RESEARCH ARTICLE OPEN ACCESS

Proactive Defensive Strategy Against Ransomware threats Using Rangan and Hash Conceal

Krishnakaarthik.T*, Prabhadevi.A**

*([1]AssistantProfessor, Department of Information Technology,Nandha College of Technology,Erode-638052
Email:krishnakaarthik.t@nandhatech.org)

** (UG-Finalyear,Department of InformationTechnology,Nandha College of Technology,Erode-638052
Email: prabhaanbu.0211@gmail.com)

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

Abstract:

Ransomware is a malware in which attacker then demands a ransom payment, usually in cryptocurrency, in exchange for providing the decryption key to unlock the files. The current approaches to detect such ransomware include monitoring processes, system calls, and file activities on the target system and analysing the data collected. Monitoring multiple processes has a very high overhead; newer ransomware may interfere with the monitoring and corrupt the collected data. To address this concern,this project adopted an open design approach to enhance the robustness of the proposed method. The proposed method detect ransomware and protects critical files from existing ransomware by applying a hiding strategy that poses a challenge to attackers in finding the target files. This project developed a proactive defence strategy against ransomware threats, leveraging "RanGAN" for early detection and "Hash Conceal" for data protection. Together, these technologies form a robust defence, ensuring rapid threat identification and minimizing data loss. This strategy aims to fortify cybersecurity against the evolvingransomwarelandscape,providingaresilientshieldforcriticalassets.Thisproactiveapproachnotonlybolstersanorganization'sresiliencetoransomwarebutalsoreducesthepotentialimpactoncritical data and operations. By leveraging RanGAN for early threat detection and Hash Conceal for data protection, organizations can enhance their cybersecurity posture and safeguard against the evolving ransomware threat landscape.

Keywords ***—Ransomware, RanGAN,Hash Conceal, Proactive Defense , Behaviour Pattern, Machine Learning.***

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

I. INTRODUCTION

Introducing a proactive defensivestrategy against ransomware threats through the Rangan and Hash Conceal project involves leveraging advanced techniques to protect against ransomware attacks. The project aims to enhance security measures by utilizing Rangan, a cutting- edge intrusion detection system, and HashConceal, a tool for obfuscating file hashes to prevent attackers from identifying and encrypting valuable data.By combining these technologies, organizations can detect and mitigate ransomware attacks more effectively. Rangan provides real- time monitoring and analysis of network trafficand system behaviorto identify suspicious activities indicative of ransomwareactivity. Meanwhile, Hash Conceal obscures file hashes, making it more challenging for attackers to target specificfilesforencryption.This proactiveto approach empowers organization fortility their defense.Today, [5] The primary goal is to create a robust and innovative approach to prevent, detect and mitigate ransomware attacks effectively, including unknown and evolving variants, while also enhancing data protection and privacy.The authors have proposed a defense mechanism aimed at protecting files from attacksbyconcealingthem.

Objectives:

1) To develop a robust and proactive defense mechanism against ransomware threats, safeguarding critical data, systems, and operations from potential attacks.
2) TodevelopRanGANtechnologyforearly ransomware detection.
3) To integrateHash Concealfor data protection.
4)Toachieveearlythreatdetection.
5)Toensuredataprotectionandconcealment.

RansomwareAttacks:

Figure 1.1 illustrates the ransomware attacks work, they typically involve malicious software that encrypts files on a victim's computer or network, rendering them inaccessible[6]. The attacker then demands a ransom payment, usually in cryptocurrency, in exchange for providing the decryptionkeyto unlock the files.These attacks can beinitiated through various means, such as phishing emails, malicious attachments, or exploiting vulnerabilities in software or networks.

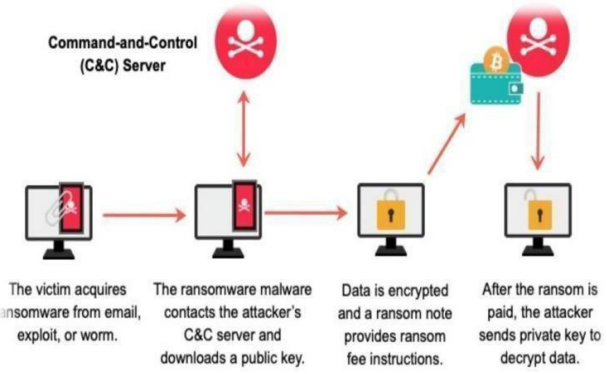


fig1.1Ransomware Attacks

II. RELATEDWORKS:

RanGAN(Rangefinder): Rangefinder is a technique that monitors file access patterns to detect ransomware activity. By analyzing the frequency and types of file modifications, Rangefinder can identify suspicious behavior indicative of ransomware encryption. Relatedwork in this area includes research papers and implementations that focus on refining and optimizing Rangefinder algorithms for better accuracy and efficiency.

