58th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Dr. Rizka Purwanto
Monash University, Indonesia

Dr. Muhammad Johan Alibasa
Monash University, Indonesia
Dr. Rabbia Saleem
UNSW Canberra, Australia
Ms. Arumjeni Mitayani
National Research and Innovation Agency (BRIN), Indonesia
Dr. Melrose Brown
Australian Defence Force Academy (ADFA), Australia

HOMOMORPHIC ENCRYPTION FOR SECURE MODEL UPDATES IN FEDERATED SATELLITE CONSTELLATIONS

Abstract

The democratization of space, driven by advancements in small and miniaturized satellites, has significantly lowered satellite manufacturing costs. This shift enables more nations and organizations to launch satellites for diverse applications, such as Earth observation, climate monitoring, or communications. While onboard AI holds great potential for supporting these satellite missions, small satellites face resource constraints that pose challenges, including limited computational power and bandwidth. A potential solution is to deploy constellations of multiple satellites for improved coverage and data throughput. Federated learning further supports these constellations by allowing local data processing on each satellite while sharing only model updates. However, even though this minimizes raw data transfers, unencrypted model or gradient updates can still leak private information from the satellites' data.

To address this confidentiality issue, we propose integrating homomorphic encryption (HE) into a multi-node federated learning framework. By aggregating encrypted model updates at a central node, without decrypting them, this approach preserves each satellite's data privacy more robustly than traditional methods. We introduce a novel encrypted framework for federated learning in satellite constellations, leveraging homomorphic encryption (HE) for secure model aggregation on unencrypted model parameter data. Our experiments, conducted over a communication network using NVIDIA Jetson devices to simulate realistic satellite operations and communications, demonstrate that homomorphic encryption can safeguard data privacy while maintaining model accuracy and manageable runtime performance. This framework not only advances federated learning in satellite constellations, but also offers a practical pathway to enhance satellite cybersecurity. The enhancement of satellite data security through privacy-preserving mechanisms contributes to the overall satellite system resilience from cyberattacks and data interception.