RESEARCH ARTICLE OPEN ACCESS

Ransomware Attack Detection and Classification Using Machine Learning

Dipak Shid*, Parikshit Patil**, Shrikrushna Shinde***, Himanshu Shinde****
Manisha Darak*****

*(Computer Engineering, RMDSCCOE, Pune, 411058, India
Email: dipakshid.rmdstic.comp@gmail.com)
**(Computer Engineering, RMDSCCOE, Pune, 411058, India
Email: parikshitpatil.rmdstic.comp@gmail.com)
***(Computer Engineering, RMDSCCOE, Pune, 411058, India
Email: shrikrushnashinde.rmdstic.comp@gmail.com)
****(Computer Engineering, RMDSCCOE, Pune, 411058, India
Email: himanshushinde.rmdstic.comp@gmail.com)
*****(Computer Engineering, RMDSCCOE, Pune, 411058, India
Email : manishadarak.rmdssoe@sinhgad.edu)

----------**********----------

Abstract:

Ransomware has become a serious cybersecurity risk, especially in industries like healthcare where patient data integrity and confidentiality are crucial. This study examines current approaches to machine learning-based ransomware detection and categorisation. For data integrity in encrypted contexts, we investigate techniques that integrate cryptographic techniques like MD5 and SHA-256 with algorithms like Support Vector Machines (SVM) and Random Forests. In hospital settings, where patient data is kept on encrypted local databases, the study focusses on real-time ransomware detection. We highlight potential research directions for improving ransomware defences while discussing issues including model accuracy, data availability, and encryption overheads.

Keywords **— Ransomware, Machine Learning, SVM, Random Forest, MD5, SHA-256, Real-Time Detection, Healthcare Security**

----------**********----------

I. INTRODUCTION

A rapidly expanding cybersecurity issue, ransomware encrypts files or locks computers and demands a fee to unlock them. It can affect both individuals and organisations. Ransomware has developed into a more complex and pervasive type of malware within the last ten years. Attacks used to be more random, but these days they frequently target particular industries like healthcare, government, and financial organisations. These assaults are particularly dangerous because they can disrupt essential operations, compromise sensitive data, and result in severe financial losses. Ransomware attacks can have serious repercussions in the healthcare industry, including disclosing private medical records, stopping emergency services, and interfering with patient care.

Traditional ransomware detection techniques, such signature-based detection, have not been able to keep up with the latest, constantly changing ransomware variants. Since signature-based techniques depend on spotting well-known malicious code patterns, they can't identify novel, undiscovered ransomware strains. Attackers regularly use ransomware as its complexity increases. By examining patterns and behaviours linked to harmful activity, machine learning provides the capability of real-time ransomware attack detection. By detecting departures from typical system behaviours, machine learning models, as opposed to signature-based techniques, are able to detect novel ransomware variants. Based on system activity data, algorithms like Random Forest and Support Vector Machines (SVM) have demonstrated potential in efficiently identifying and categorising ransomware.

By learning to distinguish between benign and malevolent activity, these models can detect ransomware before it locks down systems or encrypts data. In healthcare settings, where early ransomware detection is essential to preserving continuous access to patient data and medical services, machine learning is especially beneficial.

The project's ransomware detection method makes use of real-time patient data monitoring in local databases that are encrypted. Protecting sensitive data requires encryption, which makes sure that even in the event that ransomware infiltrates the system, the data is safe and unreadable without the right decryption keys. A dual-layered defence is created by combining encryption and machine learning, where anomalous activity instantly generates alerts. This strategy is particularly crucial in hospital settings where patient privacy and safety must be maintained and any ransomware-induced outage could have fatal repercussions.

II. MOTIVATION

Ransomware attacks pose a significant threat to the confidentiality and integrity of patient data, which can have severe consequences for both individuals and healthcare organizations. Developing effective ransomware detection solutions can contribute to improving the overall security posture of the healthcare industry. Ransomware attacks can disrupt critical healthcare operations, leading to delays in patient care, financial losses, and damage to reputation.

III. LITERATURE SURVEY

A. Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier

Ransomware attacks represent a significant danger to online resources because of their extensive impact. The Zero-day variants are particularly perilous, as they are less understood. In this context, traditional machine learning methods for detecting ransomware attacks can become reliant on specific data, indifferent to the costs of errors, and may therefore struggle to address zero-day ransomware incidents. Zero-day ransomware typically operates with previously unrecognized underlying data distributions.

