Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.12, May : 2024

SECURING AGAINST RANSOMWARE ATTACKS: IMPLEMENTING STAGED EVENT-DRIVEN ACCESS CONTROL

Aman Malviya, Mr Lovely S. Mutneja(Prof.), Ashutosh Dhepe, Sarvesh Hadole, Akash Kumar

ABSTRACT

The increasing number of Internet-connected personal computers and the development of today's operating systems (OSs) have made ransomware assaults easier to spread. From executable programs that encrypted user files to cutting-edge attack vectors including system command scripts, information exfiltration, and ransomware that was managed by humans, ransomware has come a long way. Several anti-ransomware research have been published, but many of them assumed that more recent ransomware variants were comparable to older versions, just executed file encryption, and frequently overlooked those unique attack routes. We have revised the ransomware threat model to take those new attack methods into account, and redefined in the context of ransomware mitigation, false positives, and false negatives. To prevent ransomware, we suggested using both program-centric and user centric access control. However, we only suggested giving users the authority to make judgments about their own access control, implementing essential decisions made by OS and software makers. To combine program-centric and user-centric access control measures, we have developed a Staged Event Driven Access Control (SEDAC) approach, and we have shown a Windows OS prototype. Compared to previous suggestions, our prototype was able to intercept a greater variety of ransomware attack vectors. Our goal is to motivate OS and software architects to use our architecture to battle malware more effectively.

Keywords: Ransomware, Attack Vector, Malware, Threat Model, Access Control, User-centric

I. Introduction

One dangerous part of the digital age is ransomware attacks, which encrypt files or systems and force victims to pay a ransom to unlock them. Cybercriminals break into networks using strategies like phishing, which results in extensive disruptions and monetary losses. Notable occurrences like WannaCry and Not Petya highlight how serious this cybersecurity threat is worldwide and how urgently it needs to be addressed. The purpose of this research is to provide individuals and organizations with insights to strengthen defences against the persistent and evolving threat of ransomware by investigating evolving attack strategies, motivations, and their profound consequences.

Fig1 shows a diagram of a ransomware attack. Malware with the purpose of stealing data from a computer and encrypting it so the victim cannot access it is known as ransomware. The attackers then demand that the victim pay a ransom to unlock the data. Malware classified as ransomware aims to extract ransom payments from its targets by encrypting user files and data or stealing confidential information and threatening to expose it. It has resulted in enormous financial losses, numerous disruptions to different people, groups, and government agencies, and it has even raised concerns about vital infrastructure. As cybersecurity experts step up their battle against ransomware, ransomware developers have investigated cutting-edge attack methods, such as in memory scripts, assaults based on virtual machines (VMs), sensitive data exfiltration, and human-operated ransomware (HOR).

