Comparative evaluation of the performance and effectiveness of Machine Learning and Deep Learning algorithms for anomaly detection in Android log analysis

Okangondo Loshima Junior*, Serigne Modou Kara Samb**, Mohamed Kaba Keita***, Doudou Fall***,
Moussa Dethie Sarr**, Idy Diop***

*Faculty of Science and Technology, University Cheikh Anta Diop of Dakar, Dakar 630-0101, Senegal
**Science technology mathematics computer science, iba der thiam university, thies, Senegal
***Ecole Supérieure Polytechnique, University Cheikh Anta Diop of Dakar, Dakar 630-0101, Senegal
juniorokangondoloshima@esp.sn, smkara.samb@univ-thies.sn, keita.mohamed@esp.sn, doudou.fall@esp.sn,
mdsarr@univ-thies.sn, idy.diop@esp.sn

***Abstract*—Due to the substantial rise in cyberattacks aimed at Android devices, log analysis has become critical for identifying and mitigating security anomalies. This article conducts a comparative analysis of machine learning and deep learning algorithms for the detection of anomalies within Android logs, specifically sourced from the LogHub dataset. These logs, gathered from Android smartphones equipped with extensive instrumentation, are both rare and intricate. The complexity arises from Android's multithreaded architecture, making anomaly detection a challenging task. The aim of this study is to identify the most suitable algorithms for detecting anomalies in Android logs, evaluating three algorithms per category (machine learning and deep learning). Using metrics such as precision, recall, F1 score and AUC-ROC, the analysis highlights the effectiveness of each approach depending on context. Finally, recommendations are proposed for optimizing current methodologies and exploring new research perspectives**

***Keyword*— ML, DL, DBSCAN, CNN, RNN, SVM, OCSVM**

Okangondo Loshima Junior was born in Kananga, Democratic Republic of Congo, in 1990. He obtained a Master's degree in Cybersecurity from the École Supérieure Polytechnique de Dakar, Senegal, in 2022, a Master's degree in Software Engineering from the Université Numérique Cheikh Hamidou Kane in 2021, and a Master's degree in Computer Management from the Université Notre-Dame du Kasayi, DRC, in 2015. His main field of study is cybersecurity, digital forensics and software engineering.

He is currently a doctoral student at the Doctoral School of Mathematics and Computer Science at Cheikh Anta Diop University in Dakar, where he is working on the design of a digital investigation platform adapted to infrastructures in developing countries. He is also a trainer in cybersecurity, programming and systems security at the École Supérieure Polytechnique, where he supervises practical work and research dissertations. His publications include work on optimizing digital investigation processes and anomaly detection in Android logs, accepted and pending publication in IEEE and Scopus journals. His research interests include mobile cybersecurity, the application of artificial intelligence in digital forensics, and digital infrastructure security.

Doctoral student Okangondo Loshima Junior is not yet an IEEE member, but has obtained several certifications, including Ethical Hacking Essentials (EC-COUNCIL), ISO 27001, Cyber OPS (Cisco). He actively participates in committees and conferences on cybersecurity and digital forensics.