

Machine learning dengan data yang terenkripsi secara homomorfis = Machine learning with homomorphically encrypted data

Khalid Muhammad, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20475001&lokasi=lokal>

Abstrak

ABSTRAK

Machine learning dapat digunakan untuk menganalisis berbagai macam jenis data, termasuk data yang umumnya bersifat rahasia. Sebuah model machine learning yang sudah dilatih dapat dibungkus dalam sebuah aplikasi web sehingga model tersebut dapat diakses dengan mudah via internet. Namun, jika data yang ingin dianalisis bersifat pribadi atau rahasia seperti data medis atau keuangan maka hal ini menjadi masalah, pengelola aplikasi itu dapat saja membaca data rahasia yang di-input. Skema enkripsi homomorfis dapat digunakan untuk menghadapi masalah ini. Salah satu skema enkripsi yang memiliki sifat homomorfis ialah skema enkripsi Paillier. Pada penelitian ini ditunjukkan bahwa suatu jenis model machine learning tertentu dapat menerima input data yang terenkripsi dengan skema enkripsi Paillier dan menghasilkan output yang terenkripsi dengan kunci yang sama. Konsep ini didemonstrasikan dengan melatih sebuah model machine learning dengan database MNIST. Kemudian, model ini diuji dengan data test yang terenkripsi dengan skema enkripsi Paillier. Hasil percobaan menunjukkan akurasi model mencapai 92,92.

<hr>

ABSTRACT

Machine learning can be used to analyze various kinds of data, including confidential data such as medical or financial data. A trained machine learning model can be wrapped in a web application so that people can access it easily via internet. But if the data to be analyzed is private or confidential, this will cause a problem, the application administrator may read our input. Homomorphic encryption scheme can be used to overcome this kind of problem. Paillier encryption scheme is one kind of encryption scheme that has homomorphic property. In this research, it will be shown that one type of machine learning model can take an input encrypted by Paillier encryption scheme and produce an output encrypted with the same key. This concept is demonstrated by training a machine learning model with the MNIST database of hand written digits. This model will be tested with the test data encrypted with Paillier encryption scheme. The experiment shows that the model achieved 92.92 accuracy.