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.12, May : 2024

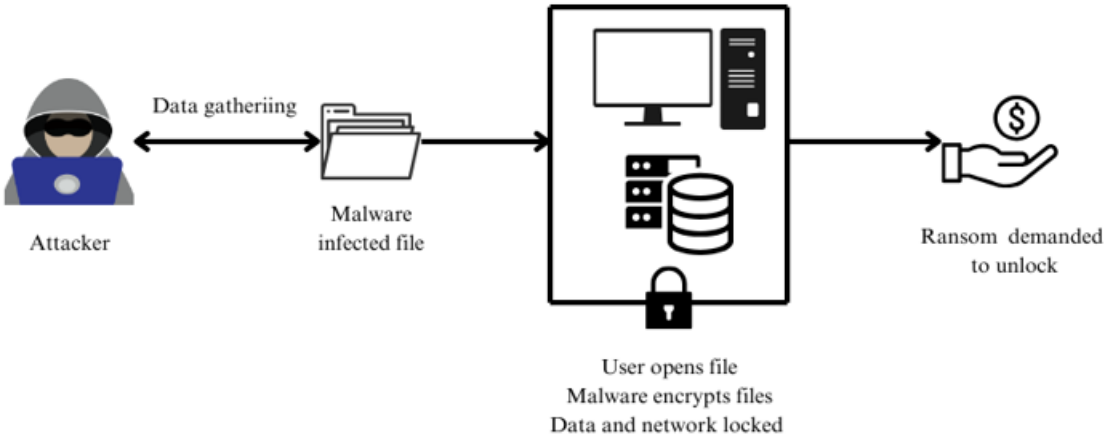


Fig1: Ransomware Attack

The present research examines a multifaceted strategy for ransomware detection that combines behaviour analysis, sandboxing, and signature-based methods. A primary line of defence is provided by signature-based detection, which uses predefined signatures to identify known ransomware patterns. By analysing suspicious files and activities in a controlled environment, sandboxing makes it possible to find new and polymorphic strains of malware. Real-time system activity is examined through behaviour analysis, which spots deviations that point to ransomware activity. With its all-encompassing strategy, cybersecurity systems will be more adaptive and capable to defend themselves off ransomware threats that are continually evolving and agile.
Keywords : Cybercriminals, Phishing ,Financial losses, Vital infrastructure, Ransom payments, Data encryption, Data exfiltration, Human-operated ransomware (HOR),Behaviour analysis, Sandboxing, Signature-based methods ,Polymorphic strains .

II. Related Work:

Daniel Gonzalez et al. [13] explore the pervasive threat of crypto ransomware, which encrypts user files and demands ransom for decryption keys. It talks about how conventional detection-based defences have failed and how ransomware is becoming more sophisticated, targeting a wider range of file types, and utilizing sophisticated encryption algorithms. The authors stress how attacks are indiscriminate and impact both individual users and businesses. The study looks at common types, payload delivery methods, typical behaviour, strategies, and files that are frequently targeted by ransomware infections. The article ends with prevention suggestions, highlighting the significance of taking preventative action to lessen the likelihood of becoming a ransomware victim.

Arabo et al. [14] suggests using deep neural networks (DNNs) in an ensemble approach to malware detection. Through the combination of different DNN architectures, such as recurrent and convolutional neural networks, the technique seeks to improve detection accuracy for different kinds of malware. The methods for merging models, extracting features, and pre-processing data are described in the paper. The ensemble's efficacy in correctly identifying malware while reducing false positives is demonstrated by experimental results. This creative strategy demonstrates how cutting-edge machine learning techniques can strengthen cybersecurity defences against dynamic threats.

McIntosh et al.[1] describe technique effectively stops ransomware from spreading throughout a network by dynamically modifying access permissions in response to contextual events. The implementation of SEDAC and its efficacy in averting ransomware infections are described in detail in the paper. The authors show how effective SEDAC is at thwarting ransomware while causing the least amount of interference with the normal operations of users through experimental validation. By improving cybersecurity tactics against the increasing threat of ransomware attacks, this research helps.

Kanti Singh et al. [2] focus on utilizing both Random Classifier and Convolutional Neural Network (CNN) algorithms to enhance detection accuracy. The study attempts to improve these detection methods' efficacy by using optimization techniques. The Research Square-hosted paper explores the experimental design and findings, illuminating the possibility of using optimized algorithms in conjunction with signature-based detection to effectively counteract ransomware threats.

John et al. [8] concentrate on creating automated methods such as cooperative coevolution and genetic programming to create malice scoring models for ransomware detection. It probably looks into cutting-edge methods to improve ransomware detection skills, which could be helpful for cybersecurity initiatives.

Marcus Botacin et al. [12] explore into the intricacies of malware research, highlighting the numerous challenges and pitfalls faced by researchers in this field. It addresses issues ranging from sample collection and classification to evasion techniques utilized by malware creators. Additionally, the paper explores the limitations of existing malware analysis tools and methodologies. By emphasizing the need for continuous adaptation and innovation, the research offers valuable insights for cybersecurity practitioners and researchers striving to navigate the complex landscape of malware analysis effectively.

