Real-Time Ransomware Detection and Visualization Framework Using Machine Learning

Sakthidevi I[1], Selvamani V[2], Absal K[3], Arun Siddharth K[4], Shrivasta G N[5]
[1]*Assistant Professor, Adhiyamaan College of Engineering*
[2,3,4,5]*UG Students, Adhiyamaan College of Engineering*

Abstract*—This project proposes a real-time ransomware detection and response framework that leverages machine learning for continuous monitoring and an intuitive dashboard for system activity visualization. The framework continuously analyzes system behaviors such as file operations, process behaviors, and resource utilization to identify potential ransomware threats. Machine learning classifiers are employed to detect abnormal patterns indicative of ransomware, triggering automated mitigation processes, including isolation of affected files or systems. A live dashboard offers real-time insights into system health, detected threats, ongoing mitigation actions, and performance metrics, ensuring transparency for users and enabling informed decision-making. The system is designed to be scalable, allowing for the detection of malware types, such as viruses and trojans, through modular updates. Focused on low-latency detection and minimal system impact, the framework ensures efficient operation while maintaining high detection accuracy. Experimental results demonstrate the framework's effectiveness in detecting and mitigating ransomware attacks in real-time, providing a comprehensive security solution for adaptive defense. This work contributes to the development of proactive malware detection systems, enhancing Ransomware across varied environments.

***Index Terms*—Ransomware Detection, Real-Time Monitoring, Machine Learning, Malware Mitigation**

I. INTRODUCTION

The dynamic nature of ransomware and other malware threats makes it a need to implement sophisticated Ransomware solutions with proactive detection and mitigation. Conventional antivirus solutions depend majorly on signature-based detection mechanisms, which are update-intensive and usually unable to detect new or polymorphic variants of malware. To overcome these limitations, the system proposed herein combines real-time monitoring of systems, heuristic-based analysis, and machine learning-powered behavioral threat detection to offer an adaptive and dynamic defense mechanism against dynamic ransomware threats. The system monitors key system parameters like CPU and memory utilization, file activity, and attempts at encryption constantly, detecting unusual behavior that might signal the existence of ransomware or other malicious activities. In contrast to traditional antivirus products, which mainly respond to recognized threats, this system uses anomaly detection methods to actively scan and eliminate suspected threats before they can do much damage. The machine learning technology included in the system improves detection rates by categorizing threats according to behavioral profiles instead of using static signatures only. Through ongoing optimization of its detection functionality based on training data from varied malware samples, the system maintains enhanced flexibility and minimized false positives. The ransomware detection component inspects file access patterns, unauthorized encryption operations, and process execution behaviors to effectively differentiate benign from malicious activity. Once a threat is detected, the system initiates an automated response for mitigation, quarantining infected files, killing malicious processes, and preventing further harm. The user-friendly interactive interface and dashboard (Fig. 2) give real-time visualizations of system performance, scan progress, discovered threats, and mitigation measures so that users can track Ransomware incidents effectively. The system also includes extensive logging and reporting features to enable users to view previous security breaches and take proper precautions against future attacks. Developed as an executable (.exe) program, the system facilitates easy deployment and user access in various computing environments without the need for complicated installations. Through the incorporation of real-time analysis, predictive threat detection, and automated

response capabilities, the suggested system greatly improves ransomware detection and mitigation. It offers a complete Ransomware framework that not only detects and neutralizes threats efficiently but also reduces system interruptions. The study emphasizes that leveraging behavioral analysis and machine learning should be used to create next-gen security products that can protect against advanced ransomware attacks.

II. RELATED WORKS

Many research works have been done to examine the behavior of ransomware and devise efficient detection and mitigation strategies. Researchers have kept looking for diverse methodologies for augmenting security strategies against ransomware attacks. Some literature works give useful insights regarding current detection strategies, their constraints, and how they could be improved.

Research by [1] Jamil Ispahany et al. investigates the use of machine learning models for detecting ransomware based on adaptability and automation. The research identifies that although ML-based models are more accurate at detection, they tend to operate as black boxes, and hence decision-making becomes hard to understand. In addition, adversarial attacks can tamper with inputs to evade detection, lowering their reliability.

Another research by [2] H. Rodriguez-Bazan et al. examines ransomware detection in Android systems with Convolutional Neural Networks (CNNs). The study proves enhanced malware classification accuracy but highlights the difficulty of acquiring large, labeled datasets. CNN models also consume a lot of computational resources, thus making real-time detection more resource demanding.

