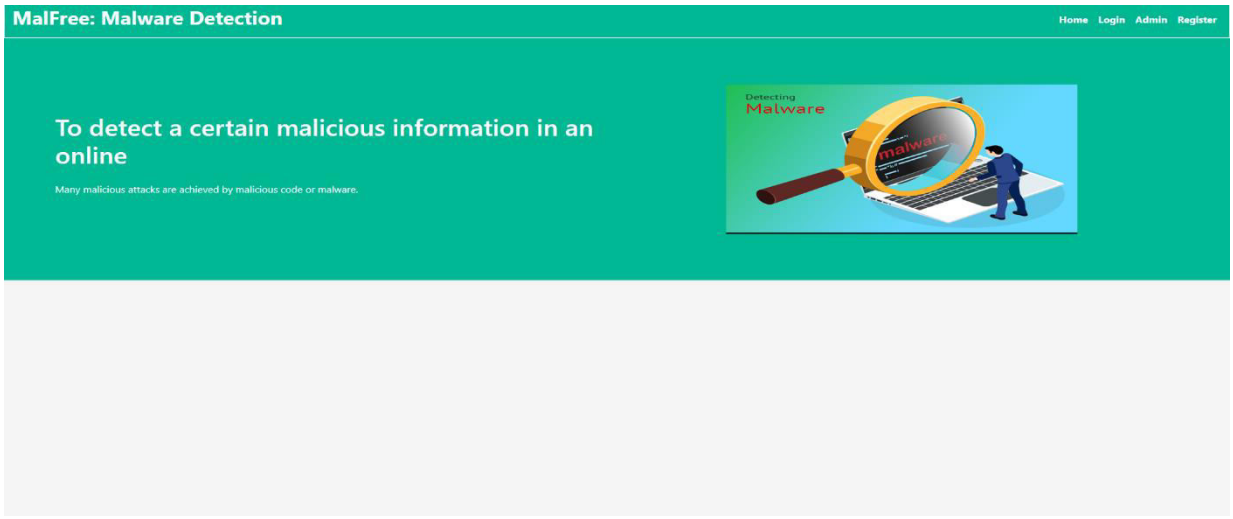
5. Feature Extraction Module
- Extracts meaningful features from malware samples
- Uses Word2Vec for opcode representation
- Identifies important malware behavior patterns

6. Deep Learning Model Module
- Trains Stacked BiLSTM model on malware datasets
- Trains GPT-2 model for advanced malware analysis

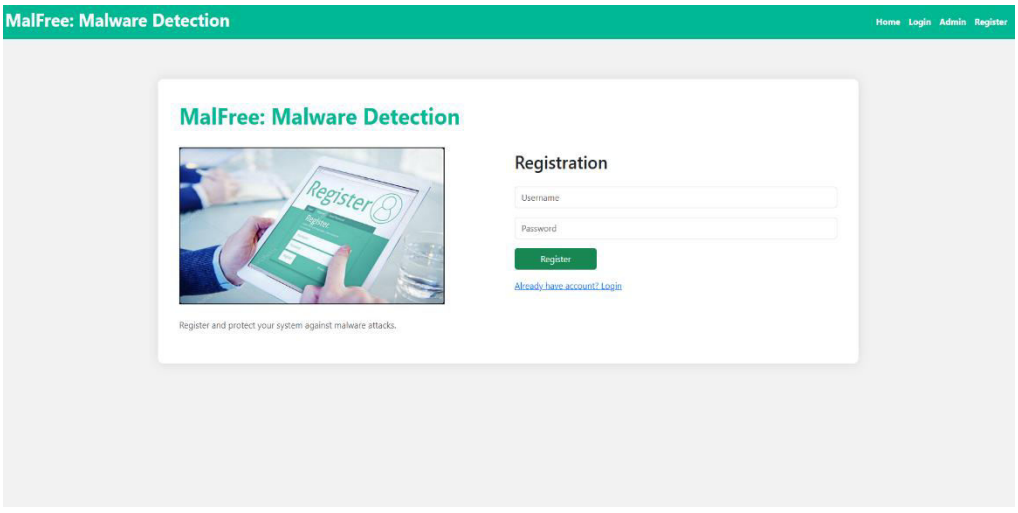
7. Malware Detection & Prevention Module
- Detects malicious files in real time
- Blocks suspicious malware execution