B. Ransomware Classification and Detection with Machine Learning Algorithms

Malicious attacks, malware, and various ransomware groups present severe security challenges in cybersecurity, potentially leading to devastating consequences for computer systems, data centres, and both web and mobile applications in numerous sectors and enterprises. Conventional anti-ransomware solutions often find it difficult to combat the increasingly sophisticated attacks that continue to emerge. Consequently, advanced methods, such as traditional frameworks and neural network-based architectures, can be highly valuable in creating effective new ransomware solutions.

C. Ransomware detection based on machine learning using memory features

Ransomware incidents have surged in recent times, impacting critical infrastructure and businesses worldwide. Regrettably, ransomware employs advanced encryption methods to encode vital files on the affected system and then requests a ransom to unlock the data. Various artificial intelligence methods, particularly machine learning, have been progressively utilized in cybersecurity, significantly aiding in the identification and prevention of various attack types.

D. Ransomware Detection using Machine and Deep Learning Approaches

With the growth and wide availability of computer and internet technologies, network security has become increasingly susceptible to hacking threats. Ransomware is a commonly employed type of malware in cyber-attacks designed to deceive victims into revealing sensitive and private information to the attackers. As a result, victims may lose access to their data until they pay a ransom for the compromised

files or information. Various strategies have been developed to address these challenges.

E. Ransomware Detection and Classification Strategies

Ransomware employs encryption techniques to render data unreachable for authorized users. Numerous ransomware families have been created and used, resulting in significant harm to governmental entities, businesses, and individual users. As these cyber threats increase, scholars have suggested various methods for detecting and classifying ransomware.

F. Ransomware Detection Using Machine Learning: A Survey

Attacks using ransomware present serious security risks to both corporate and personal data. Successful ransomware attacks cause financial losses, reputational harm, and verification and privacy violations for the owners of computer-based resources. Therefore, it is essential to quickly and precisely detect ransomware. Many techniques have been put forth to detect ransomware, each with pros and cons of their own.

G. Ransomware detection using machine learning: A review, research limitations and future directions

The frequency and impact of ransomware attacks are increasing. Since more people are working remotely as a result of the COVID-19 pandemic, businesses have had to quickly adjust. Regretfully, the rise in online activity has given cybercriminals a lot of chances to launch destructive attacks. Malicious actors have recently used ransomware to infect corporate networks in an attempt to steal millions of dollars in profits.

H. Ransomware Detection using Random Forest Technique

In the current computing world, ransomware has emerged as a significant threat that needs to be taken seriously right away in order to prevent moral and financial blackmail. Therefore, a new technique that can identify and thwart this kind of attack is desperately needed. The majority of earlier detection techniques used a dynamic analysis approach, which is a laborious procedure. The current study suggests a brand-new static analysis-based technique for ransomware detection.

I. Ransomware Detection Model Based on Adaptive Graph Neural Network Learning

Ransomware is a type of malicious software that encrypts or locks user files while demanding a large ransom. Given how quickly it is being developed and updated, it has grown to be a serious threat to the security of cyberspace. Research on information security risk detection techniques has turned its attention to ransomware detection technology.

J. Ransomware Detection using Process Memory

Attacks using ransomware have become much more frequent in recent years, severely disrupting and damaging vital systems and corporate operations. The use of artificial intelligence has been boosted by attackers' constant innovation in evading detection systems. However, because ransomware is always changing its behavior to evade detection, the majority of research only summarizes the broad aspects of AI and produces a large number of false positives. The investigator can better understand the inner workings and primary function of ransomware by concentrating on its key indicating features.

K. Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors

Numerous organizational vulnerabilities to cyber threats have been brought to light by the COVID-19 pandemic, with ransomware emerging as the main issue. As businesses

moved toward remote connectivity to guarantee uninterrupted and secure business operations, these vulnerabilities were mostly caused by the increased accessibility of digital resources. The increasing need for IT support to maintain remote operations and the security measures required to guarantee secure and continuous services across multiple digital platforms diverged significantly between 2020 and 2022. Numerous studies show that during the pandemic, ransomware attacks increased by 150–200%, upending industries all over the world. This study provides a thorough examination of the most significant ransomware attacks that occurred during the pandemic (mainly between 2020 and 2022), emphasizing both well-known and recently discovered ransomware strains that have impacted companies.

L. Ranker: Early Ransomware Detection Through Kernel-Level Behavioral Analysis

A real-time method called Ranker uses kernel-level behavioral analysis to detect ransomware early. After examining a number of ransomware families, we found that half of them display covert actions before the actual attack. Identifying ransomware early on can be accomplished by drawing conclusions from the malicious activity that precedes the attack. Since the aim of ransomware families that directly encrypt files is to interact with user files, we concentrate on tracking file changes throughout the attack in the hopes of identifying ransomware when fewer files are lost. As a result, Ranker identifies common and crucial traits by methodically describing the kernel-level behavior of ransomware both before and during an attack. Additionally, Ranker presents a portable detector for real-time ransomware identification.