HashConcealment: Hashconcealmentinvolveshiding cryptographic hash functions or keys from ransomware attackers to prevent them from encrypting files. This technique aims to disrupt the ransomware's ability to perform encryption by concealingthenecessaryinformation.Relatedwork may include studies on different methods of hash concealment, such as obfuscation techniques or dynamic key generation.

Behavioural Analysis: Another related approach involves analyzing the behavior of ransomware samples to develop signatures or behavioural patterns for detection[3]. This includes studying ransomware families, their propagation methods, and encryption techniques to crebust backup solutions, including versioning, offline backups, and secure storage,to facilitate rapid recoveryin the event of a ransomware attack.

Machine Learning and AI: Some researchate effective detection and mitigation strategies.
Backup and Recovery: Additionally, backup and recovery strategies play a crucial role in ransomware defense. Related work in this area focuses on developing roexplores the use of machine learning and artificial intelligence to detect ransomware activity based on patterns and anomalies in system behaviour [11]. This includes training models on large datasets ofransomware samples and benign software to improve detection accuracy.

MachineLearningAlgorithmsandFrameworks in Ransomware Detection:

Objective:
Evaluate machine learning efficiency in ransomware detection[9].
Methodology:
Collectdiversedata,employ variousalgorithms (e.g., decision trees, neural networks),and assess results with metrics.
AlgorithmsUsed:
Decision Trees, Neural Networks, SVMs,Random Forests, etc.
Results:
Comparealgorithmperformance,assess Framework suitability, and provide insights.
Limitations:
Ransomware threats evolve rapidly, and machine learning models may struggle to adapt to new attack techniques and tactics.

Dual Generative Adversarial Networks Based Unknown Encryption Ransomware Attack Detection

Objective:
Develop a method for detecting unknown encryption ransomware attacks using Dual Generative Adversarial Networks (GANs)[17].
Methodology:
Collect ransomware and benign data.Train.Dual GANs to distinguish between encrypted and non- encrypted files.
AlgorithmUsed:
DualGenerativeAdversarialNetworks(GANs).
Results:
High accuracy in detecting ransomware attacks. Robust performance against new and unknown ransomware variants
Limitations:
1.Data availability limitations.
2.Computational resource requirement.
3.Potentialfalsepositives/negatives inrarecases.

AnalysisofCrypto-RansomwareUsingML- Based Multi-Level Profiling:

Objective:
To leverage machine learning-based multi-level profilingforthe comprehensive analysis of crypto-ransomware attacks[12].
Methodology:
Collectdiversedata,applymulti-levelprofiling with ML, and assess results
AlgorithmsUsed:
Hybridmulti-levelprofiling(HMLP)
Results:
highestaccuracyof99.72%
Limitations:
furthertestingwithwild malwarebe neededfor practical use.

By integrating these approaches into a comprehensive defense strategy, organizations can better protect against ransomware threats and minimize the potential impact of attacks. Ongoing research and development in these areas contribute to enhancing the effectiveness of ransomware defense mechanism.

III.Existingsystem:

Static and dynamic analysis techniques become less efficient as the malware developers continuouslydevelopevasiontechnique.Behaviour based detection mechanisms may result in file lossuntil detection is achieved.Terminating themonitoring process can render the detection mechanism ineffective. Aims to devise a proactive method that can function as a secondary line of defense to address twounfavorable scenarios from a defensive stand point.failure or termination of the monitoring process before malware detection.delay in the detection mechanism requiring additional time to identify.

IV.Problem Statement:

Ransomware creators continually refine their tactics, rendering traditional signature-based detection methods ineffective. Additionally, ransomware is often delivered through a variety of vectors, including phishing emails, malicious attachments, and compromised websites. Detecting and thwarting these diverse delivery methods.Presents a significant challenge. Ransomware is known for its aggressive use of encryption. Modern variants frequently employ robust encryption algorithms, thereby rendering the recovery of encrypted filesanarduoustask without access to the decryption key. The encryption process itself isa critical component of the ransomware attack lifecycle, and its successful detection can prevent data loss.