VII. RESULTS

1. HOME PAGE



2. REGISTRATION PAGE



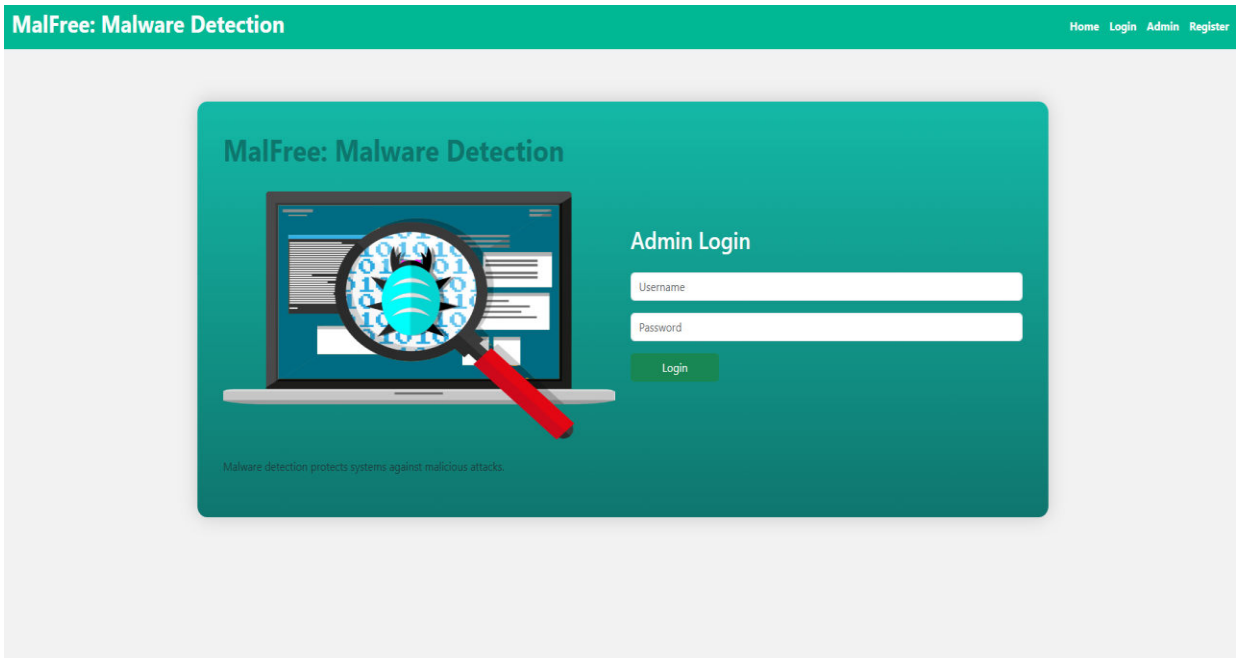
© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406083

