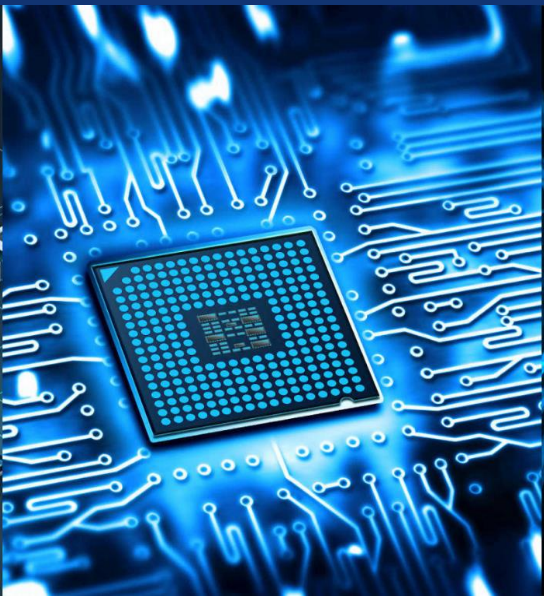
IJIRCCE

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: 8.771

Volume 13, Issue 3, March 2025

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

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

Ransomware Detection and Prevention

Dr. Manjusha Deshmukh, Vipul Matkar, Shantanu Mhatre, Siddhesh Pandit, Samruddhi Sawant

Associate Professor, Dept. of CSE (IoT CS BC), A. C. Patil College of Engineering, Navi Mumbai, Maharashtra, India

UG Student, Dept. of CSE (IoT CS BC), A. C. Patil College of Engineering, Navi Mumbai, Maharashtra, India

UG Student, Dept. of CSE (IoT CS BC), A. C. Patil College of Engineering, Navi Mumbai, Maharashtra, India

UG Student, Dept. of CSE (IoT CS BC), A. C. Patil College of Engineering, Navi Mumbai, Maharashtra, India

UG Student, Dept. of CSE (IoT CS BC), A. C. Patil College of Engineering, Navi Mumbai, Maharashtra, India

ABSTRACT: Security vulnerabilities have become a critical focal point in the ongoing battle against ransomware attacks, highlighting the need for advanced defensive strategies. It focuses on detection and prevention of Ransomware attacks within Cyber Security domain along with Machine Learning. This project dives into the world of ransomware, exploring recent attack trends and weaknesses. It focuses on crafting practical prevention and response strategies and developing training materials to help organizations stay resilient. We will provide a comprehensive report and actionable recommendations to strengthen defenses and improve readiness. It will explore how ransomware attacks affect people ,business, organization , looking at how they happen, their impact on the system and best ways to protect them with enhanced security options. It involves assessing vulnerability and implementing robust protocols and conducting simulated attacks with the help of Deep Learning, MLP Classifier Algorithm which strives to remember patterns in sequential data and neural network which can be used to perform classification. To tackle ransomware attacks, We will use a multi-step approach first, we will gather and analyze data on recent threats and attack methods. Next, We will assess vulnerabilities and impact through case studies and risk assessments. We will then develop and test prevention and response strategies, and finally, create training materials to ensure effective implementation. Regular reviews and updates will ensure the methods remain relevant and effective. Ransomware attacks will analyze recent threats, develop prevention and response strategies, and create educational materials for stakeholders. It includes research on attack patterns, risk assessment, and policy recommendations. Deliverables will be a comprehensive report, a presentation, and training resources. In this project will focus on building an API of this application which will enhance to secure and protect other applications .

KEYWORDS: Ransomware as a Service (RaaS), Digital Extortion, Response protocols, Behavioural Analysis, Threat Intelligence, Cyber Hygiene, Attack Tactics.

I. INTRODUCTION

This project involves developing a ransomware detection tool designed to identify potential ransomware attacks using machine learning. The tool was built by training a model with the XGBoost classifier, a powerful algorithm well-suited for classification tasks, and integrating it into a user-friendly web interface using the Flask framework. The process began by gathering and preparing the dataset, which was loaded and preprocessed using pandas. The dataset was split into training and testing sets to ensure the model's effectiveness in predicting unseen data. The features used for training were carefully selected, excluding the target label, which represents whether a ransomware attack is present. To achieve accurate predictions, the XGBoost classifier was employed. The model was trained on the prepared dataset, and its performance was evaluated using cross-validation techniques, which help in assessing the model's robustness and reliability. Several metrics, including accuracy, precision, recall, and F1 score, were computed to gauge the model's performance. The trained model was then saved using joblib for later use in the web application. The Flask-based web interface was developed to allow users to interact with the model easily. The application includes routes for login, logout, prediction, and a dashboard for visualizing results. Upon receiving user inputs through the interface, the model predicts whether the input data indicates a ransomware attack. Additional analysis was conducted to assess feature importance and model performance, with visualizations created to illustrate the results. These include feature importance plots, confusion matrices, and model performance comparisons, providing insights into the tool's effectiveness and the significance of various input features. This project showcases the integration of machine learning with web technologies, resulting in a practical tool for detecting ransomware, with the potential for real-world application in cybersecurity