V.ProposedSolution:

The proposed system for a proactive Anti Agent Against Ransomware Threats, integrating "RanGAN" and "Hash Conceal," is designed to provide a robust and comprehensive defense mechanism.

RanGANTechnologyIntegration:

RanGAN employs advanced machine learning techniques to actively monitor network and system activities, learning and recognizing ransomware behavior patterns in real-time.

HashConcealImplementation:

Hash Conceal employs advanced cryptographic methods tosecure data,renderingit inaccessible to ransomware encryption.

AdvantageOfProposedSolution:

1.EarlyDetection: Identifiesransomware before they cause harm.

2.DataProtection: Securescriticaldata from ransomware encryption.

3.RapidResponse: Enablesquickreactionsto mitigate attacks.

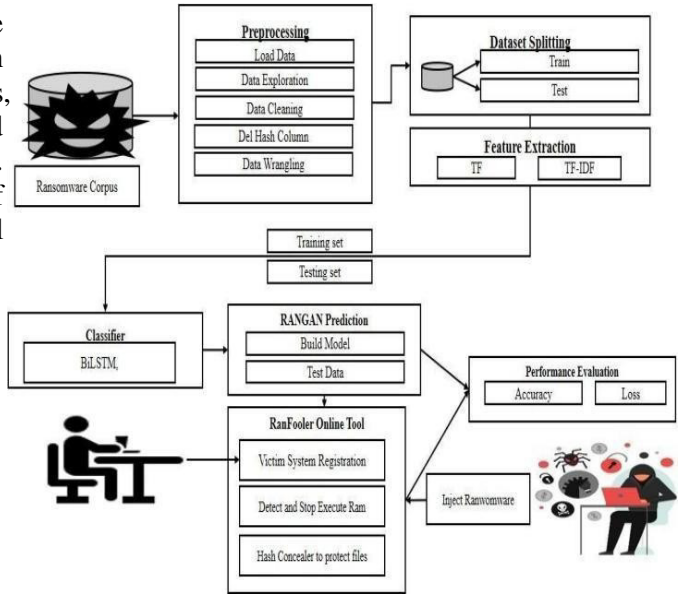
4.Reduced Downtime: Minimizes operationaldisruptionsduringincidents.

5.InsiderThreatMitigation:Guards against internal actors.

6.Cost Efficiency: Saves expenses by avoiding ransom payments.

AlogorithmsUsedForProposedSolution:

1. BiLSTM:ToTraintheModel
2. .RanGAN: To predict ransomware
3. HashConcealer :ToProtecttheFiles



SystemArchitecture:

fig5.1System architecture

Figure 5.1 illustrates the preprocessing process **Load Dataset** : Byte files and Asm files are basically the Ransomware assembly code that contains the information related to the function calls and variable allocation.

Pre-processing: The byte files are exclusivelyused for model training and processing, the appropriate files were first separated from the asm files. the byte files were converted into text files so that the features could be read into the Python code.

Figure 5.2 illustrates **Feature Extraction:** Shallow deep learning- based feature extraction method is used for representing any given Ransomware based on its opcodes. Each byte file has a varying amount of Ransomware code in it, resulting indifferentsizesforeachfile.ThisPiece ofinformation can

be usedas an identification parameter for each Ransomware file.

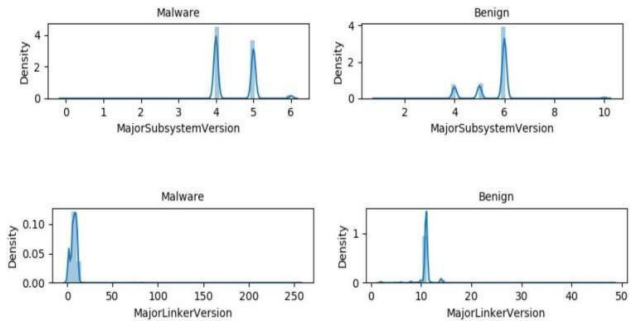


Fig5.2 FeatureExtraction

Ransomware Build and Train: The trainingprocess involves leveraging sophisticated models such as Bidirectional LongShort-Term Memory (BiLSTM) and Gated Recurrent Unit (GRU). Trained on a subset of the dataset, these models acquire the ability to distinguish between benign and malicious samples,layingthefoundationforsubsequentsteps intheRanGAN Classification .fig5.3.