M. RThreatDroid: A Ransomware Detection Approach to Secure IoT Based Healthcare Systems

Due to their extensive use and simplicity of integration with Internet of Things (IoT)-based medical devices, smartphone devices have become increasingly prevalent in the healthcare industry. A new hybrid ransomware detection technique is presented in this work that extracts plain or encrypted threat text by analyzing text, application code, and image data. One useful tool that might be among the best for detecting ransomware is the use of threatening text. Our suggested hybrid approach makes use of multi-machine learning classifier models and both static and dynamic techniques. Additionally, a ransomware family classification is provided by the suggested method.

N. Ransomware detection based on machine learning using memory features

Studies using machine learning to identify ransomware are still scarce because of the obfuscation of malware, the accuracy of models, the high false-positive rate, and the failure to set up an appropriate analysis environment. Therefore, creating efficient machine learning-based ransomware detection methods is essential. In order to detect ransomware with high accuracy and few false positives, this study intends to develop a strong machine-learning model that can identify unknown samples using memory dumps. It also provides a thorough examination of how memory traces can aid in ransomware detection. In order to accomplish this, a new dataset comprising recent ransomware group attack samples such as Revil, Lockbit, and BlackCat was created. Following that, a comparative performance analysis was carried out on a collection of machine learning models.

IV. BLOCK DIAGRAM

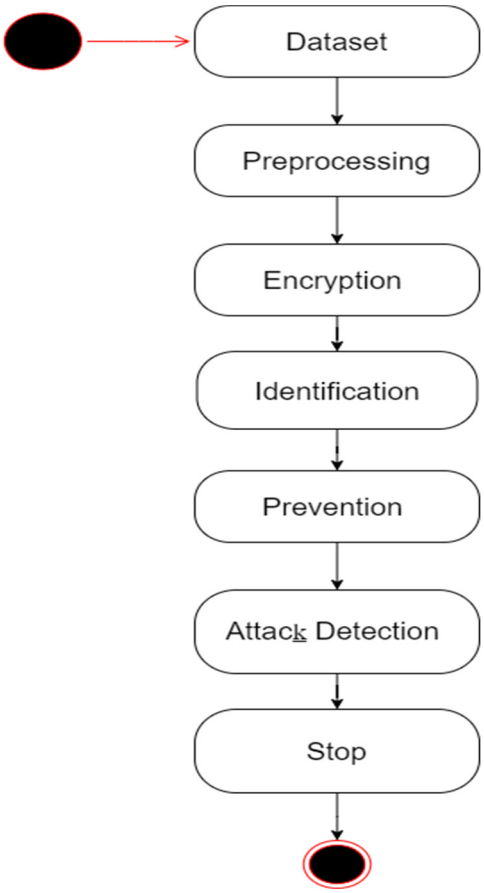

Fig 1. Block Diagram

V. METHODOLOGY

According to the study, machine learning models are very good at identifying ransomware attacks, particularly when paired with encryption techniques.

Detection Accuracy: Machine learning models, especially SVM and Random Forest, showed excellent accuracy in differentiating between benign and malevolent activity. In addition to known ransomware variations, these models were able to identify novel, unidentified strains that were overlooked by conventional signature-based techniques.

Difficulties with Real-time Detection: The significant computational overhead associated with encryption and real-time monitoring was one of the difficulties noted. For machine learning algorithms to continuously analyse system behavior, a large amount of processing power is needed. It is still difficult to strike a balance between detection accuracy and system performance in healthcare settings where real-time data access is essential.

False Positives: Despite the general accuracy of machine learning models, false positives are still a concern. A false positive happens when the system misidentifies harmless activity as ransomware, causing needless alerts or system shutdowns. Operations may be affected, particularly in vital industries like healthcare.

The function of encryption: Techniques like MD5 and SHA-256 were essential in protecting private information. The encrypted data was safe and unreachable by attackers without the necessary decryption keys, even if ransomware was able to get inside the system. This two-pronged strategy, which combined encryption and machine learning detection, worked incredibly well to lessen the effects of ransomware attacks.

Data Input and Encryption: The system receives patient data, such as personal details and medical history. Before being saved in the hospital's local database, this private information is instantly encrypted using robust cryptographic algorithms like SHA-256 to guarantee that it is shielded from unwanted access or manipulation.