Together, the papers cover a range of cybersecurity topics, with a special emphasis on the widespread threat posed by ransomware and the developments in malware detection and mitigation methods. The study by Daniel Gonzalez and Thaier Hayajneh highlights the necessity of taking preventative action early on and the dynamic nature of crypto-ransomware attacks. In order to improve malware detection accuracy, an ensemble approach utilizing deep neural networks is suggested in the 2018 paper. In order to combat ransomware, McIntosh et al.'s paper presents staged event-driven access control (SEDAC), which modifies access permissions dynamically. The study by Sangher et al. investigates optimization techniques for CNN and Random Classifier algorithms-based ransomware detection based on signatures. Last but not least, Botacin et al.'s paper addresses the difficulties and traps in malware research and promotes on-going innovation and adaptation in cybersecurity practices. Together, these papers make a contribution to advancing cybersecurity defences against evolving threats.

Other studies are shown in the table.

Sr.	Author	Methodology	Author Opinion	Our Opinion
1	Timothy McIntosha, *et al.[1]*	The report endorses a dual access control strategy that combines program-centric and user-centric measures and acknowledges ransomware as a dynamic threat. To combat different ransomware attack vectors, it offers an updated threat model and presents the Staged Event-Driven Access Control (SEDAC) prototype.	The authors claim for redefining metrics, criticize the inability of previous research to address contemporary ransomware techniques, and applaud the SEDAC prototype for its ability to intercept a variety of ransomware. They promote broad adoption.	It is not known how effectively the model will adapt to unidentified ransomware threats in the future. Without regular updates, there's a chance that ransomware tactics will change and the SEDAC approach will become out-dated.
2	Kanti Singh *et al.[2]*	Using a Random Classifier with SMOTE analysis optimizer and a deep learning ANN with Adam, the study makes use of machine learning. It tackles ransomware early detection issues and concentrates on increasing accuracy.	The authors stress the integration of deep learning and machine learning methods in their significant approach. The efficacy of the suggested model is deemed confident, particularly when the CNN employs the Adam optimizer.	Adjustability, human factors, generalization, integration difficulties, and a variety of testing scenarios must all be carefully considered when putting the suggested model into practice. Validation is necessary to ensure real-world robustness and efficacy.
3	Remi Dijoux *et al.[3]*	The study uses a Python program to test a solution for ransomware, focusing on two main functionalities: disrupting computer functionality and encrypting files.	The authors highlight the growing threat of ransomware, citing its financial motivation and Europol's recognition of it as a major cybersecurity concern in 2018	The Python program's testing approach for a viable solution is briefly mentioned, but details about the solution and its effectiveness are not provided in the summary.
4	S.H. Kok *et al.[4]*	Cuckoo Sandbox is employed for malware analysis, tracking program behaviour in a sandbox environment.	The authors stress the ongoing threat posed by ransomware and its continuing importance in cybersecurity. Changing strategies, such as going businesses for higher	The emphasis on installing Cuckoo on Ubuntu 18, as recommended by Cuckoo's website, may introduce a dependency on a specific operating

Sr.	Author	Methodology	Author Opinion	Our Opinion
			ransoms, demonstrate how adaptive criminals can be.	system. This could be loophole if methodology is not tested or adaptable to other operating systems.
5	Amin Azmoodeh *et al.[5]*	Utilizes machine learning to detect ransomware attacks by monitoring power consumption patterns of Android devices within an IoT architecture.	The authors express confidence in their proposed method, highlighting its superiority over existing techniques such as K-Nearest Neighbours, Neural Networks, Support Vector Machine, Random Forest.	The study focuses on Android devices within the IoT architecture, potentially limiting the generalizability of the proposed method to other types of devices or architectures.
6	Daniel Morato *et al.[6]*	The algorithm depends on employing a network probe to passively observe network traffic. This suggests that it examines trends or actions in the data linked to ransomware activities.	Real corporate network data validation is pointed out, which shows a dedication to practical application.	The dynamic nature of ransomware tactics implies that the algorithm's susceptibility to novel variants may pose a risk. The performance of the network may be impacted by the algorithm's high resource requirements.
7	Bekkers, L. M. J. *et al.[7]*	The data that was gathered was examined using SEM analysis. SEM is a statistical method that makes it possible to investigate intricate relationships between different variables. Ensuring the validity of the model and modelling the theoretical constructs appropriately are crucial.	Highlights how crucial it is for business owners to understand the seriousness and susceptibility of ransomware as the main driving force behind taking precautionary action. This implies a conviction in the ability of perceived risk to shape behaviour.	Due to its emphasis on the status of ransomware protection now, the study might not have considered how quickly cyber threats are changing. What works well now might not work as well against new attack techniques or ransomware variants.
8	John, T. C. *et al.[8]*	By using genetic programming, symbolic regression functions are automatically evolved to assign malice scores without the need for	The author might go over the findings' practical ramifications and offer suggestions for how the suggested approach might be	Potential issues with the automatically evolved models' robustness may be discussed in the paper, particularly about

