RS-FEDRAD: Robust and Scalable Federated Ransomware Detection Using TTP-Enhanced Dataset

Chinonso E. Ali
Hubei Engineering Research Center on Big Data Security, School of Cyber Science & Engineering, Huazhong University of Science and Technology, Wuhan 430074
Shenzhen Huazhong University of Science and Technology Research Institute, Shenzhen, China

Songfeng Lu
Hubei Engineering Research Center on Big Data Security, School of Cyber Science & Engineering, Huazhong University of Science and Technology, Wuhan 430074
Shenzhen Huazhong University of Science and Technology Research Institute, Shenzhen, China

Francis A. Ruambo
Hubei Engineering Research Center on Big Data Security, School of Cyber Science & Engineering, Huazhong University of Science and Technology, Wuhan 430074
Department of Information Systems and Technology, College of Information and Communication Technology, Mbeya University of Science and Technology, Mbeya 131, Tanzania

Francelle Tchamini
Hubei Engineering Research Center on Big Data Security, School of Cyber Science & Engineering, Huazhong University of Science and Technology, Wuhan 430074

Abstract

Ransomware continues to pose a significant challenge to the cyberspace industry, with rising frequency and complexity threatening data integrity, availability, and confidentiality. Current detection methods often fail to effectively address modern ransomware due to inadequate feature sets and over reliance on centralized architectures, posing privacy and scalability challenges. We present RS-FEDRAD, a robust and scalable federated learning (FL)-based ransomware detection system that combines FL with deep dynamic analysis, using a novel Tactics, Techniques, and Procedures (TTP) enhanced dataset to overcome these limitations. This approach first captures critical ransom-ware behavioral attributes such as application programming interface (API) calls, dynamic link library (DLL) usage, and mutual exclusion (Mutex) operations, before mapping them to their corresponding ransomware-related TTPs using the MITRE ATT@CK framework. Extensive experimental evaluations highlight the effectiveness of the framework against unknown black-box and known white-box attacks, utilizing a hybrid convolutional neural network (CNN) and long short-term memory (LSTM) to achieve an impressive accuracy of 99.90% and an average federated accuracy of 99.50%. RS-FEDRAD offers a scalable, privacy-preserving solution that enhances ransomware detection and understanding of attacker strategies through its TTP-enhanced feature set., advancing ransomware mitigation with adaptive, decentralized, and robust security for today's rapidly evolving threat landscape.

Keywords

Deep learning, Dynamic analysis, Federated learning, MITRE ATT@CK framework, Ransomware detection, TTP enhanced dataset.