penerapan data mining untuk monitoring intrusi: studi kasus balai jaringan informasi dan komunikasi = Implementation of data mining for intrusion monitoring: a case study of the information and communication network center

Annisa Andarrachmi, author

Abstrak

ABSTRAK
Balai Jaringan Informasi dan Komunikasi (BJIK) sebagai salah satu balai di Badan Pengkajian dan Penerapan Teknologi (BPPT) memiliki tugas dalam penerapan teknologi informasi dan komunikasi (TIK) untuk kepentingan pemerintah pusat, daerah, publik, komunitas ilmu pengetahuan teknologi, dan industri. Tugas tersebut diwujudkan salah satunya dengan membangun sistem informasi monitoring teknologi informasi dan komunikasi yang bernama Simontik. Kemajuan tren teknologi dan ancaman siber yang tidak dapat dihindari membutuhkan adanya penerapan data mining untuk monitoring intrusi dalam melindungi informasi penting dimana perangkat lunak anti virus dan firewall tidak cukup memberikan perlindungan penuh sesuai dengan kondisi BJIK saat ini. Sejalan dengan hal tersebut, beberapa penelitian terdahulu juga menjelaskan teknik deep learning atau deep neural network pada data mining yang telah mencapai keberhasilan jauh lebih baik di berbagai aplikasi khususnya big data sets classification karena memberikan hasil yang akurat dalam menyelesaikan permasalahan sistem monitoring intrusi. Berdasarkan hal tersebut, penelitian ini menggunakan teknik classification dengan algoritme deep learning, support vector machine, dan random forest sebagai pembanding. Penelitian ini menggunakan metodologi knowledge discovery from data (KDD) dimana data mining hanya merupakan suatu langkah penting dalam urutan prosesnya. Hasil akhir dari penelitian ini merupakan model prediksi yang dikemudian diuji dengan dataset Simontik untuk diketahui akurasinya. Hasil yang didapatkan dari penelitian ini adalah algoritme deep neural network dan random forest menghasilkan akurasi yang paling baik, yaitu sebesar 99,91% dibandingkan dengan algoritme support vector machine yang memiliki akurasi sebesar 98,11%.
ABSTRACT
The Information and Communication Network Center (BJIK) as one of the centers in the Agency for the Assessment and Application of Technology (BPPT) has the task of implementing information and communication technology (ICT) for the benefit of the central, regional, public, technological and industrial science communities. One of the tasks is realized by building an information and communication technology monitoring information system called Simontik. The unavoidable progress of technological trends and cyber threats requires the application of data mining for intrusion monitoring in protecting important information where anti-virus software and firewalls do not provide full protection in accordance with current BJIK conditions. In line with this, several previous studies also explained that deep learning techniques or deep neural networks in data mining that have achieved success are far better in various applications, especially the big data sets classification because they provide accurate results in solving intrusion monitoring system problems. Based on this, this study uses classification techniques with deep learning algorithms, support vector machines, and random forest as a comparison. This study uses the knowledge discovery from data (KDD) methodology where data mining is only an important step in the sequence of the process. Result of

this study is a prediction model which is then tested with the Simontik dataset to determine its accuracy. The results obtained from this study are that deep neural network and random forest algorithms produce the best accuracy, which is 99.91% compared to the support vector machine algorithm which has an accuracy of 98.11%.