ABSTRACT

Binary Classification on Encrypted Image Data Using Paillier's Homomorphic Encryption and Convolutional Neural Network

by

Faisal Malik Widya Prasetya

15/380915/PA/16723

Machine learning algorithm has been developed and used for solving many real-world problems. Deployment of machine learning in cloud computing platform also enhance the power of machine learning to solve those problems online. Unfortunately, deployment of machine learning for private data in cloud computing platform is limited due to cloud system privacy and confidentiality issue. Common practice of confidential and private cloud system approach takes a lot of steps to modify data and unable to take an advantage of cloud computing since the computation is done in local computer and in this case.

Homomorphic encryption can be used to solve this problem. Homomorphic encryption allows computation on ciphertext. This allows secure computation to be performed in cloud server. Unfortunately, due to the limit of operations that can be performed in homomorphic encrypted data, current approach of machine learning algorithm in homomorphic encrypted data still has a problem. Since they are using fully homomorphic encryption which can only perform binary operation between ciphertext, the model can only analyze data that is encrypted using the same public key as the training data.

This research proposes a solution to implement machine learning algorithm, especially convolutional neural network for diagnosing pneumonia on encrypted CXR image using Paillier's cryptosystem. Paillier's cryptosystem has two main homomorphic properties which allow the encrypted CXR to be operated on CNN model without encrypting the model and perform retraining on each different public key. There are several modifications that are needed on CNN model in order to make the operation on encrypted CXR possible. Evaluation will be conducted for the overall performance of the proposed model by comparing it with model that analyzes unencrypted CXR, i.e. the original CNN.

Keywords: Machine Learning, Cloud System, Homomorphic Encryption, Paillier's Homomorphic Encryption, Convolutional Neural Network

INTISARI

Klasifikasi Biner pada Data Gambar Terenkripsi menggunakan Enkripsi Homomorfik Paillier dan Convolutional Neural Network

by

Faisal Malik Widya Prasetya

15/380915/PA/16723

Algoritma pembelajaran mesin telah dikembangkan dan digunakan untuk memecahkan banyak masalah dunia nyata. Penerapan pembelajaran mesin di platform cloud computing juga meningkatkan kekuatan pembelajaran mesin untuk memecahkan masalah tersebut secara daring. Sayangnya, penyebaran pembelajaran mesin untuk data pribadi dalam platform cloud computing terbatas karena masalah privasi dan kerahasiaan pada sistem cloud. Praktik umum pendekatan sistem cloud yang rahasia dan privat menggunakan banyak langkah untuk memodifikasi data dan tidak dapat mengambil keuntungan dari cloud computing karena komputasi dilakukan di komputer lokal.

Homomorphic encryption dapat digunakan untuk menyelesaikan masalah ini. Homomorphic encryption memungkinkan komputasi pada ciphertext. Ini memungkinkan perhitungan yang aman dilakukan di server cloud. Sayangnya, karena batas operasi yang dapat dilakukan dalam data terenkripsi homomorfik, pendekatan saat ini dari algoritma pembelajaran mesin dalam data terenkripsi homomorfik masih memiliki masalah. Karena mereka menggunakan fully homomorphic encryption yang hanya dapat melakukan operasi biner antara ciphertext, model hanya dapat menganalisis data yang dienkripsi menggunakan public key yang sama dengan data training.

Penelitian ini mengajukan solusi untuk mengimplementasikan algoritma pembelajaran mesin, khususnya convolutional neural network untuk mendiagnosis pneumonia pada gambar CXR terenkripsi menggunakan cryptosystem Paillier. Cryptosystem Paillier memiliki dua sifat homomorfik utama yang memungkinkan CXR terenkripsi untuk dioperasikan pada model CNN tanpa mengenkripsi model dan melakukan training ulang pada setiap public key yang berbeda. Ada beberapa modifikasi yang diperlukan pada model CNN untuk memungkinkan operasi pada CXR terenkripsi menjadi mungkin. Evaluasi akan dilakukan untuk kinerja keseluruhan dari model yang diajukan dengan membandingkannya dengan model yang menganalisis CXR tidak terenkripsi, yaitu CNN asli.

Keywords: Pembelajaran Mesin, Cloud System, Homomorphic Encryption, Paillier's Homomorphic Encryption, Convolutional Neural Network