WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cybersense- Ransomware Detection Tool

Dhiraj Prakash[1], Arunachalam M[1], Mr. Kiran Kumar M N[2]

[1]UG Scolar, Departmentof Computer Applications, BMS College Of Commerce and Management, India
[2]HOD, Department of Computer Applications, BMS College Of Commerce and Management, India

A B S T R A C T

Ransomware is a rapidly growing cyber threat that encrypts victims' data and demands ransom payments for restoration. To mitigate this risk, we propose a Ransomware Detection Tool that leverages machine learning to identify and respond to malicious behavior in real-time. This tool extracts relevant features from system activity, including file operations, process behaviors, and entropy patterns, to distinguish between benign and malicious software. By training on a labeled dataset of ransomware and legitimate applications, the model achieves accurate classification and early detection of ransomware threats. Integrated with a user-friendly web interface, the tool enables users to scan files and monitor system activity, offering timely alerts and actionable insights. This solution enhances endpoint security, providing a proactive defense against ransomware attacks with minimal system overhead.

Keywords: Ransomware Detection, Cybersecurity, Machine Learning, Malware Analysis, File Scanning, Behavioral Analysis, Threat Prevention, Real-time Detection, Secure Computing

Introduction

Ransomware has emerged as one of the most significant cybersecurity threats in recent years, targeting individuals, organizations, and critical infrastructure. It is a type of malicious software that encrypts a victim's data and demands a ransom for decryption, often causing severe data loss and operational disruptions. As cyberattacks grow in sophistication, there is an increasing need for intelligent and proactive security measures.

The Ransomware Detection Tool is designed to identify and mitigate such threats before significant harm is done. It uses machine learning techniques to analyze system behavior and detect anomalies that indicate ransomware activity. Key components of the tool include:

- Feature Extraction: Collecting data from file operations, process behaviors, encryption patterns, and system events.
- Classification Model: A trained machine learning model that distinguishes between normal and malicious activity.
- Real-time Monitoring: Continuous analysis of system processes and files to detect potential threats as they occur.
- Alert System: Notifies users immediately upon detection of suspicious activity, allowing for rapid response.

Common techniques used in ransomware detection include entropy analysis, API call monitoring, and behavioral profiling. The tool is also integrated with a lightweight web interface, enabling users to easily upload and scan files for threats. This proactive approach strengthens endpoint security and reduces the risk of data compromise from ransomware attacks.

Literature Review

A. **Bojan Kolosnjaji** used deep learning models (CNNs/RNNs) to detect ransomware based on system behavior, improving detection of complex malware patterns.
B. **Feng, Zhu, and Tao** applied machine learning for behavior-based detection using features like entropy and file activity, achieving accurate classification.
C. **Sgandurra & Muñoz-González** conducted dynamic ransomware analysis in sandbox environments to identify malicious activity during execution.
D. **Vinayakumar et al.** developed deep learning models for analyzing network traffic to detect ransomware and other cyber threats in real time.
E. **Berleant (2023)** explored automating cybersecurity analysis using NLP and ML to extract patterns and detect evolving ransomware threats.
F. **Salatino (2024)** reviewed AI-based tools for malware screening and discussed integrating traditional and modern techniques for ransomware detection.
G. **Li (2022)** studied automated threat report generation from logs, highlighting its role in summarizing ransomware behavior across systems.

* *Corresponding author.* Tel.: +0-000-000-0000 ; fax: +0-000-000-0000.
E-mail address: author@institute.xxx

H. **Ramdhan & Amin (2014)** outlined a structured approach to cybersecurity research, guiding literature sourcing and analysis for threat detection studies.

Methodology

The ransomware detection system involves several key stages to analyze file or system behavior and accurately classify potential ransomware threats. These stages are detailed below:

3.1 Uploading or Monitoring Input

• The system provides a user interface that allows users to upload files or monitor running system processes for analysis.

• It supports various file types and live activity data, ensuring wide applicability for both offline and real-time detection scenarios.

3.2 Feature Extraction

• System-level behaviors such as file creation/modification, encryption patterns, process execution, and API calls are analyzed.

• Entropy values, file size changes, and abnormal access patterns are extracted as features for classification.

• This step is crucial for identifying behavioral anomalies commonly associated with ransomware.

3.3 Model Training and Testing

• A labeled dataset containing benign and ransomware samples is used to train a supervised machine learning model (e.g., Random Forest, SVM, or Neural Network).

• The model learns to differentiate between normal and malicious behaviors based on the extracted features.

• Performance metrics such as accuracy, precision, recall, and F1-score are used to evaluate the model.

