Title: "Guarding Agriculture's IoT Realm: Detecting Malware and Strengthening Cybersecurity"

The agriculture sector is undergoing a digital revolution through widespread IoT adoption, transforming farming practices, monitoring and consumer-farmer interactions. Yet, this shift from traditional to wireless, sensor-based systems poses cybersecurity challenges. Weak security algorithms in some agricultural IoT devices make gateways susceptible to attacks like congestion and denial of service. Precision agriculture devices are also at risk of device capture attacks, jeopardizing sensitive data. Interconnected objects like drones and sensors communicate through machine-to-machine or cloud networks, emphasizing the need for robust authorization and trust mechanisms to safeguard vital agricultural data. This transition necessitates vigilant cybersecurity measures.

In the proposed model, IoT malware from the MQTT dataset has been detected and classified with the help of different machine learning algorithms such as Random Forest, CNN, Gradient Boost, Light GBM, and Naive Bayes which are then compared on the basis of their accuracy, F1 score, and confusion matrix. It is observed that Random Forest outperforms the other algorithms and is effective in classifying the malware with an accuracy of 90.5%. In conclusion, this model offers a comprehensive resource for researchers and agriculturists seeking to secure IoT deployments in agriculture. Using the observations of the model, security threats can be analysed and effective countermeasures can be suggested to improve the overall cybersecurity and resilience of IoT-enabled agricultural systems in an era of rapid digital transformation.