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3. ADMIN LOGIN PAGE



4. MALWARE DETECTION

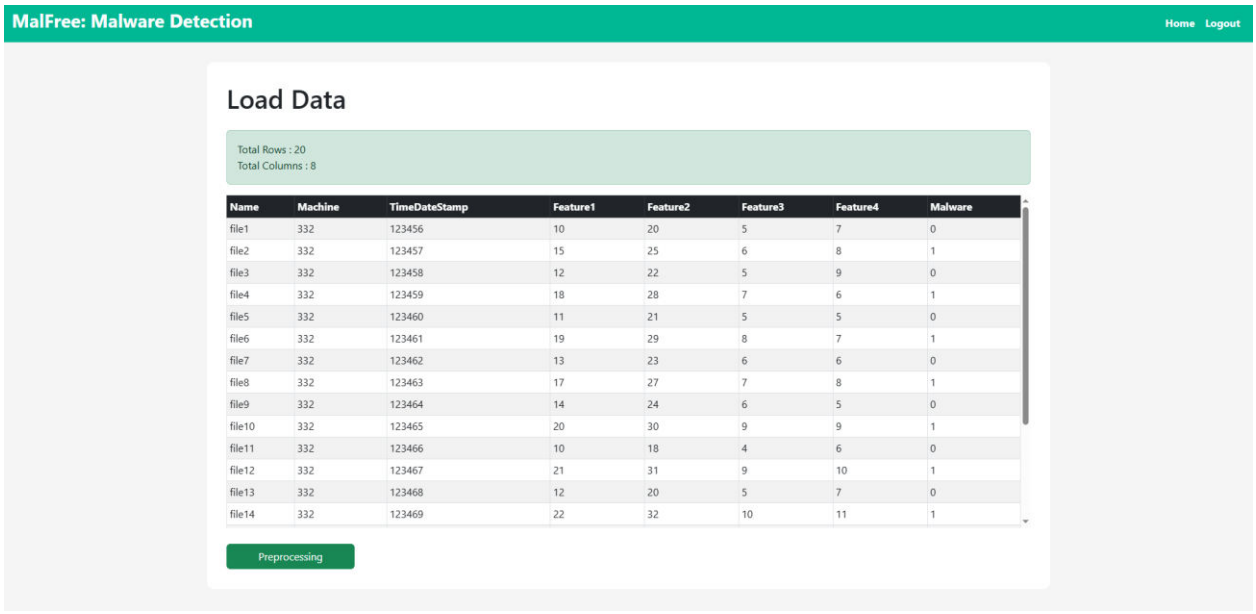
© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406083

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

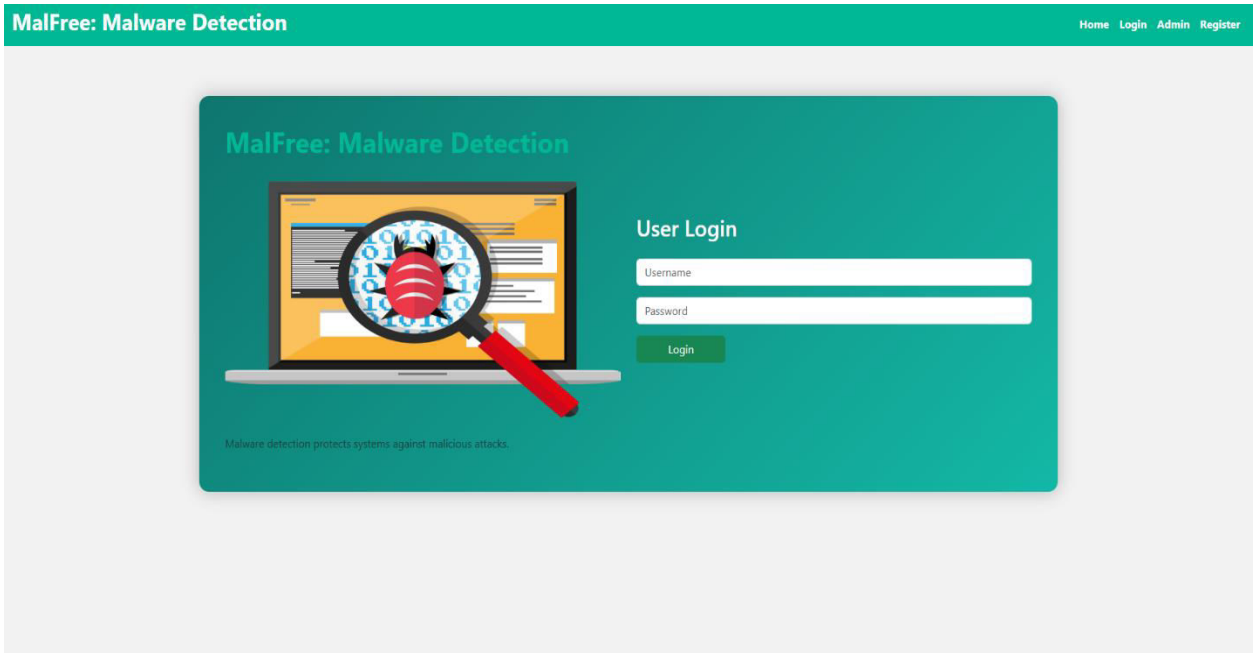
International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