#	Precision	Recall	F1-score	Support
Benign	0.99	0.96	0.97	1004
Malware	0.99	1.0	0.99	2919
Microavg	0.99	0.99	0.99	3923
Macroavg	0.99	0.98	0.98	3923
Weighted avg	0.99	0.99	0.99	3923

fig5.3 RanGAN classification

Ransomwareprediction:

Scan Ransomware Code: RanFooler offers two types of online scans for computer. One is the Antivirus Scan that detects known Ransomware and other Ransomware programs hiding in your computer.The other one is the Prevent Scan that detects ransomware threats that are new and have unknown characteristics.

RanGAN for Real-time Ransomware Prediction: The generator model is pivotal in creating synthetic ransomware samples. It blends noise with ransomware samples from the dataset, producing a mixture fed into the malware detection system.

StopExecuteRansomwareCode: An adaptive Ransomware detection engine that received.Ransomware code. RanFooler can be used to detect and remove the binaries that are covertly fetched. If the anti-virus engine can correctly identify all types of Ransomware, this approach can form a powerfuldefense.

Block and Remove Ransomware: Real-time blockers designed to prevent Ransomware & potentially unwanted apps from installing or executing. Removes the latest adware, browser hijackers, trojans, worms, scamware, viruses & other Ransomware from the computer safely.

SystemIntegration: Behindthescenes, RanFoolerintegratestheselected configuration the backend, associating the chosen files with the provided MAC ID for the users system. The users system is dynamically updated in real-time basedon the configured settings.

Continuous Monitoring: RanGAN continuously monitors the configured systems for any changes orpotential ransomware activity. Automated alerts and notifications keep users informed about the status of their protected files.

HashConcealer:

Hash Conceal for Data Protection: To protect valuable files from ransomware attacks[1], the system employs Hash Conceal technology. This approach involves hiding files in a hidden layer while creating link files in the user layer to access these hidden files.

MappingTable and Hash Table: To facilitatefile recovery, the system maintains a mapping table thatpairs originalfilepaths withhidden filepaths.

Linker for File Access:A linker component is added to the system to redirect users to the hidden files upon accessing the link files.

VI.Conclusion:

In conclusion, adopting a proactive defensive strategy that incorporates Rangan and hash concealment techniques offers a multifaceted approach to mitigating

ransomware threats and safeguarding sensitive data. By strategically deploying Rangan decoys throughout the network, organizations can distract and confuse attackers, leading to early detection and mitigation ofransomwareattacks. Additionally, hash concealmentensurestheprotectionofsensitive databyencryptingitwithcryptographichash functions,preventingunauthorizedaccess and tampering.ThecombinedadvantagesofRangan andhashconcealmentinclude enhancedresilience againstransomware attacks,earlywarning capabilities, minimizedimpactoncritical infrastructure, and compliance with data protection regulations. Furthermore, these techniques provide valuableinsights intoattacker tactics and behaviors, enablingorganizationstorefinetheirsecurity strategiesandbetterdefendagainstevolvingthreats. Intoday'srapidlyevolvingthreatlandscape, proactive defensiveapproachisessentialfor organizations tostayahead ofransomware adversaries.By integratingRanganand hashconcealment intotheircybersecurity framework,organizationscanstrengthentheir defenses,mitigaterisks,andensurethe confidentiality,integrity,andavailabilityoftheir data assets.

VII.FutureEnhancement:

Looking ahead, the proactive defensivestrategy against ransomware, incorporating RanGAN and Hash Conceal, envisions key enhancementsforheightenedresilience.To future- proof against quantum threats, the integration of quantum-resistant cryptography is paramount, ensuring the enduring security ofdata. Additionally, the adoption of blockchain for decentralized file tracking aims to establish an immutable ledger, enhancing traceability and file integrity across the system.

References:

[1].Alwashali A.A.M.A, Rahman N. A. A, and Ismail N, ‘‘A survey of ransomware as a service (RaaS) and methods to mitigate the attack,’’ in Proc.14th Int. Conf. Develop. eSyst. Eng. (DeSE), Sharjah, UAE, Dec. 2021, pp. 92–96, doi: 10.1109/DeSE54285.2021.9719456.

