IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 12 August 2024, accepted 11 September 2024, date of publication 16 September 2024,
date of current version 30 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3461965

SURVEY

AI-Based Ransomware Detection: A Comprehensive Review

JANNATUL FERDOUS[1], RAFIQUL ISLAM[2], ARASH MAHBOUBI[3], AND MD ZAHIDUL ISLAM[4]

[1]School of Computing, Mathematics and Engineering, Charles Sturt University, Wagga Wagga, NSW 2650, Australia
[2]School of Computing, Mathematics and Engineering, Charles Sturt University, Albury, NSW 2640, Australia
[3]School of Computing, Mathematics and Engineering, Charles Sturt University, Port Macquarie, NSW 2444, Australia
[4]School of Computing, Mathematics and Engineering, Charles Sturt University, Bathurst, NSW 2795, Australia

Corresponding author: Jannatul Ferdous (jferdous@csu.edu.au)

This work was supported by Charles Sturt University (CSU) Ph.D. Project Operating Fund.

ABSTRACT Ransomware attacks are becoming increasingly sophisticated, thereby rendering conventional detection methods less effective. Recognizing this challenge, this study reviews advanced detection mechanisms and explores the potential of artificial intelligence (AI) techniques to improve detection capabilities. This study reviews the recent literature, including journal articles, conference proceedings, and online resources since 2017, to offer insights into the current state of AI-based ransomware detection and suggests future research directions. This study contributes significantly to the development of a systematic evaluation framework that evaluates each component of the AI-based detection model framework using specific criteria and methodologies and analyzes how various AI algorithms respond to different ransomware attacks, thereby providing insights for more effective and robust detection methods. This review begins with an overview of AI and ransomware, and discusses various types of ransomware attacks, the process of an attack chain, and emerging trends. We then review the existing literature on the core components of AI-based ransomware detection models, including the datasets and challenges arising during data collection, data pre-processing, feature engineering techniques, model training, and performance evaluation for effective model training. This study assessed the detection performance of AI models using metrics such as accuracy, precision, recall, and F1-score. By synthesizing these findings, we identify gaps in the current research and suggest future directions for enhancing AI-based ransomware detection techniques. The insights provided aim to guide researchers and practitioners in developing more robust methods for detecting and mitigating ransomware attacks by using AI.

INDEX TERMS Artificial intelligence, cyberattack, deep learning, feature engineering, machine learning, ransomware attack, ransomware datasets.

I. INTRODUCTION

Ransomware attacks have recently attracted the attention of cybersecurity experts because of the rapid growth of their threats and the development of new variants that can avoid antivirus and anti-malware software [1]. It is now a highly lucrative business for cybercriminals, posing a growing threat to organizations, with trillions of dollars in financial losses. Ransomware is malicious software that encrypts data or restricts access to computer systems, often demanding payment for releasing the affected files [2]. They typically appear in two primary forms, crypto-ransomware and locker-ransomware. Crypto-ransomware encrypts all files in the target device, whereas locker ransomware renders the device inoperable by locking the entire system rather than only specific files [3].

Ransomware attacks have significantly adverse effects on IT systems. The consequences of these attacks include data or information loss owing to file encryption, financial costs to businesses for incident handling, other security-related

The associate editor coordinating the review of this manuscript and approving it for publication was Vicente Alarcon-Aquino.