FedREVAN: Real-time DEtection of Vulnerable Android Source Code Through Federated Neural Network with XAI

Janaka Senanayake (Faculty of Science, University of Kelaniya, Kelaniya, Sri Lanka)

Computer Security. ESORICS 2023 International Workshops

pp 426–441

Published Date: 12 March 2024

ISBN: 978-3-031-54128-5

Abstract

Adhering to security best practices during the development of Android applications is of paramount importance due to the high prevalence of apps released without proper security measures. While automated tools can be employed to address vulnerabilities during development, they may prove to be inadequate in terms of detecting vulnerabilities. To address this issue, a federated neural network with XAI, named FedREVAN, has been proposed in this study. The initial model was trained on the LVDAndro dataset and can predict potential vulnerabilities with a 96% accuracy and 0.96 F1-Score for binary classification. Moreover, in case the code is vulnerable, FedREVAN can identify the associated CWE category with 93% accuracy and 0.91 F1-Score for multi-class classification. The initial neural network model was released in a federated environment to enable collaborative training and enhancement with other clients. Experimental results demonstrate that the federated neural network model improves accuracy by 2% and F1-Score by 0.04 in multi-class classification. XAI is utilised to present the vulnerability detection results to developers with prediction probabilities for each word in the code. The FedREVAN model has been integrated into an API and further incorporated into Android Studio to provide real-time vulnerability detection. The FedREVAN model is highly efficient, providing prediction probabilities for one code line in an average of 300 ms.

Citation

Senanayake, J., Kalutarage, H., Petrovski, A., Al-Kadri, M.O., Piras, L. (2024). FedREVAN: Real-time DEtection of Vulnerable Android Source Code Through Federated Neural Network with XAI. In: Katsikas, S., et al. Computer Security. ESORICS 2023 International Workshops. ESORICS 2023. Lecture Notes in Computer Science, vol 14399. Springer, Cham. https://doi.org/10.1007/978-3-031-54129-2_25

Publisher

Springer, Cham