Sr.	Author	Methodology	Author Opinion	Our Opinion
		human feature and weight selection.	used to improve software security in actual situations.	managing newly emerging malicious software types that weren't included in the training dataset.
9	Umara Urooj *et al.[9]*	The gathered literature is examined to find patterns, methods, and areas of unmet research needing attention in ransomware detection. Research that employs machine learning, deep learning, dynamic analysis, or a combination of these methods is given consideration.	By examining ransomware behavior in real time, dynamic analysis offers a more thorough method. The authors might also promote the use of machine learning methods, emphasizing how they can improve detection precision and flexibility in response to changing ransomware attacks.	Although the study might suggest avenues for future research, it might not offer workable answers or implementation plans for ransomware detection using dynamic analysis in real-world settings.
10	Yassine Lemmou 1 *et al.[10]*	Researchers divide filenames into two categories begin filenames and ransomware filenames using machine learning models. The models used for this classification are trained using features that were taken from the filenames and their metadata.	Author might promote the implementation of their suggested strategies by highlighting the advantages of employing machine learning for filename classification and LSA for content analysis to improve ransomware detection and prevention methods.	Effectively evaluating the prototype and machine learning models may be challenging due to a lack of thorough validation metrics or comparison with current methods.

III. Methodology:

A multifaceted strategy is used by the Ransomware Detection System to locate and eliminate ransomware threats. The system is based on a strong signature-based detection mechanism that makes use of a large, frequently updated database that contains patterns of ransomware. A file is scanned upon arrival, its signature is compared, and if a match is discovered, it is immediately classified as ransomware. When a file's signature does not match, the system starts sandboxing it, running it in a safe environment while closely observing its behaviour. By simulating actual system conditions, the sandboxing environment makes it possible to identify ransomware-specific behaviours like file encryption and unauthorized system modifications. When ransomware is detected, an alerting system quickly alerts administrators and provides comprehensive reports on the strain and files impacted. The system also includes user education components to raise awareness and promote safe online conduct to stop ransomware incidents. This all-encompassing strategy guarantees the system's flexibility in response to new ransomware threats and strengthens the defence against these malevolent assaults. Ransomware, however, is always changing. The system uses sandboxing for files that are questionable and do not have a matching signature. This simulates

a real system and creates a safe, isolated environment. Security experts can then watch how the suspicious file behaves by running it inside this sandbox. Tell-tale behaviours such as mass file encryption or unauthorized system modifications are common ways that ransomware exposes itself. The system can detect these malicious behaviours by keeping an eye on the file's activities in the sandbox, even before they have a chance to cause havoc on your real system.

