Towards Enabling Security and Privacy in the AI Marketplace

Venkata Satya Sai Ajay Daliparthi[1[0000−0001−6895−4503]], Nurul Momen[1[0000−0002−5235−5335]], Kurt Tutschku[1[0000−0003−4814−4428]], and Miguel De Prado[2[0000−0003−4350−1617]]

[1] Blekinge Institute of Technology, Karlskrona, Blekinge, Sweden
venkatasatyasaiajay.daliparthi@bth.se, nurul.momen@bth.se, kurt.tutschku@bth.se
[2] Bonseyes Community Association, Lausanne, Vaud, Switzerland
miguel.deprado@bonseyes.com

Abstract. The AI marketplace engages individuals and SMEs to collaborate and exchange AI artifacts by providing AI-as-a-Service to enhance the application deployment workflow. This work discusses the findings and experiences involved in working towards enabling security and privacy in the AI marketplace operations that include:
(1) Protocols for transparent trading of AI artifacts that focus on (i) the compatibility of the trained models, (ii) the reproducibility of the claimed metrics, and (iii) the uncertainty quantification of the model decision
(2) The design of a decentralized data marketplace that uses crowdsourcing methods for data collection and employs isolated environments to preserve data privacy during model training.

Keywords: Trust Management · Data Marketplaces · Smart Contracts