Keselamatan pembelajaran bersekutu dalam era 6G: Kajian tentang teknik konseptual dan platform perisian yang digunakan untuk penyelidikan dan analisis

Description

Pembelajaran Bersekutu (FL) ialah paradigma AI yang berkembang pesat yang membolehkan pelbagai entiti melatih model secara kolaboratif tanpa berkongsi data individu mereka, yang penting untuk mengekalkan privasi. Terdapat pelbagai jenis FL yang muncul berdasarkan peranti, data dan seni bina rangkaian seperti yang digambarkan dalam Rajah 1. Dengan kemunculan rangkaian Generasi Keenam (6G) yang dijangkakan, FL dijangka menjadi semakin penting untuk menangani cabaran yang berkaitan dengan privasi data, keselamatan, dan kebolehskalaan dalam sistem teragih dan heterogen. Penyelidikan semasa dalam domain keselamatan FL dalam sistem komunikasi 6G adalah luas, tetapi kejayaan kajian ini sebahagian besarnya bergantung pada konsep dan platform yang digunakan untuk analisis dan penilaian. Artikel ini bermula dengan memberikan gambaran keseluruhan FL dalam konteks rangkaian 6G, menekankan keperluan untuk analisis menyeluruh untuk mendapatkan FL dalam persekitaran yang melibatkan pelbagai entiti teragih dan heterogen seperti yang ditunjukkan dalam Rajah 2. Ia kemudiannya mengenal pasti dan menyemak secara sistematik teknik konsep dan platform perisian yang penting untuk menjalankan penilaian berkaitan keselamatan FL dalam komunikasi 6G.

Sebagai hasil penyelidikan, kajian ini menyerlahkan cabaran penting yang dihadapi semasa analisis keselamatan FL dalam 6G, yang termasuk isu yang berkaitan dengan kerumitan persekitaran yang diedarkan, kepelbagaian entiti yang mengambil bahagian dan skala sistem yang terlibat. Akhir sekali, semakan menggariskan isu penyelidikan terbuka utama yang masih belum dapat diselesaikan. Ini termasuk membangunkan rangka kerja keselamatan yang lebih teguh, meningkatkan kebolehskalaan FL dalam rangkaian 6G, dan mencipta alat dan platform yang lebih berkesan untuk analisis komprehensif. Dengan menangani cabaran ini, penyelidikan masa depan boleh memajukan keselamatan FL dalam sistem komunikasi 6G dengan ketara, memastikan rangkaian dipacu AI yang lebih selamat dan lebih dipercayai.