Data Access by Physicians: Using decryption keys, authorized personnel, including physicians, can safely access encrypted patient data. Through this procedure, sensitive data can only be retrieved or updated by authorized users, and attempts by unauthorized users to gain access are reported to the system for additional review.

Machine Learning-Based Anomaly Detection: The algorithms used in machine learning continuously analyze behavioral patterns to identify anomalous activity, such as unauthorized encryption or unusual file access. These models can detect both well-known and novel ransomware attack variants

because they have been trained to recognize ransomware signatures.

Alert and Response System: The system instantly notifies the administrator by triggering an alert when it detects a possible ransomware threat. In order to reduce any possible harm, this alert prompts the administrator to take corrective action, such as separating compromised systems, stopping illegal access, or starting a data recovery procedure.

Encryption-Based Data Protection: Patient data is encrypted, making it unreadable and inaccessible without the right decryption keys, even in the event that ransomware manages to breach the system. This two-pronged strategy, which combines machine learning detection with encryption, guarantees data security and integrity across the healthcare setting.

VI. CONCLUSION

More sophisticated detection methods are required due to the growing complexity and frequency of ransomware attacks, which specifically target healthcare systems. Because ransomware variant are constantly changing, traditional signature-based methods are no longer adequate. Through real-time threat identification and system behavior analysis, machine learning models like Random Forest and Support Vector Machines (SVM) provide more intelligent and adaptable solutions. By categorizing ransomware activity before it has a chance to compromise vital healthcare data, these techniques offer a stronger defence.

The dual-layer protection offered for sensitive data is one of the biggest benefits of combining machine learning with cryptographic techniques like MD5 and SHA-256. This combination guarantees that the encrypted data is safe even in the event that ransomware infiltrates a system. While encryption protects data integrity, machine learning improves the early detection of suspicious activity. In healthcare settings, where protecting patient data's availability and confidentiality is crucial, this multi-layered defense is crucial.

In summary, a major advancement in cybersecurity for healthcare systems has been made with the incorporation of machine learning for ransomware detection and classification. More developments are required to improve these techniques and solve practical issues, guaranteeing improved defense against changing ransomware threats.

VII. REFERENCE

[1] J. Feng et al., "TapLab: A Fast Framework for Semantic Video Segmentation Tapping Into Compressed-Domain Knowledge," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 3, pp. 1591-1603, 1 March 2022

[2] M. Alassad, M. N. Hussain and N. Agarwal, "How to Control Coronavirus Conspiracy Theories in Twitter? A Systems Thinking and Social Networks Modeling Approach," *2020 IEEE International Conference on Big Data (Big Data)*, Atlanta, GA, USA, 2020.

[3] M. Aljabri et al., "Ransomware Detection Based on Machine Learning Using Memory Features," Journal of Information Security and Applications, vol. 55, p. 102615, 2020.

[4] R. A. M. Alsaidi et al., "Ransomware Detection Using Machine and Deep Learning Approaches," IEEE Access, vol. 8, pp. 213822–213834, 2020.

[5] Vehabovic, A., Ghani, N., Bou-Harb, E., Crichigno, J., & Yayimli, A. (2022). "Ransomware Detection and Classification Strategies." 2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom).

[6] A. Alraizza and A. Algarni, "Ransomware Detection Using Machine Learning: A Survey," IEEE Access, vol. 8, pp. 213819–213821, 2020.

[7] B. M. Khammas, "Ransomware Detection Using Random Forest Technique," International Journal of Advanced Computer Science and Applications, vol. 11, no. 11, pp. 1–7, 2020

[8] Li, J., Yang, G., & Shao, Y. (2024). "Ransomware Detection Model Based on Adaptive Graph Neural Network Learning." Applied Sciences, 14(11), 4579.

[9] A. Singh, R. A. Ikuesan, and H. Venter, "Ransomware Detection Using Process Memory," in Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICCWS), 2020.

[10] Z. Baig, S. H. Mekala, and S. Zeadally, "Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors," IT Professional, vol. 25, no. 5, pp. 37–45, 2023.

[11] M. J. Iqbal, S. Aurangzeb, M. Aleem, G. Srivastava, and J. C.-W. Lin, "RThreatDroid: A Ransomware Detection Approach to Secure IoT-Based Healthcare Systems," IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2574–2583, 2023

[12] M. Aljabri et al., "Ransomware Detection Based on Machine Learning Using Memory Features," Journal of Information Security and Applications, vol. 55, p. 102615, 2020.

[13] H. Zhang, L. Zhao, A. Yu, L. Cai, and D. Meng, "Ranker: Early Ransomware Detection Through Kernel-Level Behavioral Analysis," IEEE Access, vol. 8, pp. 213678–213690, 2020.

