Transparency in Detecting Man-in-the-Middle Attacks on SS7 Networks Using SHAP Explainable AI

Fauzan Rizqi Muhammad[1], Parman Sukarno[2], and Aulia Arif Wardana[3]

[1] zannrz@student.telkomuniversity.ac.id
[2] psukarno@telkomuniversity.ac.id
School of Computing, Telkom University
[3] aulia.wardana@pwr.edu.pl
Wrocław University of Science and Technology, Wrocław, Poland

Abstract. This study addresses the security vulnerabilities inherent in the SS7 protocol, with a specific focus on mitigating Man-in-the-Middle (MITM) attacks. Despite technological advancements, persistent security issues in Signaling System No. 7 (SS7) underscore the need to enhance user protection and minimize risks. The primary objective is to leverage Explainable Artificial Intelligence (XAI) to make AI decisions in telecommunications more transparent and justifiable. This research is using advanced machine learning algorithms, including Random Forest, Autoencoders, and K-Means Clustering, integrated into SHapley Additive exPlanations (SHAP) to enhance the interpretability of AI models. The limited availability of specific SS7 datasets forces this study to use existing dataset that was used by another study. The research methodology involves data collection and pre-processing, followed by the implementation and optimization of algorithms to effectively detect and analyze vulnerabilities. The integration of XAI aims to make the machine learning detection process transparent, improving the security of the SS7 protocol. This approach is crucial to identify potential attack vectors and reduce associated risks. The results demonstrate high precision, with the Random Forest algorithm achieving 94% accuracy, the autoencoders showing a low loss around ± 0.10, and K-Means Clustering achieving a high Silhouette Score of 0.999. Furthermore, SHAP values provide information on the distinctions and similarities between the algorithms.

Keywords: MITM Attacks · SS7 Protocol · XAI · Machine Learning · Intrusion Detection