5. Load Data



6. USER LOGIN PAGE



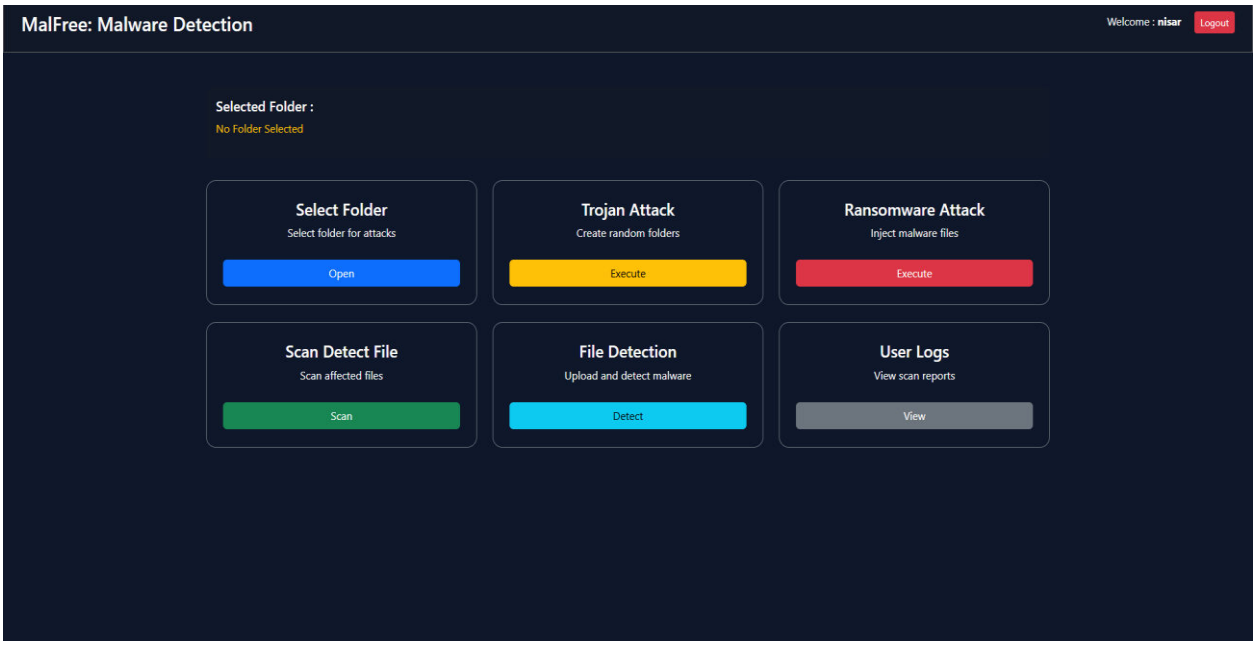
© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406083