3.4 Real-Time Classification

• Once trained, the model is deployed to analyze uploaded files or monitored activities in real time.

• When suspicious patterns are detected, the system classifies the activity as ransomware and triggers an alert.

3.5 Loading of Ransomware Dataset

• A CSV dataset containing labeled records of ransomware and benign file behaviors is used during training and testing.

• The dataset includes various ransomware families to improve model generalization.

3.6 Python Libraries Used

The following Python libraries were utilized in the development of this project:

• Pandas

• NumPy

• Scikit-learn

• Matplotlib

• Joblib

• Seaborn

Results

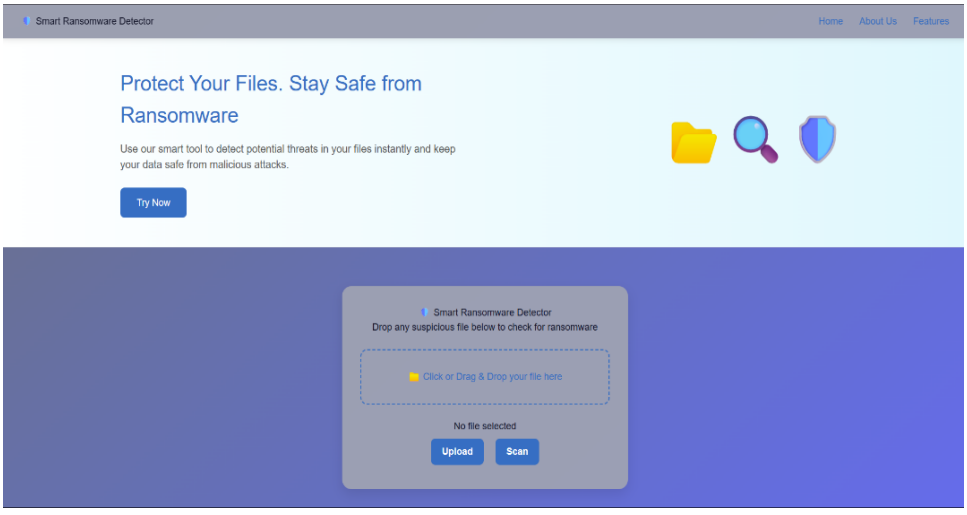

Figure 1

This is the home page of the web application, which is the only page available. It displays a welcome message and provides a brief guide on how to use the application. Users can start using the app directly from this page.

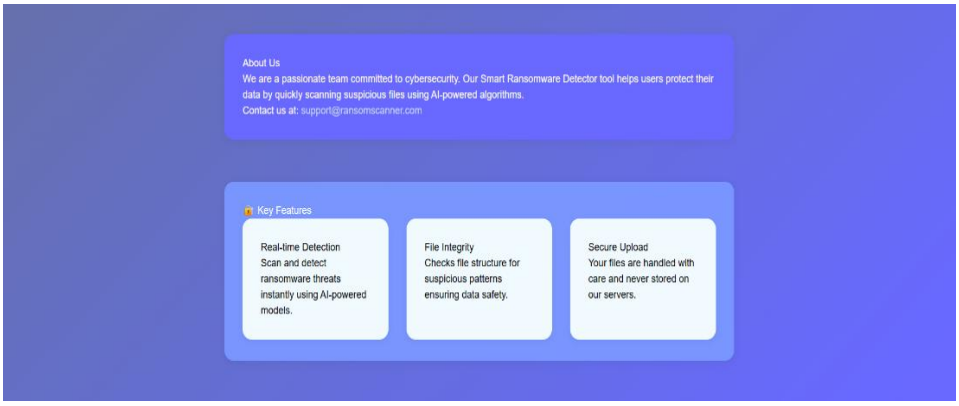

Figure 2

Welcome to our web application, a tool designed to assist users in detecting ransomware threats efficiently and effectively. Our goal is to provide a user-friendly platform that enables both cybersecurity professionals and everyday users to upload files or monitor system activities for potential ransomware attacks. The application processes the input data, analyzes behavioral patterns, and delivers real-time alerts to help protect your valuable data. We are committed to enhancing cybersecurity awareness and offering practical solutions through advanced machine learning technology.

