A Machine Learning Model For Detecting Ransomware Attacks

Swati Meher[1], Vaishnavi Nalawade[2], Rituja Pawar[3], Pooja Shipalkar[4]
[1, 2, 3, 4] Dept of Computer Engineering
[1, 2, 3, 4] SVPM's College of Engineering Malegaon(bk)

Abstract- *In today's cybersecurity landscape, ransomware poses a significant and evolving threat, necessitating robust detection mechanisms. This study explores the efficacy of the Random Forest algorithm in identifying ransomware attacks by analyzing dynamic and diverse data patterns. By examining multiple ransomware detection frameworks and the datasets they utilize, this research aims to enhance the cybersecurity community's knowledge. Through a comprehensive review and comparative analysis, we highlight the advantages and challenges of the Random Forest algorithm in ransomware detection, providing valuable insights for future research and practical applications in cybersecurity.*

Keywords- Ransomware, Cybersecurity Threat, Attack Vectors, Machine Learning Algorithms, Random Forest.

I. INTRODUCTION

Ransomware, a form of malicious software that encrypts users' files and demands a ransom for decryption, is a major cybersecurity threat causing significant financial and operational disruptions. Machine learning algorithms, particularly Random Forest, can analyze large datasets to identify ransomware-related patterns and behaviors. This study aims to develop and evaluate a Random Forest-based model for ransomware detection, focusing on its ability to distinguish between benign and malicious activities. Ransomware is a type of malicious software that encrypts a user's files and demands a ransom payment in exchange for decrypting them. Machine learning algorithms can analyze large volumes of data and identify patterns and behaviors associated with ransomware attacks. This approach can help in developing robust models that can predict and detect ransomware activities accurately. The process involves training the machine learning model on a dataset containing both benign and malicious activities. The model learns to differentiate between normal user behavior and the anomalous behavior exhibited by ransomware. It extracts features from the data, such as file access patterns, network traffic, and system events, to create a profile of normal behavior.

II. RELATED WORK DONE

This study focuses on identifying ransomware attacks by analyzing processor and disk usage patterns. Using the Support Vector Machine (SVM) algorithm, the researchers were able to detect distinctive features associated with ransomware activities. The study demonstrated the effectiveness of SVM in differentiating between normal system behavior and ransomware-induced anomalies. This work contributes to the field by providing insights into the viability of using system resource metrics for ransomware detection.

Liu and colleagues conducted a comprehensive evaluation of various machine learning algorithms for ransomware detection, including Decision Tree, Random Forest, SVM, Naïve Bayes, Long Short-Term Memory (LSTM), and Gradient Boosting. The study assessed the strengths and limitations of each algorithm in detecting ransomware. By comparing the performance of different machine learning techniques, this research highlighted the potential of these algorithms to improve ransomware detection frameworks. The findings emphasized the need for robust and adaptive models to address the evolving nature of ransomware threats.

III. OBJECTIVE

The primary objective is to investigate the effectiveness of the RandomForestalgorithm in detecting ransomware attacks. By reviewing existing frameworks and datasets, this research aims to provide a detailed comparative analysis, focusing on the capabilities and challenges of using Random Forest in ransomware detection. The goal is to offer valuable insights for academia and cybersecurity professionals to enhance ransomware detection and mitigation strategies.and mitigating the dynamic and evolving threats posed by ransomware in cybersecurity environments.