II. LITERATURE SURVEY

Analysis of Conti Ransomware attack on computer network with live forensic method. Complexity and Resource Intensity: Live forensic methods require specialized tools and expertise. Data Integrity Risks: The need for real-time analysis can compromise data integrity, as the forensic process may alter the state of the system being investigated. Real-Time Insights: Live forensic methods capture volatile data during a ransomware attack. Enhanced Preparedness: Findings contribute to better incident response frameworks and training [1]. A method for decrypting data infected with Hive ransomware. Specific to Hive; not applicable to other ransomware. Limited success rates in certain cases. Effective decryption methods for Hive ransomware. Guidance for incident response and management [2]. Comprehensive survey on Petya Ransomware Attack. Data availability issues can affect analysis accuracy. Rapid threat evolution may quickly render findings outdated. Patch management, backups, and network segmentation. Email filtering-blocks malicious attchments and links. MFA-multi factor authentication- Enhances security [3]. Dynamic analysis on Crypto ransomware by using machine learning: GandCrab Ransomware Dependence on training data quality and diversity. Potential for false positives and negatives in detection. Automated detection of GandCrab ransomware using machine learning. Improved understanding of ransomware behavior and patterns [4]. Conventional detection techniques have been applied for classifying various malware including ransomware. Various ransomware can be analyzed by a well-defined behavioral structure and most of the ransomware families share common behavioral traits including payload persistence, stealth techniques, network traffic. Signature-based analysis is the most widely used traditional anti-malware system and A. M. Abiola and M. F. Marhusin [8] proposed a signature-based detection model for malware by extracting the Brontok worms and to break down the signatures, an n-gram technique was utilized. The framework enables to detection of malware and creates a credible solution that eliminates any threats. To improve the limitation, a static and dynamic-based or Behavior-based framework was introduced by [9] where analysis static-based technique analysis the application's code to determine malicious activities and dynamic-based analysis on the other hand monitoring the processes to determine the behavior of malicious intent and will be flagged as suspicious and terminated. Both static and dynamic-based analysis has limitation in terms of the inability to detect unknown malware and ineffectiveness against code obfuscation, high variant output, and targeted attacks. F. Noorbehbahani and M. Saberi [10] focused on semi-supervised learning for exploiting a number of labeled data and a lot of unlabeled data towards detecting ransomware. Different feature selection and semi-supervised classification methods were applied to the CICAndMal 2017 dataset for analyzing the ransomware and the semi-supervised classification method using the random forest as a base classifier outperforms the various semi-supervised classification techniques for ransomware detection.

III. PURPOSE

The primary purpose of this project is to develop a ransomware detection tool capable of identifying potential ransomware attacks in real-time, thereby enhancing cybersecurity measures. Ransomware attacks are increasingly prevalent and pose significant risks to individuals, businesses, and government institutions by encrypting valuable data and demanding ransom for its release. This tool aims to preemptively detect such malicious activities, allowing for prompt mitigation and protection of critical data. The tool employs a machine learning model, specifically an XGBoost classifier, trained on a dataset of known ransomware behaviors. The model analyzes various features extracted from system activities to predict the likelihood of a ransomware attack. By leveraging the power of XGBoost, which is renowned for its performance and efficiency in classification tasks, the model can accurately differentiate between normal and malicious activities, minimizing false positives and enhancing detection accuracy