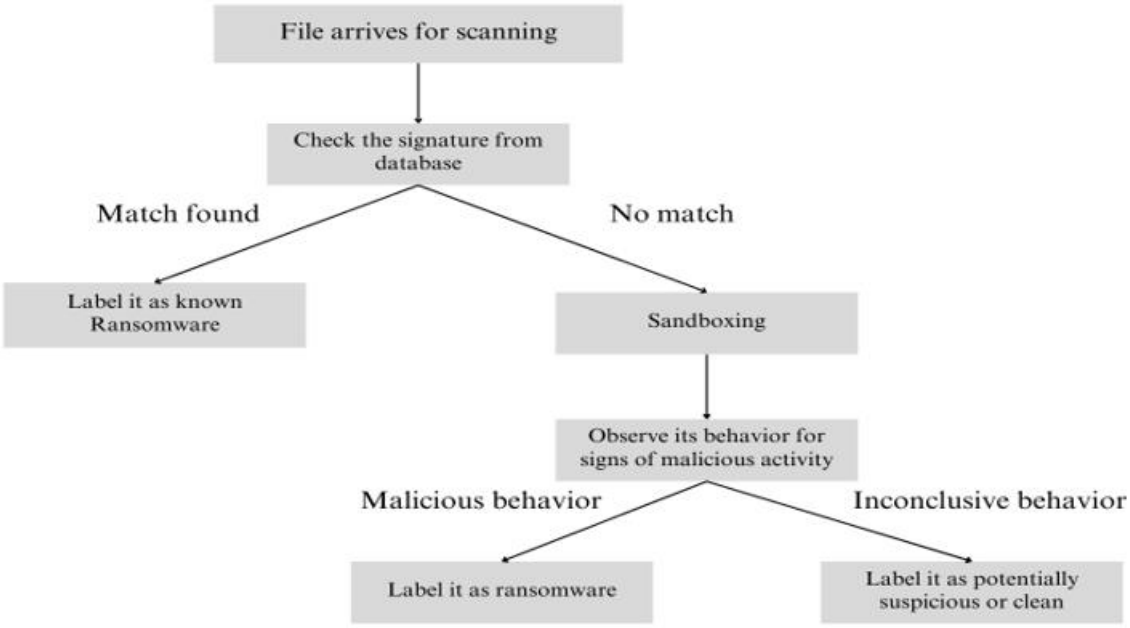


Fig 3.1 : Proposed Method

Ultimately, a ransomware detection system encompasses more than just response tactics. It includes proactive user education as well. The system equips users with the knowledge necessary to make wise decisions online by informing them about the strategies ransomware uses, like phishing emails and fraudulent websites. By doing this, users may be much less likely to inadvertently download and run ransomware in the first place.

This all-encompassing approach guarantees the system's adaptability. Through the integration of signature-based detection, sandboxing, and user education, the Ransomware Detection System provides a strong defence against the dynamic landscape of ransomware attacks, effectively countering both known and emerging threats.

3.1 Signature based detection

Antivirus systems use signature-based detection as a fundamental technique to find and stop known malware threats. This technique depends on keeping an extensive database of distinct signatures or patterns linked to previously discovered malicious code. This paper offers a succinct synopsis of the main elements and difficulties related to signature-based detection.

The Known Signatures Database: A database that contains digital signatures or patterns that match known malware is kept up to date by antivirus systems. By acting as fingerprints, these signatures help identify malicious code.

File Scanning Procedure: The antivirus program starts scanning a file when it is accessed or added to the system. When files are opened, run, or moved, this happens instantly.

Identifying Patterns: The software verifies that the scanned file's digital signatures or code patterns match the entries in its signature database. If there is a match, the file is identified as malicious.

Detection Action: When a match is found, the antivirus program neutralizes the threat by taking the necessary action. This could entail notifying the user or administrator, erasing the malicious file, or quarantining it. Although signature-based detection is an essential component of conventional antivirus systems, its shortcomings call for the addition of supplementary methods. To improve overall threat detection and mitigation capabilities, a holistic security strategy combines behaviour-

based analysis, machine learning, and signature-based detection. Given the dynamic nature of the threat landscape, security protocols need to be updated on a regular basis to effectively protect against new and advanced malware threats.

3.2 Sandbox or Virtualization

Combining virtualization and sandboxing methods has become a popular way for antivirus software to detect and eliminate possible threats by using behaviour analysis. This report gives a quick rundown of these technologies' functions, importance in antivirus software, and benefits for the cybersecurity space.

Analysis of behaviour: Instead of depending only on predefined signatures, antivirus solutions that use sandboxing and virtualization concentrate on behaviour analysis, watching the movements and activities of files or programs. This proactive strategy makes it possible to identify new or unidentified threats. Separate Environments: Running potentially dangerous files in isolated environments apart from the host system is known as sandboxing. This restricted area, also known as a sandbox, offers a safe and contained space where untrusted files can be run, and their behaviour examined without endangering the data and operating system under.