Additional work by [4] C. Zhou et al. investigates an I/O-based ransomware detection method that observes file system operations in real-time. Although this approach provides explicit knowledge of ransomware behavior, it has difficulty detecting memory-resident and network-focused ransomware attacks. The study proposes that the integration of I/O-based detection with behavioral analysis could enhance its effectiveness.

The paper of [3] M. L. Hernandez-Jaimes et al. introduces Nilsimsa fingerprinting to improve ransomware detection on the Internet of Medical Things (IoMT). The research points out how digital signatures can facilitate quick threat discovery in healthcare but also identifies weaknesses in distinguishing similar yet functionally different files.

Research by [5] K. Thummapudi et al. explores ransomware detection using processor and disk usage monitoring. Their work highlights the potential of system resource analysis in detecting anomalies associated with ransomware behavior. This method, however, can produce false positives when discriminating between ransomware and benign high-resource programs. The study recommends combining behavioral profiling to increase detection accuracy.

In another paper, [6] J. Ferdous et al. discuss data protection mechanisms against malware in hyper-connected settings. Although encryption-based defenses provide robust security, they are still susceptible to ransomware exploiting storage systems prior to encryption. The authors suggest adaptive security measures to address changing threats.

Moreover, [7] X. Deng et al. introduce an early ransomware detection model based on deep reinforcement learning on Portable Executable (PE) headers. Their method efficiently detects ransomware but needs large, labeled datasets and computational power, which is a scalability issue.

In addition, [8] C. C. Moreira et al. explore detecting new ransomware families based on structural features. Their work enhances variant detection but needs regular updates to combat changing ransomware strategies.

Though these studies are of great value in the detection of ransomware, issues persist with respect to accuracy enhancement, minimizing false positives, and achieving low-latency mitigation. Hybrid techniques that combine machine learning, behavioral analytics, and anomaly detection need to be addressed in future studies to maximize ransomware prevention while maximizing resource usage and detection efficiency.

III. METHODOLOGY

A. Data Collection

The data set used in this research includes extracted system file attributes and their respective threat classifications with the aim of determining ransomware-infected files. The prominent features are file metadata, execution habits, access permissions,

random data, and heuristic-based threat signs. The data set comprises an equal balance of benign and ransomware-impacted system files to facilitate an effective learning process. Missing values were handled, and unwanted features, like file paths and timestamps, were discarded in order to avoid data leakage and ensure the generalizability of the model.

B. Data Preprocessing

Data preprocessing activities included categorical feature encoding for features like file type, execution flags, and discovered threat families. Numerical fields for file entropy, behavior score, and frequency of execution were normalized to provide uniformity. The data was divided into 80% for training and 20% for testing purposes while maintaining equal representation of benign as well as ransomware-infected files. The class imbalance was addressed by using methods such as Random Under-Sampling (RUS) to avoid bias. The features with minimal variance or duplicative information were discarded to make the model more efficient and performant.

C. ML Model for Ransomware Detection

A Random Forest Classifier was used because it can support high-dimensional data and avoid overfitting. The model was trained to classify system files as safe or infected with ransomware based on their behavioral traits and metadata. Hyperparameter tuning was used to tune the number of decision trees, feature selection, and depth limitations to enhance model accuracy and recall. The model's performance in ransomware detection was evaluated using accuracy, precision, recall, and F1-score, ensuring effectiveness with minimal false negatives.

D. Real-Time Ransomware Prediction and Visualization

A dynamic visualization dashboard was created with Dash and Plotly to offer live insights into predictions made by the model. The system continuously scans for file scan results, exhibiting a spike-based waveform visualization of changes in ransomware detection confidence. The live graph is dynamic and depends on identified threats, allowing security analysts to dynamically view trends of ransomware activities and model performance.

E. ML-Powered Threat Detection System

To provide proactive protection, the model trained was deployed into an online ransomware detection system that periodically checks system files for threats of ransomware. The model evaluates incoming files, marks them as safe or malicious, and initiates countermeasures like quarantining infected files, blocking suspicious processes, and alerting users of potential ransomware intrusions. The system becomes increasingly effective over time as it evolves to deal with new variants of ransomware, providing constantly updated protection against ever-changing threats.

