Amrita School of Engineering, Bengaluru
Department of ECE
B. Tech. AY 2023-2024 (IX Semester)
Objective Details – 19EAC499 /Project Phase-2

ZEROTH PRESENTATION

"Enhancing Ransomware Defense: Intelligent Early Detection and Advanced KNN-Density Algorithm Approach for Endpoint Security"

TEAM MEMBERS:

REG. NO.	NAME
BL.EN.U4EAC19069	Somarouthu Prudhvi Raju

Mentor: Dr. Ganapathi Hegde
Batch Id:89

INTRODUCTION

- Ransomware is **malware** used by cybercriminals to encrypt valuable files and data on computers or networks. Victims must then pay a ransom, usually in cryptocurrency, to access their data.
- Ransomware can infiltrate systems by exploiting phishing emails, malicious attachments or software vulnerabilities. It has evolved with targeted attacks and easy-to-use ransomware-as-a-service models that allow even a non-expert to launch attacks.
- Successful ransomware attacks can result in financial losses, operational disruptions and security breaches. Protecting against ransomware requires strong cybersecurity practices, regular data backups, software updates, and user education about potential threats.

MOTIVATION

- Strengthening cyber resilience through proactive defence.
- Elevating endpoint protection to new heights.
- Focusing on protecting individual devices (endpoints) recognizes their vulnerability as entry points for ransomware. Strengthening endpoint security will create a robust barrier against ransomware attacks, enhancing overall cybersecurity.

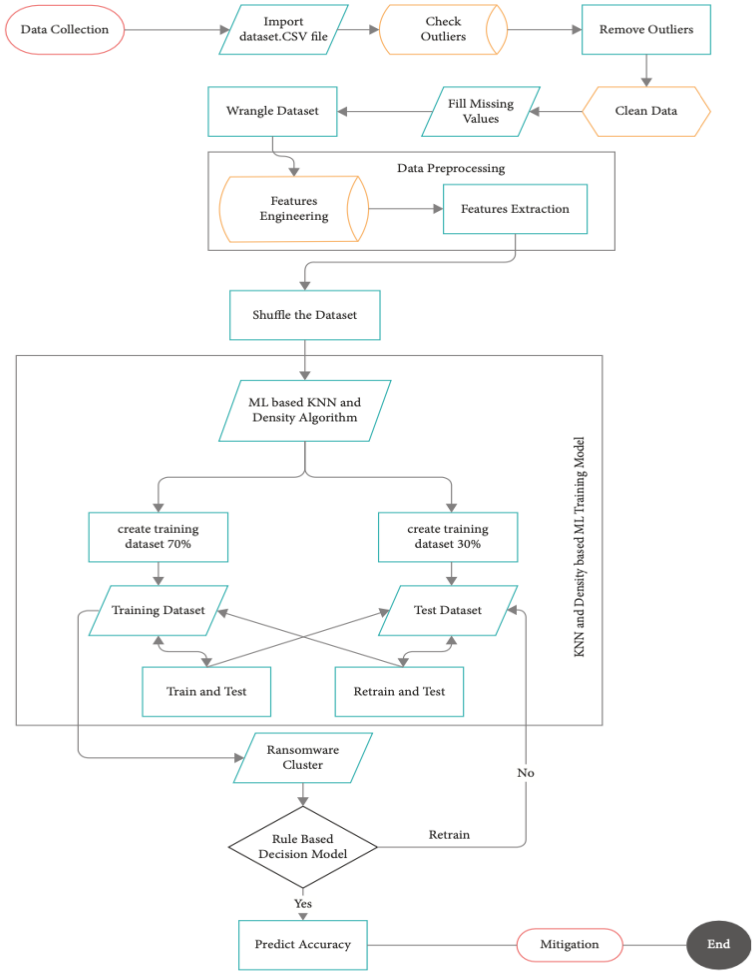
Problem Statement

- Data Loss and File Vulnerability: Victims are at risk of losing their important files and data, which can lead to irreversible loss.
- Financial Consequences: The consequences of ransomware attacks can result in significant financial consequences, including ransom payments, IT recovery costs, legal fees and necessary network adjustments.
- Extended impact: In addition to immediate costs, victims may experience lasting effects such as reduced productivity, business disruption and the need to invest in staff and customer credit monitoring services.

OBJECTIVES

- Develop a proactive algorithm for early identification of ransomware pre-attacks, mitigating potential damage to endpoint systems.
- Create an advanced KNN-density algorithm for ransomware detection, surpassing existing methods in accuracy and precision.
- Minimize false positives by optimizing detection to enhance algorithm usability without unnecessary disruptions.
- Provide practical value to cybersecurity companies, improving anti-ransomware solutions and user protection.
- Contribute to cybersecurity research by introducing a novel machine learning-based approach, inspiring further advancements.

FLOW DIAGRAM



Advanced ransomware pre-attack detection algorithm for endpoint data protection

APPLICATIONS

- SolarWinds Security Event Manager (SEM)
- SolarWinds Patch Manager
- Bitdefender Anti-Ransomware
- Trend Micro Ransomware File Decryptor

REFERENCES:

[1] Du, J., Raza, S.H., Ahmad, M., Alam, I., Dar, S.H. and Habib, M.A., 2022. Digital Forensics as Advanced Ransomware Pre-Attack Detection Algorithm for Endpoint Data Protection. Security and Communication Networks, 2022, pp.1-16.

[2]Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B.C. and Assi, C., 2023. The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. IEEE Access.

[3] B. Shi, L. Han, and H. Yan, "Adaptive clustering algorithm based on kNN and density," Pattern Recognition Letters, vol. 104, pp. 37–44, 2018.

[4] B. Jethva, "A New Ransomware Detection Scheme Based on Tracking File Signature and File Entropy," (Doctoral Dissertation), B.Eng, Gujarat Technological University, Gujarat, India, 2019.