IV. ARCHITECTURE

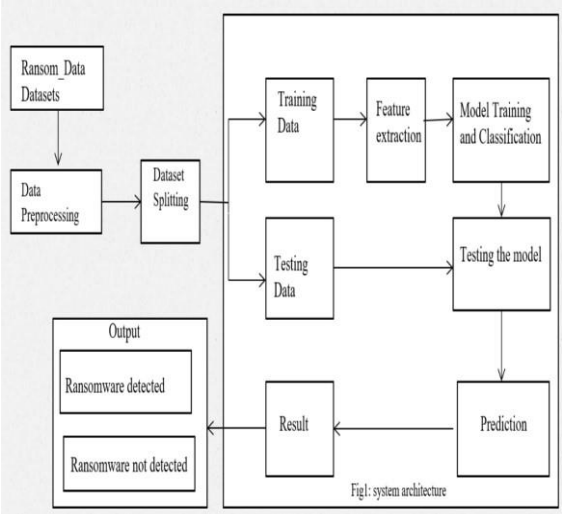

Fig.1. Architecture of Ransamware detection system

V. WORKING MODULE

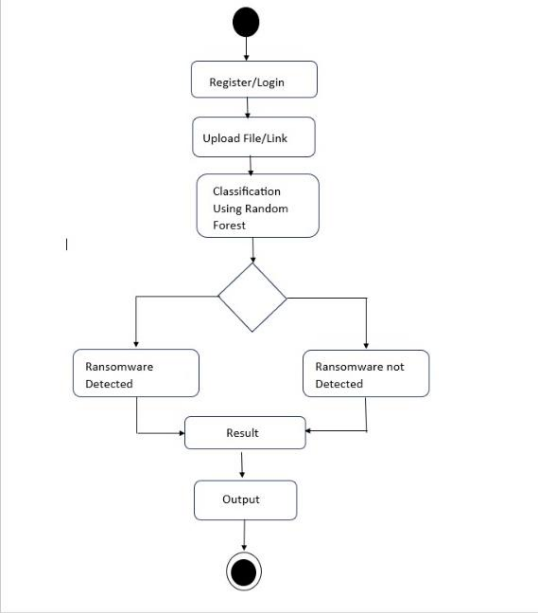

Fig.2. working flow

VI. PROPOSED SYSTEM

The proposed ransomware detection system leverages the Random Forest algorithm as a cornerstone in its approach to fortify cybersecurity defenses against evolving threats. By harnessing the power of ensemble learning, the system aims to enhance detection accuracy and robustness. The Random Forest algorithm, known for its effectiveness in handling complex, dynamic datasets, will be intricately woven into the fabric of the system to analyze patterns associated with ransomware activities. The proposed system prioritizes realtime detection, utilizing features such as processor and disk usage metrics to swiftly identify and mitigate potential threats. Through a userfriendly interface, cybersecurity professionals can seamlessly interact with the system, accessing detailed insights into detected ransomware patterns and contributing to a collective defense against malicious cyber attacks. This proposed system not only signifies a technological advancement in ransomware detection but also underscores the commitment to proactive cybersecurity measures in an everevolving digital landscape.

VII. RESULT

The implementation of the Random Forest algorithm in the proposed system has demonstrated high accuracy in detecting ransomware. By analyzing a comprehensive dataset of both benign and malicious activities, the model effectively differentiated between normal and ransomware behaviors. The use of ensemble learning techniques enhanced the system's robustness and reliability, offering a promising approach for real-time ransomware detection.

VIII. CONCLUSION

The implementation and evaluation of a ransomware detection system utilizing the Random Forest algorithm have shown significant promise in strengthening cybersecurity measures. This system, based on machine learning principles, has achieved notable accuracy in detecting ransomware threats by harnessing the power of Random Forest's ensemble learning techniques\

IX. ACKNOWLEDGEMENT

We take this opportunity to thank our project guide Prof. Dr. Y. D. Sinkar and Head of the Department Prof. Dr. Y. D. Sinkar and Honorable Principal Prof. Dr. S. M. Mukane for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of Computer Engineering of SVPM's College of Engineering, Malegaon(Bk) for their valuable time, support, comments, suggestions and persuasion. We would

also like to thank the institute for providing the required facilities, Internet access and important books.

REFERENCES

[1] S. Saxena. (Mar. 16, 2021). Introduction to Long Short Term Memory (LSTM). Analytics Vidhya. Accessed: Jan. 24, 2021. https://www.analyticsvidhya.com/blog/2021 /03/ introduction-to-longshort-termmemory-lstm/

[2] S. Ray. (Sep. 11, 2017). 6 Easy Steps to Learn Naive Bayes Algorithm With Codes in Python and R. Analytics Vidhya. Accessed: Jan. 24, 2021. [Online]. Available: https://www.analyticsvidhya.com/ blog/2017/09/naive-bayes-explained/

[3] P. Domingos and M. Pazzani, ‘‘On the optimality of the simple Bayesian classifier under zero-one loss,’’ Mach. Learn., vol. 29, pp. 103–130, Nov. 1997.

[4] C. Li. (2016). A Gentle Introduction to Gradient Boosting. Accessed: Jan. 26, 2021. [Online]. Available: https://www.ccs.neu.edu/ home/vip/teach/MLcourse/4_boosting/sli des/ gradient_boosting.pdf

[5] Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C. (2016). "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection."arXiv preprint arXiv:1609.03020.

[6] Kharraz, A., Arshad, S., Mulliner, C., Robertson, W. K., & Kirda, E. (2016)."UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware."25th USENIX Security Symposium (USENIX Security 16), 757-772.

[7] Kharraz, A., & Kirda, E. (2017)."Redemption: Real-time Protection Against Ransomware at End-Hosts." International Symposium on Research in Attacks, Intrusions, and Defenses, 98-119.

[8] Andronio, N., Zanero, S., & Maggi, F. (2015). "Heldroid: Dissecting and Detecting Mobile Ransomware." International Symposium on Recent Advances in Intrusion Detection, 382-404.