IV. ARCITECTURE

The architecture of the system under development is designed to facilitate real-time detection, analysis, and mitigation of ransomware and other ransomware security threats. The system functions as a series of integrated modules that collaborate to ensure total security. Fig 1: Architecture Diagram illustrates the operation flow, which reflects how each module integrates with the system. The system starts with the system monitoring module, which constantly monitors system performance, such as CPU usage, memory usage, and running processes. By monitoring deviations from normal resource usage, this module can identify suspicious activity that could be a sign of a security threat. After a potential anomaly is detected, the scanning module performs a full scan across system files, external storage media, and live URLs to determine potential threats. The scanning function is aimed at offering real-time visualization to ensure transparency and enable users to track current activities. The ransomware detection module also examines scanned files to determine ransomware-related behavior, such as unauthorized encryption efforts and suspicious file changes. By employing machine learning algorithms, this module discriminates between normal and malicious behavior, minimizing false positives and enhancing the accuracy of threat detection. When a security threat is confirmed, the system invokes the threat mitigation module, which quarantines infected files, kills malicious processes, and blocks further harm by limiting unauthorized runs. If required, it tries to recover affected files using recovery processes to reduce data loss.

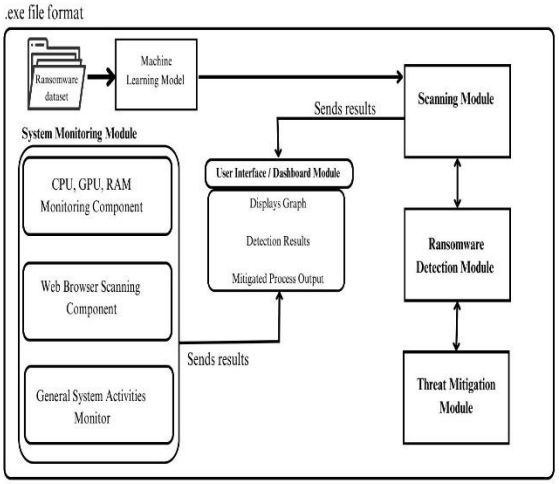

Fig 1: Architecture Diagram

All activities of the system, ranging from monitoring to mitigation, are presented via the user interface and dashboard module. The unified interface gives immediate feedback on system performance, scan progress, threats found, and mitigation steps. Users are able to view reports, examine threat statistics, and undertake further security actions according to system recommendations. The whole system is bundled into an executable program, making it easy to deploy and accessible to users. By combining these modules in a harmonious manner, the system provides an adaptive and proactive security system that can detect and react to changing ransomware threats efficiently.

V. RESULTS AND OUTCOME

The suggested system illustrates a resilient and adaptive mechanism for ransomware detection and mitigation using the combination of machine learning algorithms and real-time system monitoring. The application has an easy-to-use user interface, as illustrated in Fig 2: User Interface, which supports user interaction with primary system functionalities such as real-time scanning, threat detection, and mitigation procedures. The interface promotes transparency by giving users clear information on detected threats, system performance, and security status.

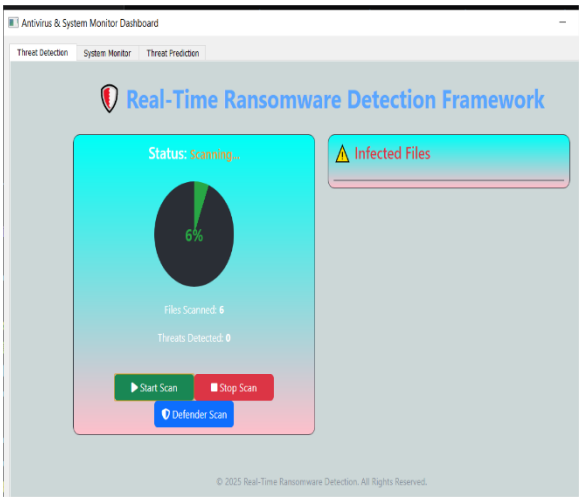

Fig 2: User Interface

The effectiveness of the threat prediction mechanism is demonstrated in Fig 3: Threat Prediction Graph, which graphically represents the classification of files scanned by the system's machine learning model. The findings prove that the predictive model effectively detects ransomware, trojans, and other malware types with minimal false positives, thereby improving overall detection reliability. The model continuously learns from evolving threat trends and dynamically adjusts to make improvements in malware identification and mitigation.