[2].Aslan Ö.A. andSamet R, ‘‘A comprehensive review on malware detection approaches,’’ IEEE Access, vol. 8, pp. 6249–6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

[3].Arabo A, Dijoux R, Poulain T, andChevalier G, ‘‘Detecting ransomwareusing process behavior analysis,’’ Proc. Comput. Sci..H. Oz,

[4].Aris A, Levi A, and Uluagac A. S,‘‘A surveyon ransomware: Evolution, taxonomy, and defense solutions,’’ ACM Comput. Surv., vol. 54,no.11s,pp.1–37,Sep.2022,doi:10.1145/3514229

[5].ChoiJ,LeeJ,LeeG,YuJ,andParkA, ‘‘ A defense mechanism against attacks on files by hiding files,’’ J. Korea Soc. Ind. Inf. Syst., vol.27,no.2,pp.1–10,2022, doi:10.9723/jksiis.2022.27.2.001.

[6].Corbet S and Goodell J.W, ‘‘The reputational contagioneffectsofransomwareattacks,’’Finance Res.Lett., vol.47,Jun.2022,Art. no. 102715,doi: 10.1016/j.frl.2022.102715

[7].Chen Q, and Bridges R.A, ‘‘Automated behavioral analysis of malware: A case study of WannaCry ransomware,’’ in Proc. 16th IEEE Int. Conf.Mach. Learn.Appl.(ICMLA),MiamiBeach, FL, USA, Dec. 2017, pp. 454–460, doi: 10.1109/ICMLA.2017.0-119.

[8].GanfureG.O,C.-F.Wu,Y.-H.Chang,andW.-K. Shih, ‘‘RTrap: Trapping and containingransomware with machine learning,’’ IEEE Trans. Inf. Forensics Security, vol. 18, pp. 1433.

[9].Karthik .S, Karthick.M., Karthikeyan.N, Kannan.S, A multi-Mobile Agent and optimal itinerary planning-based data aggregation in Wireless Sensor Networks, Computer Communications 184 (2022) 24–35, https://doi.org/10.1016/j.comcom.2021.11.019

[10].Karthick.M, Chandru Vignesh.C, Alfred Daniel.J, Sivaparthipan.C.B, An Efficient Multi- mobile Agent Based Data Aggregation in Wireless Sensor Networks Based on HSSO Route Planning, Ad Hoc & Sensor Wireless Networks, Vol. 57, pp. 187–207, DOI: 10.32908/ahswn.v57.10319.

[11].Lee K, Lee S, and Yim K, ‘‘Machine learning based file entropy analysis for ransomware detectioninbackupsystems,’’IEEEAccess,vol.7,pp.110205–110215, 2019.

[12] M. Karthick, Dinesh Jackson Samuel, B. Prakash, P. Sathyaprakash, Nandhini Daruvuri, Mohammed Hasan Ali, R.S. Aiswarya, Real-time MRI lungs images revealing using Hybrid feed forward Deep Neural Network and Convolutional NeuralNetwork,IntelligentDataAnalysis27(2023) S95–S114, DOI 10.3233/IDA-237436.

[13].MelandP.H,BayoumyY.F.F,andSindreG,‘‘The ransomware-as-aservice economy within the darknet,’’ Comput. Secur., vol. 92, May 2020, Art. no. 101762, doi: 10.1016/j.cose.2020.101762.

[14].Moser A, Kruegel C, andE Kirda, ‘‘Limits of static analysis for malware detection,’’ in Proc.23rd.Annu. Comput. Secur. Appl. Conf. (ACSAC), Dec. 2007, pp. 421–430, doi: 10.1109/ACSAC.2007.21.

[15].PoudyalSandDasguptaD,‘‘Analysisof crypto-ransomwareusingMLbasedmulti-levelprofiling,’’IEEEAccess,vol.9,pp.122532122547 ,2021,doi:10.1109/ACCESS.2021.3109260.

[16].YusteJandPastranaS,‘‘Avaddonransomware: An in-depth analysis and decryption of infected systems,’’ Comput. Secur., vol. 109,Oct. 2021, Art. no. 102388, doi: 10.1016/j.cose.2021.102388.

[17].ZhouB,GuptaA,JahanshahiR,EgeleM,and Joshi, ‘‘Hardware performance counters candetect malware: Myth or fact?’’ in Proc. Asia Conf.