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

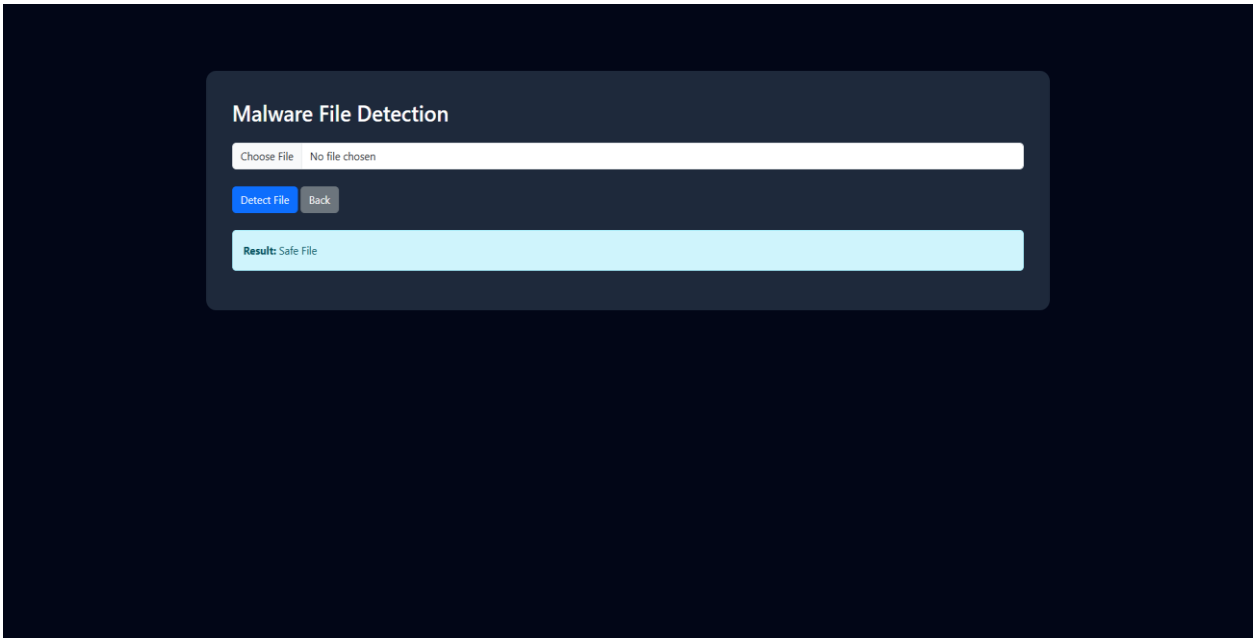
International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

7. ATTACK LIST



8. MALWARE SCAN



www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VIII. CONCLUSION

The development and implementation of "Cybersecurity Firmware for Malware Detection and Prevention Using Transformer Learning" successfully address the major limitations found in traditional malware detection systems. By shifting from static signature-based detection to an intelligent deep learning-based framework, the proposed system provides a more accurate and proactive approach to cybersecurity protection.

The integration of Stacked BiLSTM and GPT-2 Transformer models enables efficient malware classification, real-time threat detection, and automated prevention, ensuring stronger system security and improved operational reliability. The experimental results validate the effectiveness of the framework and demonstrate its potential as a scalable cybersecurity solution for modern digital infrastructures.

IX. FUTURE ENHANCEMENT

The proposed framework provides a strong foundation for intelligent malware detection; however, several opportunities exist for future enhancement. A major improvement would be the integration of advanced predictive machine learning models capable of forecasting malware evolution trends before attacks occur.

Future versions of the framework may also include cloud-based threat intelligence integration, enabling real-time global malware updates and collaborative security monitoring. Another significant enhancement would be support for cross-platform environments, including Windows, Linux, Android, and IoT devices, ensuring broader system protection.

Additionally, the framework can be extended by incorporating Artificial Intelligence-driven recommendation systems for automated threat response and advanced ransomware detection modules. These future enhancements will ensure that the proposed cybersecurity framework remains adaptive, scalable, and capable of addressing the evolving challenges of modern cyber threats.

REFERENCES

[1] Microsoft Malware Classification Challenge (BIG 2015), Kaggle Dataset, 2015.
[2] Abadi, M., Agarwal, A., Barham, P., et al., "TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems", 2016.
[3] Pedregosa, F., Varoquaux, G., Gramfort, A., et al., "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, Vol. 12, pp. 2825–2830, 2011.
[4] Python Software Foundation, Python Documentation, 2026.
[5] Pallets Project, Flask Documentation, 2026.
[6] Devlin, J., Chang, M.W., Lee, K., and Toutanova, K., "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding", 2018.
[7] Radford, A., Wu, J., Child, R., et al., "Language Models are Unsupervised Multitask Learners (GPT-2)", OpenAI, 2019.
[8] S. Vinayakumar, K. P. Soman, and P. Poornachandran, "Applying Deep Learning Approaches for Network Traffic Prediction and Malware Detection," Journal of Cyber Security Technology, 2020.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details