Autonomous Software Security Vulnerability Detection based on Machine Learning

Abstract:

In the realm of cybersecurity, timely and accurate detection of software vulnerabilities is paramount. This research presents a comprehensive comparative analysis of three advanced neural network models—Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), and Convolutional Neural Networks (CNN)—in the context of detecting vulnerabilities within software code. Building upon the foundational work of VUDENC (Vulnerability Detection with Deep Learning on a Natural Codebase), this study extends the exploration to a more diverse set of deep learning models. The primary dataset, derived from VUDENC project's collection of real-life Python code vulnerabilities from GitHub, is uniformly processed and utilized to train and test each model under identical conditions. The research focuses on determining the efficacy of each model in accurately identifying various software vulnerabilities, assessed through metrics such as accuracy, precision, and recall. Preliminary results have indicated notable differences in the models' performance, with each exhibiting unique strengths and challenges. The study not only contributes to the field by identifying the most effective techniques for vulnerability detection but also provides insights into the adaptability and scalability of these models for real-time software vulnerability detection development. The findings aim to pave the way for more robust, efficient, and automated vulnerability detection systems, ultimately enhancing software security in today's interconnected digital world.