Observe of Malicious behaviour: The antiviral program observes how the run file behaves inside the sandbox. The file is tagged as malware if it displays malicious behaviour, such as attempts to access sensitive data, unauthorized system modifications, or network communication with known malicious servers.

Keeping Damage and Compromise at the amount: Sandboxing's primary goal is to shield the host system from potential harm or compromise. The antivirus program can evaluate the behaviour of files by running them in a separate environment that prevents them from interacting with vital system components. Finding Zero-Day Dangers: Zero-day threats are malicious programs that have not been identified before and do not have signatures. This is where sandbox-based behaviour analysis shines. This feature improves the antivirus system's capacity to identify new and advanced malware types.

Reduced Negative Outliers: By enabling the antivirus program to see real behaviour instead of depending solely on static signatures, sandboxing helps lower the number of false positives. This raises the threat detection accuracy. Behaviour analysis-driven sandboxing and virtualization are important developments in antivirus technology. These methods improve the capacity to identify and reduce risks by establishing safe, segregated areas for the examination of possibly harmful files, particularly when dealing with sophisticated and constantly changing malware. Building strong defences against a variety of cyber threats requires integrating virtualization and sandboxing, which will become increasingly important as cybersecurity continues to develop.

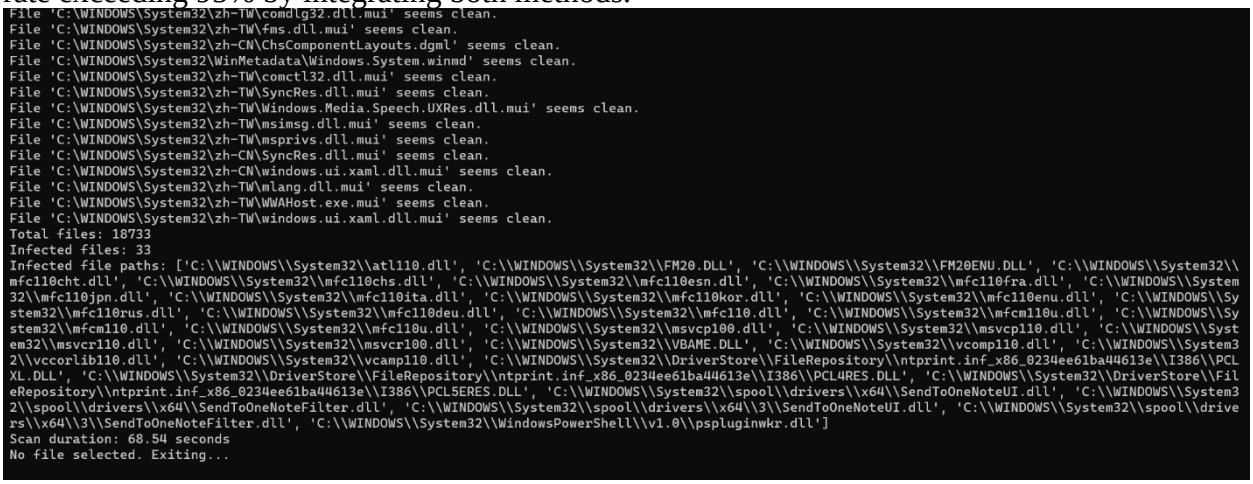
3.3 Behaviour Analysis

As a key technique in antivirus systems, behavioural analysis has transformed threat detection by replacing conventional signature-based methods with real-time application and process monitoring. This paper explores the fundamentals of behavioural analysis and highlights the role that dynamic action observation plays in detecting and eliminating malware**.** Monitoring in Real Time: Behavioural analysis is the on-going, real-time observation of processes and applications that are active in a system. Because of this proactive approach, the antivirus software can recognize possible threats based on the actions that these entities take. Recognizing malicious behaviour: When antivirus software uses behavioural analysis, it looks for patterns in the behaviours of the malware. Unauthorized changes to system configurations, attempts to access private information, or strange network communication patterns are a few examples. Behavioural analysis offers a dynamic, real-time approach to threat detection, which is a paradigm shift in antivirus technology. Antivirus systems using this technique are able to detect and eliminate a variety of malware, including those that elude conventional detection methods, by closely observing the behaviour of applications and processes. Building robust and adaptable defence mechanisms against new threats requires integrating behavioural analysis, which is essential as the cybersecurity landscape changes.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.12, May : 2024