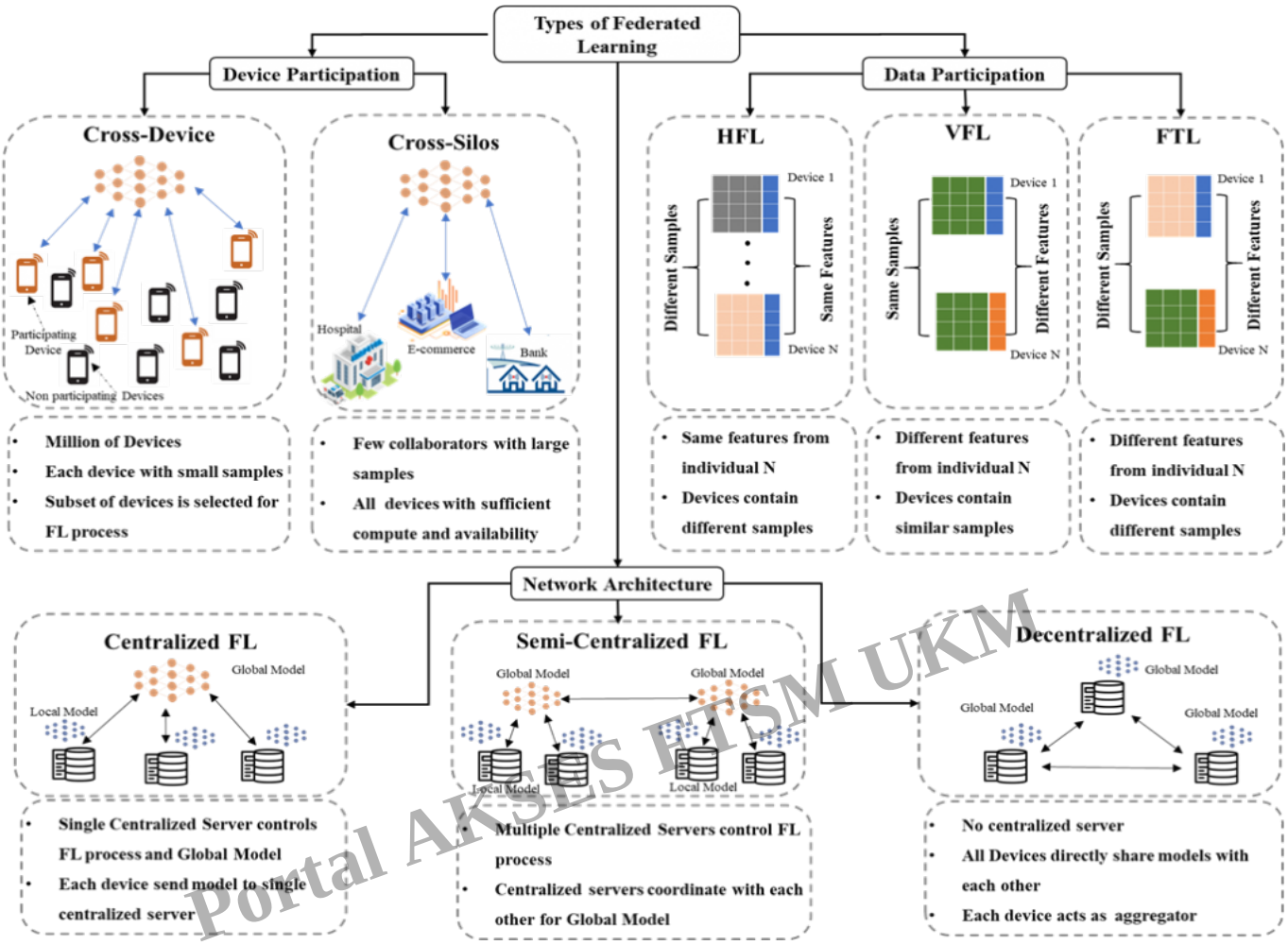

FIGURE 1. Types of Federated Learning

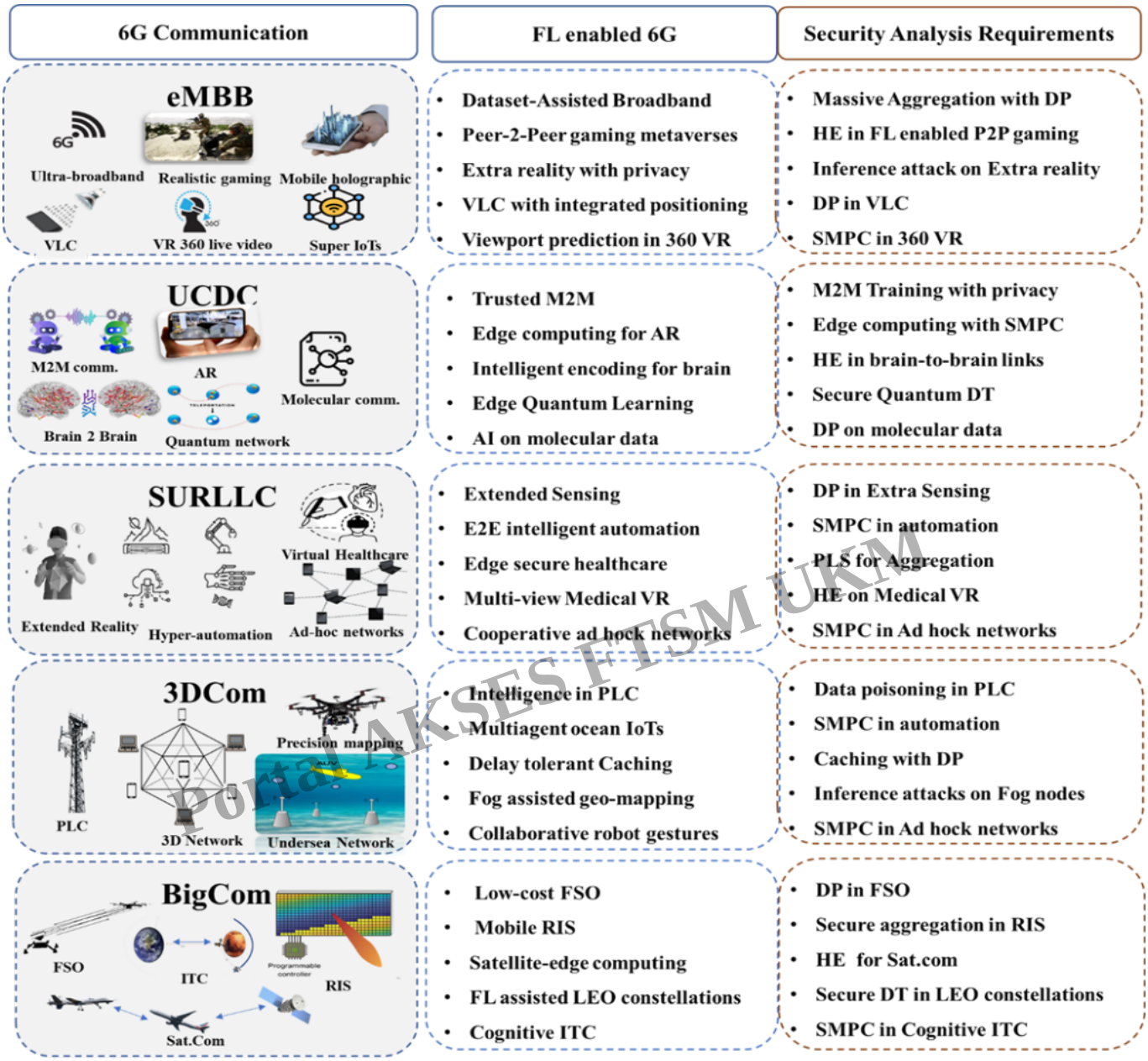

FIGURE 2. Security of FL in 6G communication

Oleh:
Rosilah Hassan
rosilah@ukm.edu.my

Pengarang Bersama:
Syed Hussain Ali Kazmi
Faizan Qamar
Kashif Nisar
Mohammed Azmi Al-Betar

Category

1. Aktiviti Penyelidikan

Date Created
2024/12/12
Author
root