ABSTRACT

FACIAL RECOGNITION USING MACHINE LEARNING AND FEDERATED LEARNING

By:

Faza Nanda Yudistira

19/438446/PA/18904

Biometric recognition, particularly facial recognition, has been a part of our daily lives. One of the most potent surveillance technologies ever created is facial recognition software, which maps, analyses, and then validates the identification of a face in a picture or video (Klosowski, 2020). While many individuals only use facial recognition to unlock their phones or organise their images, how businesses and governments use it will have a much bigger impact on people's lives.

Software for facial recognition uses machine learning, which needs a lot of data to "learn" and deliver accurate results. There is always a greater risk when there is a lot of data. In the event of a data breach, this issue might become quite significant because the privacy of the users could be seriously endangered and made public. This research intends to investigate the most accurate and effective machine learning technique that can be used to develop a predictive model, and then use federated learning to train the model to overcome such concerns.

Using the presented methods suggested and a dataset obtained from UTKFace, we were able to develop models with great accuracy and performed well for prediction while also respecting the clients' data privacy through the use of federated learning.

Key Words: *Analytical Study, Algorithm Implementation, Error Measurement Tools, Federated Learning, Machine Learning*

ABSTRAK

PENGENALAN WAJAH DENGAN *MACHINE LEARNING* DAN *FEDERATED LEARNING*

Oleh:

Faza Nanda Yudistira

19/438446/PA/18904

Pengenalan biometrik, khususnya pengenalan wajah, telah menjadi bagian dari kehidupan kita sehari-hari. Salah satu teknologi pengawasan paling ampuh yang pernah diciptakan adalah perangkat lunak pengenalan wajah, yang memetakan, menganalisis, dan kemudian memvalidasi identifikasi wajah dalam gambar atau video (Klosowski, 2020). Meskipun banyak orang hanya menggunakan pengenalan wajah untuk membuka kunci ponsel atau mengatur gambar mereka, cara perusahaan dan pemerintah menggunakannya akan berdampak jauh lebih besar pada kehidupan masyarakat.

Perangkat lunak pengenalan wajah menggunakan *machine learning*, yang memerlukan banyak data untuk "dipelajari" dan memberikan hasil yang akurat. Selalu ada risiko yang lebih besar bila ada banyak data. Jika terjadi pelanggaran data, masalah ini mungkin menjadi cukup signifikan karena privasi pengguna dapat sangat terancam dan dipublikasikan. Penelitian ini bermaksud untuk menyelidiki teknik *machine learning* yang paling akurat dan efektif yang dapat digunakan untuk mengembangkan model prediktif, dan kemudian menggunakan pembelajaran gabungan untuk melatih model guna mengatasi masalah tersebut.

Dengan menggunakan metode yang disarankan dan kumpulan data yang diperoleh dari UTKFace, kami berhasil mengembangkan model dengan akurasi tinggi dan berkinerja baik untuk prediksi sekaligus menghormati privasi data klien melalui penggunaan *federated learning*.

Kata Kunci: *Kajian Analitik, Implementasi Algoritma, Alat Ukur Kesalahan, Federated Learning, Machine Learning*