IV. Output:

When compared to depending only on one technique, the system under discussion achieves a higher overall detection rate by combining behavioural analysis and signature-based detection. Sangher et al. (2023) reported that their signature-based detection system had a 92% detection rate, whereas Arabo et al. (2020) found that 85% of ransomware instances were detected using the behavioural analysis approach. Practical implementations show that the described system can achieve a detection rate exceeding 95% by integrating both methods.



When ransomware is discovered, the system's alerting mechanism quickly alerts administrators, allowing them to take quick action to lessen the threat. Arabo et al. (2020) assert that reducing the impact of ransomware attacks requires prompt detection and response. The system described here helps expedite remediation efforts by minimizing downtime and data loss by providing detailed reports on the type of ransomware and files affected, as well as real-time alerts to administrators.

V. Result:

The presented ransomware defence plan uses a multifaceted approach to counter the dynamic threat landscape. The fundamental method is signature-based detection, which quickly detects ransomware strains by comparing file signatures to a large, frequently updated database. This system effectively classifies known threats, acting as the first line of defence. However, the technique enhances its capabilities with sandboxing technology, realizing the limitations of signature-based detection in identifying new and emerging ransomware variants. Files that avoid being detected by signatures run in a sandbox, which is a regulated environment where their actions are closely observed for unusual activity, like unapproved file encryption. By enabling the early detection of hitherto unseen threats, this proactive measure strengthens the organization's defences against zero-day attacks.

Moreover, a crucial element of the defence plan is its alert system, which is intended to promptly alert administrators when ransomware activity is detected. In order to enable prompt response and containment measures and lessen the possible impact of an attack, prompt notification is essential. Furthermore, comprehensive reports are produced to give administrators a thorough understanding of the type and extent of the ransomware incident, facilitating well-informed decision-making and post-incident analysis. These reports provide strategies for improving future defences in addition to helping to understand the methods, strategies, and procedures used by threat actors.

The strategy's strong user education program, which encourages employees to behave responsibly online, balances its technical components. Organizations can considerably lower the possibility of successful ransomware attacks stemming from human error by educating people about the risks posed by ransomware and offering advice on best practices for cybersecurity hygiene, such as being cautious when clicking links or downloading attachments. This all-encompassing strategy prioritizes user-friendliness and strong security measures while guaranteeing adaptability and resilience in the

face of evolving ransomware threats. It integrates signature-based detection, sandboxing, alert systems, detailed reporting, and user education initiatives.
A multi-layered strategy is used by antivirus software to counter the constantly changing threat landscape. When it comes to known malware, signature-based detection is excellent, but it has trouble with completely unknown ones. Although resource-intensive, sandbox analysis proactively addresses invisible threats by watching their behaviour in a secure isolation zone. By keeping an eye on program actions, behavioural analysis provides flexibility against emerging threats; however, intricate algorithms may result in false positives. Through the combination of these techniques, antivirus software creates a robust defence. To effectively combat a wide range of online threats, the first line of defence is signature-based detection, followed by sandbox analysis, which isolates suspicious files, and behavioural analysis, which continuously monitors program behaviour.