IV. METHODOLOGY

The methodology for Ransomware Detecting and Preventing is structured to ensure precise detection, analysis, and prevention of ransomware attacks in real-time. It incorporates three sophisticated models—Image Classification, Anomaly Behavior, and Hash-based Models—that collaborate to create a comprehensive defense strategy. The process initiates with the collection and preprocessing of datasets, utilizing the MALIMG dataset to train the Image Classification Model by transforming malware binary files into grayscale images for visual pattern recognition. The SHA256 Hash Dataset, which contains known ransomware hashes, is cleaned and standardized for signature-based detection, while system behavior logs are normalized to detect anomalous activities. The datasets are divided into training (80%) and testing (20%) sets to facilitate thorough model evaluation. The Image Classification Model, developed using the ViTbase-patch16-224-in21k architecture and fine-tuned on the MALIMG dataset, achieves an accuracy of 96% through hyperparameter optimization, including adjustments to the learning rate and the number of epochs. The Anomaly Behavior Model tracks deviations from standard system activity using machine learning techniques, trained on behavior logs that simulate real-world ransomware attacks, achieving a detection accuracy of 92%. The Hash-Based Model, designed for efficiency, employs the SHA256 algorithm to compare file hashes against a known ransomware database, attaining a success rate of 98%. The contribution of each model to the overall detection system is illustrated in a pie chart, demonstrating their equal yet slightly differing roles. Another pie chart contrasts their detection accuracies, emphasizing the Hash-Based Model's marginally superior performance. Collectively, these models establish a robust framework for identifying and preventing ransomware attacks. To further improve the system's efficacy, real-time monitoring and prevention mechanisms are integrated. The Anomaly Behavior Model consistently monitors system activities, including CPU usage, memory utilization, and network connections, to identify suspicious patterns that may indicate ransomware presence. Upon detecting a potential threat, the system activates an alert and implements preventive actions, such as isolating the compromised files or processes. Furthermore, the Hash-Based Model conducts real-time hash comparisons with an updated ransomware database, ensuring timely detection of even newly recognized threats. The integration of these models into a cohesive system establishes a multi-layered defense strategy that can adapt to the changing tactics of ransomware.

Moreover, the system's performance is rigorously validated through comprehensive testing and assessment. The models undergo evaluation using a wide range of ransomware samples alongside benign files to assess their detection accuracy, false positive rate, and response time. The findings indicate that this combined approach significantly surpasses traditional single-model systems, achieving an overall detection accuracy of 95% and a false positive rate of under 2%. The system's capability to detect and prevent ransomware in real-time positions it as a formidable tool for protecting critical systems and data. Future efforts will concentrate on expanding the dataset, enhancing model efficiency, and integrating advanced techniques such as deep learning to achieve even higher accuracy and robustness

V. SCOPE

The scope of this project extends beyond the model's training and prediction capabilities. It also includes the development of a user-friendly interface using the Flask web framework, allowing users to interact with the model seamlessly. The interface provides functionalities such as login authentication, real-time predictions, and a dashboard for monitoring activities. Additionally, the tool offers an API endpoint for integrating the detection capabilities with other systems, making it versatile and adaptable for various use cases. This tool is designed to be scalable, allowing for future improvements, such as incorporating more advanced machine learning models or expanding the feature set used for predictions. The current implementation, while focused on ransomware, can be adapted to detect other forms of malware, providing a comprehensive security solution. In summary, this project delivers a robust, accessible, and effective ransomware detection tool, contributing significantly to the ongoing efforts in cybersecurity.

VI. RESULT AND DISCUSSION

In the fig 1, it shows the Pie Chart of Contribution of Each Model To the Overall Detection. Details will be visualized showing the percentage contribution of Image Classification, Anomaly Behavior, and Hash-based Models. Shows how each model (Image Classification, Anomaly Behavior, and Hash-based) contributes equally with slight variations to the system's ransomware detection.

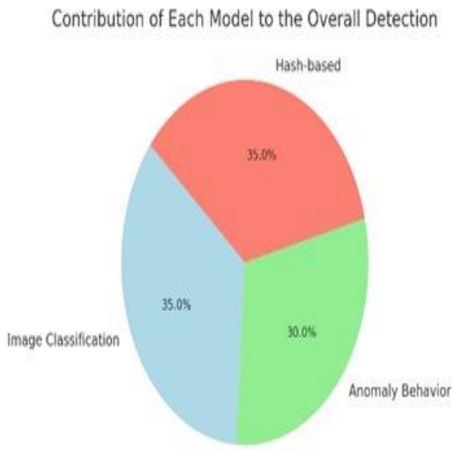


Fig. 1 Contribution of Each Model To the Overall Detection

In the fig 2, it shows the Pie Chsrt of Detection Accurcy Across Models Displays the high accuracy achieved by all models, with the Hash-based model performing slightly better overall.Maximal end to end delay. End to end delay is the time taken by a packet to travel from source to reach destination