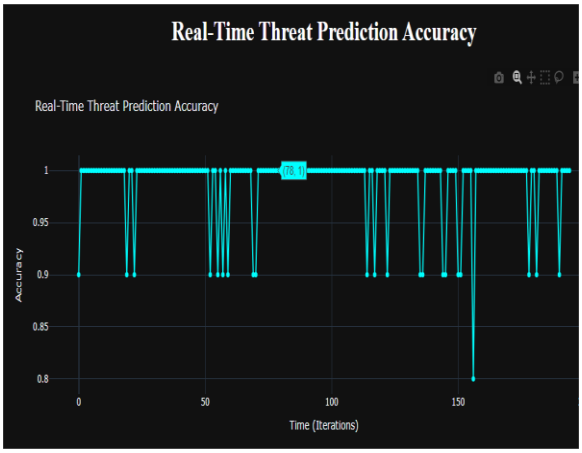

Fig 3: Threat Prediction Graph

System performance indicators, as illustrated in Fig 4: CPU Monitoring Graph, show that the system runs with low resource utilization. The live monitoring of CPU and memory usage ensures that the security operations run effectively without placing a heavy computational load. This ensures that the system is responsive and does not disrupt normal user operations while offering constant threat detection and response.

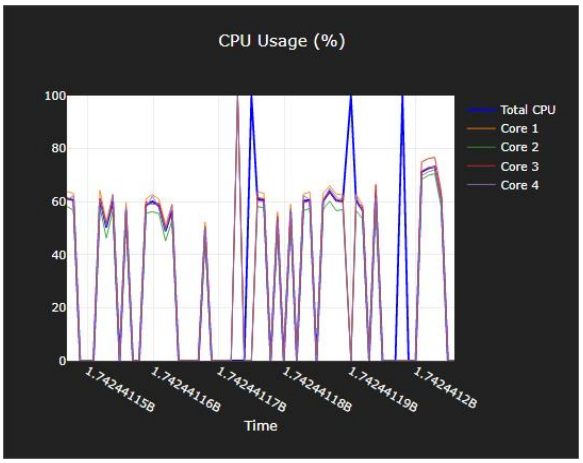

Fig 4: CPU Monitoring Graph

Figure 5 compares the performance of Random Forest, Naïve Bayes, and Support Vector Machine (SVM) in ransomware prediction using Accuracy, Precision, Recall, and F1-Score. Random Forest demonstrates superior performance with an accuracy of 0.987, highlighting its ability to detect complex ransomware behaviors. Its high Precision, Recall, and F1-Score further confirm its reliability in distinguishing ransomware from benign programs. In contrast, Naïve Bayes, with an accuracy of 0.728, performs the worst, likely due to its independence assumption, which is unsuitable for ransomware detection where file behaviors are often interdependent. SVM, achieving approximately 0.85 accuracy, strikes a balance between predictive performance and computational efficiency.

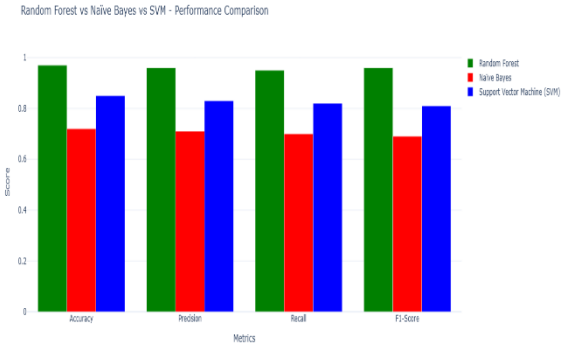

Fig 5: Random Forest vs Naive Bayes vs SVM

Fig 6 gives a detailed comparison of three machine learning algorithms—Random Forest, Naïve Bayes, and Support Vector Machine (SVM)—for ransomware prediction. It shows that Random Forest performs way better than the other models in all the major metrics with an accuracy of 0.9871 and very high precision, recall, and F1-score, and is thus the most accurate model for ransomware classification.

Comparison Table (Random Forest vs. Naïve Bayes vs. SVM):

Metric	Random Forest	Metric	Naïve Bayes	Metric	SVM
Accuracy	0.987152	Accuracy	0.72874	Accuracy	0.85
Precision	0.987154	Precision	0.722095	Precision	0.83
Recall	0.987152	Recall	0.72874	Recall	0.82
F1-Score	0.987151	F1-Score	0.715128	F1-Score	0.81

Fig 6: Performance Metrics

The overall result of the system confirms its efficacy in anticipating and countering ransomware threats. The combination of real-time monitoring, behavioral analysis, and automated response features provides a robust Ransomware framework. The findings highlight the system's potential as a scalable and deployable security solution, offering an intelligent defense against evolving ransomware threats without compromising system stability and usability.