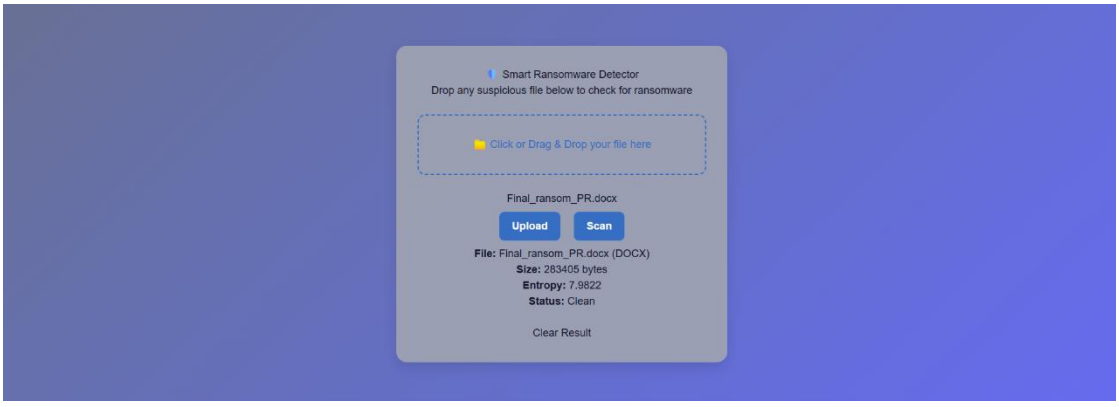

Figure 3

At present, the system has completed its analysis of the uploaded file and has determined it to be free of any indicators of malicious ransomware activity

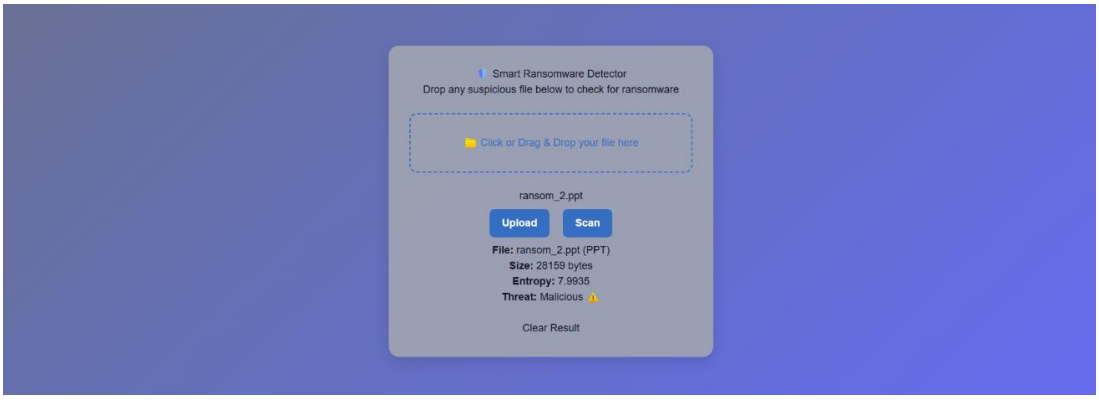

Figure 4

At present, the system has completed its analysis of the uploaded file and identified indicators consistent with malicious ransomware activity.

Conclusion

The ransomware detection system represents a significant advancement in applying machine learning and behavioral analysis to cybersecurity. By leveraging techniques such as feature extraction from file and process behaviours, anomaly detection, and classification algorithms, the system provides an effective approach to identifying ransomware threats from uploaded files. This project enhances the capability to detect and mitigate ransomware attacks, offering valuable protection for users and organizations while contributing to the broader field of proactive cybersecurity.

Acknowledgements

I would like to express my sincere gratitude to my mentors, faculty members, and peers for their valuable guidance, support, and encouragement throughout the development of this ransomware detection tool. I also extend my appreciation to the open-source community for providing essential tools, datasets, and frameworks that made this work possible.

References

1. Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016). Deep learning for ransomware detection. *Proceedings of the 9th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 1–6. https://doi.org/10.1145/2976749.
2. Feng, L., Zhu, Q., & Tao, X. (2017). Behavior-based ransomware detection using machine learning. *IEEE Access*, 5, 18357–18367. https://doi.org/10.1109/ACCESS.2017.2749343
3. IEEE Std 1619™-2007 (2008). IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices. *IEEE Computer Society*.
4. Symantec Security Response. (2020). *Ransomware threats and trends report*. Symantec Corporation.
5. Conti, M., Gangwal, A., & Ruj, S. (2018). Survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, 50(5), 1–37. https://doi.org/10.1145/3137574
6. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018). Detecting malware using deep learning and hash-based visualization. *International Journal of Information Security and Privacy (IJISP)*, 12(4), 61–89. https://doi.org/10.4018/IJISP.2018100104
7. Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, 74, 144–166. **https://doi.org/10.1016/j.cose.2017.11.004**
8. Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016). Cryptolock (and drop it): Stopping ransomware attacks on user data. *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, 303–312. **https://doi.org/10.1109/ICDCS.2016.44**