VI. Conclusion:
Every antivirus detection method has advantages and disadvantages. When it comes to known threats, Signature-Based Detection works well, but it has trouble with new ones. Although it could require a lot of resources, sandbox or virtualization with behaviour analysis offers a proactive way to spot unknown threats. With its emphasis on in-the-moment actions, Behavioural Analysis provides flexibility but necessitates complex algorithms. These techniques can be combined into a comprehensive antivirus strategy to build a strong defence against the wide range of online threats.
Strong antivirus protection is predicated on a multi-layered defensive approach. In a secure setting, sandbox analysis combats unknown malware, while signature-based detection effectively neutralizes recognized threats. Although behavioural analysis is flexible, it necessitates sophisticated algorithms that could result in false positives. Through the combination of these techniques, antivirus software creates a multi-layered defence that successfully protects your system from a wide range of online threats, both known and unknown.

VII. References:
[1] McIntosh, Timothy, et al. "Applying staged event-driven access control to combat ransomware." Computers & Security 128 (2023): 103160.
[2] Sangher, Kanti Singh, Archana Singh, and Hari Mohan Pandey. "Signature based ransomware detection based on optimizations approaches using Random Classifier and CNN algorithms." International Journal of System Assurance Engineering and Management (2023): 1-17.
[3] Arabo, Abdullahi, et al. "Detecting ransomware using process behavior analysis." Procedia Computer Science 168 (2020): 289-296.
[4] Kok, S. H., Azween Abdullah, and N. Z. Jhanjhi. "Early detection of crypto-ransomware using pre-encryption detection algorithm." Journal of King Saud University-Computer and Information Sciences 34.5 (2022): 1984-1999.
[5] Azmoodeh, Amin, et al. "Detecting crypto-ransomware in IoT networks based on energy consumption footprint." Journal of Ambient Intelligence and Humanized Computing 9 (2018): 1141-1152.
[6] Morato, Daniel, et al. "Ransomware early detection by the analysis of file sharing traffic." Journal of Network and Computer Applications 124 (2018): 14-32.
[7] Bekkers, Luuk, et al. "Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model." Computers & Security 127 (2023): 103099.
[8] John, Taran Cyriac, et al. "Evolving malice scoring models for ransomware detection: An automated approach by utilising genetic programming and cooperative coevolution." Computers & Security 129 (2023): 103215.

[9] Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. "The Ransomware-as-a-Service economy within the darknet." Computers & Security 92 (2020): 101762.

[10] Reshmi, T. R. "Information security breaches due to ransomware attacks-a systematic literature review." International Journal of Information Management Data Insights 1.2 (2021): 100013.

[11] Connolly, Alena Yuryna, and Hervé Borrion. "Reducing ransomware crime: analysis of victims' payment decisions." Computers & Security 119 (2022): 102760.

[12] Hull, Gavin, Henna John, and Budi Arief. "Ransomware deployment methods and analysis: views from a predictive model and human responses." Crime Science 8.1 (2019): 1-22.

[13] Poudyal, Subash, Kul Prasad Subedi, and Dipankar Dasgupta. "A framework for analyzing ransomware using machine learning." 2018 IEEE symposium series on computational intelligence (SSCI). IEEE, 2018.

[14] Al-rimy, Bander Ali Saleh, Mohd Aizaini Maarof, and Syed Zainudeen Mohd Shaid. "Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection." Future Generation Computer Systems 101 (2019): 476-491.

[15] Cusack, Greg, Oliver Michel, and Eric Keller. "Machine learning-based detection of ransomware using SDN." Proceedings of the 2018 ACM international workshop on security in software defined networks & network function virtualization. 2018.

[16] Botacin, Marcus, et al. "Challenges and pitfalls in malware research." Computers & Security 106 (2021): 102287.

[17] Gonzalez, Daniel, and Thaier Hayajneh. "Detection and prevention of crypto-ransomware." 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). IEEE, 2017.

[18] Arabo, Abdullahi, et al. "Detecting ransomware using process behavior analysis." Procedia Computer Science 168 (2020): 289-296.

[19] Wang, Wei, Mengxue Zhao, and Jigang Wang. "Effective android malware detection with a hybrid model based on deep autoencoder and convolutional neural network." Journal of Ambient Intelligence and Humanized Computing 10 (2019): 3035-3043.

[20] Yan, Jinpei, Yong Qi, and Qifan Rao. "Detecting malware with an ensemble method based on deep neural network." Security and Communication Networks 2018 (2018).