VII. CONCLUSION

In conclusion, the suggested system offers a cost-effective and adaptive method for ransomware detection and mitigation through the incorporation of real-time system monitoring, machine learning-driven threat analysis, and automated mitigation capabilities. The system efficiently detects ransomware threats through the analysis of anomalous system activities, including unauthorized file encryption and atypical resource usage, to guarantee proactive security measures. In contrast to conventional signature-based detection, this solution increases flexibility through the identification of new ransomware strains and reducing false positives. An interactive dashboard provides users with the ability to observe system activity, graph threat trends, and take action instantly when needed. Through the bundling of all functionalities into an executable application, the system guarantees ease of deployment and portability across different environments. Although the system shows excellent performance in threat detection and mitigation, it can be further improved by optimizing the learning model and adding more behavioral analysis methods. This research advances intelligent Ransomware solutions

by enhancing ransomware detection accuracy, response effectiveness, and system security, offering a stronger defense against evolving ransomware threats.

REFERENCES

[1] J. Ispahany, M. R. Islam, M. Z. Islam, and M. A. Khan, "Ransomware Detection Using Machine Learning: A Review, Research Limitations and Future Directions," IEEE Access, May 2024, doi: 10.1109/ACCESS.2024.3397921.

[2] Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramirez-Gutierrez, K. A., & Guevara-Martinez, E.Title: Enhancing Machine Learning Approach Based on Nilsimsa Fingerprinting for Ransomware Detection in IoMT, IEEE Access, Vol. 12, 2024,DOI: 10.1109/ACCESS.2024.3480889.

[3] H. Rodriguez-Bazan, G. Sidorov, and P. J. Escamilla-Ambrosio, "Android ransomware analysis using convolutional neural network and fuzzy hashing features," IEEE Access, vol. 11, pp. 121724–121736, 2023, doi: 10.1109/ACCESS.2023.3328314.

[4] C. Zhou, L. Guo, Y. Hou, Z. Ma, Q. Zhang, M. Wang, Z. Liu, and Y. Jiang, "Limits of I/O-based ransomware detection: An imitation-based attack," in Proc. IEEE Symposium on Security and Privacy (SP), 2023, doi: 10.1109/SP46215.2023.00170.

[5] K. Thummapudi, P. Lama, and R. V. Boppana, "Detection of Ransomware Attacks Using Processor and Disk Usage Data," IEEE Access,May 2023, doi: 10.1109/ACCESS.2023.3279819.

[6] J. Ferdous, R. Islam, M. Bhattacharya, and M. Z. Islam, ''Malware resistant data protection in hyper-connected networks: A survey,'' 2023,arXiv:2307.13164

[7] X. Deng, M. Cen, M. Jiang, and M. Lu, ''Ransomware early detection using deep reinforcement learning on portable executable header,'' Cluster Comput., vol. 27, no. 2, pp. 1867–1881, Apr. 2024, doi: 10.1007/s10586-023-04043-5

[8] C. C. Moreira, D. C. Moreira, and C. Sales, ''A comprehensive analysis combining structural features for detection of new ransomware families,'' J. Inf. Secur. Appl., vol. 81, Mar. 2024, Art. no. 103716, doi: 10.1016/j.jisa.2024.103716.

[9] E. B. Karbab, M. Debbabi, and A. Derhab, ''SwiftR: Cross-platform ransomware fingerprinting using hierarchical neural networks on hybrid,features,'' Exp. Syst. Appl., vol. 225, Sep. 2023, Art. no. 120017, doi: 10.1016/j.eswa.2023.120017.

[10] Q. M. Yaseen, ''The effect of the ransomware dataset age on the detection accuracy of machine learning models,'' Information, vol. 14, no. 3, p. 193,Mar. 2023, doi: 10.3390/info14030193.

[11] L. Liu, X. Kuang, L. Liu, and L. Zhang, ''Defend against adversarial attacks in malware detection through attack space management,''Comput. Secur., vol. 141, Jun. 2024,Art.no.103841,doi:10.1016/j.cose.2024.103841.

[12] M. G. Reshmi, S. Harini, and V. K. Vijayarani, AI-Based Ransomware Detection: A Comprehensive Review," In 2023 International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 1697–1702, doi: 10.1109/ICICCS58265.2023.10197399. 5