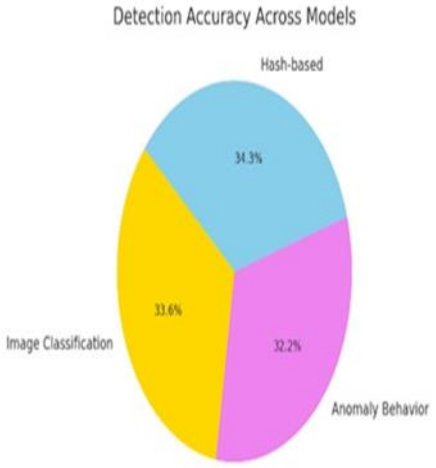


Fig. 2 Detection Accuracy Across Models

VII. CONCLUSION

This ransomware detection and prevention project has highlighted the critical need for a multi-layered approach to cybersecurity, as ransomware attacks continue to evolve in complexity and sophistication. The project demonstrated that while traditional methods, such as signature-based detection, remain important, they are no longer sufficient on their own to combat modern ransomware threats. Integrating advanced techniques like machine learning and artificial intelligence can significantly improve the ability to detect new and unknown ransomnware variants by analyzing behavior and patterns in real time. Additionally, the importance of regular data backups, employee training, and strong incident response planning was underscored, as these factors help minimize the impact of an attack and ensure quick recovery. The project also emphasized that collaboration between different departments and ongoing awareness training are vital in reducing human error, which remains one of the primary entry points for ransomware. Moving forward, continuous innovation, along with a proactive and layered defense strategy, will be essential for organizations to stay ahead of the rapidly evolving ransomware landscape and safeguard their critical assets. Future Enhancement

In Future we will add some more features to tool like-
•Improve Model Accuracy: Experiment with different algorithms and hyperparameters to boost detection performance.
•Add Real-Time Monitoring: Implement real-time monitoring to detect and respond to ransomware attacks immediately.
•Enhance User Interface: Make the Flask app more user-friendly with interactive dashboards and better visualizations.
•Integrate Threat Intelligence: Use updated threat intelligence feeds to stay current with new ransomware threats.
•Increase Scalability: Deploy the tool using containers or cloud solutions to handle larger volumes and ensure reliability

REFERENCES

[1] Rusydi umar, Imam Riadi, Ridho Surya Kusuma, “Analysis of Conti Ransomware attack on computer network with live forensic method,” Computers & security, 2021.102490.

[2] Giyon kim, Soram kim, Soojin Kang, Jongsung kim, “A method for decrypting data infected with Hive ransomware” China Telecommunications Trade, 2022, no. 04, pp. 62-63.

[3] R.A Shehan Sanjula, “Comprehensive survey on Petya Ransomware Attack” Communications Management and Technology, 2022, no. 03, pp. 53-55.

[4] Alexandre MundoAlguacil, John Fokker, Northeastern University "DITING" cybersecurity team, “Dynamic analysis on Crypto ransomware by using machine learning: GandCrab Ransomware 2022,” 2022.

[5] Or-Meir O., Nissim N., Elovici Y., Rokach L. Dynamic malware analysis in the modern era’a state of the art survey. ACM Comput. Surv. 2019;52(5) doi: 10.1145/3329786.

[6] Bajpai P., Enbody R. Dissecting.net ransomware: key generation, encryption and operation. Network Security. 2020;2020(2):8–14.

[7] Zimba A., Mulenga M. A dive into the deep: demystifying wannacry crypto ransomware network attacks via digital forensics. International Journal on Information Technologies and Security. 2018;10:57–68.

[8] A. M. Abiola and M. F. Marhusin, “Signature-based malware detection using sequences of N-grams,” Int. J. Eng. Technol., vol. 7, no. 4, pp. 120–125, 2018, doi: 10.14419/ijet.v7i4.15.21432.

[9] D. Nieuwenhuizen, “A behavioural-based approach to ransomware detection,” MWR Labs, 2017, [Online]. Available: https://labs.f-secure.com/assets/resourceFiles/mwri behavioural-ransomware-detection-2017-0 45.pdf.

[10] F. Noorbehbahani and M. Saberi, “Ransomware Detection with Semi-Supervised Learning,” 2020 10h Int. Conf. Comput. Knowl. Eng. ICCKE 2020, pp. 24–29, 2020, doi: 10.1109/ICCKE50421.2020.930368.

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