IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 3, Issue 3, July 2023
Impact Factor: 7.301

Autonomous Ransomware Forensics: Advanced ML Techniques for Attack Attribution and Recovery

Gaurav Sarraf
Independent Researcher
sarrafgsarraf@gmail.com

Abstract: *Ransomware attacks are one of the most disastrous cybersecurity risks, as they encrypt important information and require financial compensation to decrypt keys, leading to billions of monetary losses every year. The advanced development of ransomware families requires highly sophisticated machine learning solutions to be detected and automatically analyzed. In this study, autonomous ransomware forensics framework was introduced using sophisticated machine learning models to perform attack attribution and recovery procedures on a holistic ransomware identification dataset. The methodology involves systematic preprocessing of data such as data cleaning, categorical variables label encoding, and rectification of class imbalance by use of under-sampling mechanisms, Principal Component Analysis (PCA) to facilitate optimal selection of features, and data normalization to promote quality of structured input. A higher accuracy (ACC), precision (PRE), recall (REC), and F1-score (F1) of 98.21%, 97.33%, and 97.45%, respectively, for the constructed Long Short-Term Memory (LSTM) neural network model indicates improved computational capability to identify ransomware behavioral patterns and time sequences. Evaluation against other popular classification models, such as Random Forest (with a 96.90% accuracy rate), Support Vector Machine (91.67% accuracy), and Convolutional Neural Network (94.38% accuracy), demonstrates the efficacy of the LSTM architecture. The autonomous framework enables real-time threat attribution and automated recovery protocol initiation, significantly reducing incident response time and operational disruption in enterprise cybersecurity environments while eliminating dependency on manual forensic expertise.*

Keywords: Cybersecurity, Ransomware Forensic, Ransomware Detection Dataset, Machine Learning, LGBM, Ransomware Attack, Artificial Intelligence, Attribution and Recovery

DOI: 10.48175/IJARSCT-11978W