INTISARI

PENCOCOKAN DATA PENGGUNA JARINGAN INTERNET DENGAN MENGGUNAKAN ALGORITMA HOMOMORPHIC ENCRYPTION

Oleh

YULIANA

19/448738/PPA/05821

Teknologi jaringan saat ini berhadapan dengan isu keamanan jaringan, serangan siber dan lainnya. Salah satu isu dari masalah keamanan jaringan adalah penyusupan, kegiatan ini dilakukan untuk menyusup ke jaringan pengguna secara diam-diam melalui jaringan internet. Untuk mendeteksi dan mencegah serangan pada jaringan dapat dilakukan dengan pemantauan terkait dengan *log* jaringan. Data *log* jaringan yang dipantau dapat digunakan untuk pencocokan pengguna jaringan internet. Pencocokan data pengguna jaringan internet dilakukan untuk mengetahui bahwa pengguna tidak disusupi penyerang. Pemantauan lalu lintas jaringan dapat menggunakan *Intrusion Detection System*

Namun *Intrusion Detection System* bergantung pada data yang dipantau dan bertentangan dengan kebutuhan privasi. Sehingga perlu adanya teknik untuk mengatasi masalah privasi pada *Intrusion Detection System*. Pada proses pencocokan dibutuhkan suatu algoritma *machine learning* yang kompatibel dengan data terenkripsi. Oleh karena itu diperlukan metode untuk melindungi pengambilan informasi pada data pengguna jaringan dan penggunaan algoritma *machine learning* pada data terenkripsi.

Penelitian yang dilakukan adalah pencocokan data pengguna jaringan internet dengan menggunakan algoritma *homomorphic encryption*. Model dapat mengatasi masalah privasi pada penggunaan *Intrusion Detection System* dan mengatasi keterbatasan *machine learning* dalam pencocokan data terenkripsi. Hasil prediksi dari model sama dengan hasil prediksi pada data *plaintext* yang mencapai akurasi 97,7%. Kesalahan prediksi mendekati nol yang menunjukkan bahwa hasil prediksi sesuai dengan data aktual. Perbedaan antara model dengan pengujian pada data *plaintext* terletak pada waktu proses prediksi. Dibandingkan dengan pengujian menggunakan data *plaintext*, model yang diusulkan dengan menggunakan *keysize* 256 dapat dianggap sebagai *tradeoff* menguntungkan antara konsumsi waktu dan masalah keamanan.

Kata Kunci: Intrusion Detection System, Homomorphic Encryption, Privacy-Preserving, Machine Learning.

ABSTRACT

INTERNET NETWORK USER DATA MATCHING USING HOMOMORPHIC ENCRYPTION ALGORITHM

by

YULIANA

19/448738/PPA/05821

Today's network technology is dealing with network security issues, cyber attacks and others. One of the issues of network security problems is intrusion, this activity is carried out to infiltrate the user's network secretly through the internet network. To detect and prevent attacks on the network can be done by monitoring related to network logs. Monitored network log data can be used for matching internet network users. Internet network user data matching is done to find out that the user is not infiltrated by an attacker. Network traffic monitoring can use the Intrusion Detection System

However the Intrusion Detection System relies on monitored data and goes against privacy requirements. So it is necessary to have a technique to overcome privacy problems in the Intrusion Detection System. The matching process requires a machine learning algorithm that is compatible with encrypted data. Therefore, a method is needed to protect the retrieval of information on network user data and the use of machine learning algorithms on encrypted data.

The research conducted is matching the data of internet network users using the homomorphic encryption algorithm. The model can overcome the privacy concerns of using the Intrusion Detection System and overcome the limitations of machine learning in matching encrypted data. The prediction results from the model are the same as the prediction results for plaintext data which reaches 97.7% accuracy. The prediction error is close to zero which indicates that the prediction result is in accordance with the actual data. The difference between the model and testing on plaintext data lies in the prediction process time. Compared to testing using plaintext data, the proposed model using keysize 256 can be considered as a favorable tradeoff between time consumption and security concerns.

Keywords: Intrusion Detection System, Homomorphic Encryption, Privacy-Preserving, Machine Learning