PENERAPAN PEMBELAJARAN MESIN DALAM UPAYA PENCEGAHAN KEJAHATAN SIBER

TUGAS AKHIR

Oleh:

Nabil Hudiya Rahman

2010933011

Pembimbing:

Ir. Insannul Kamil, M. Eng., Ph. D, IPU, ASEAN Eng., APEC Eng.

DEPARTEMEN TEKNIK INDUSTRI

FAKULTAS TEKNIK

UNIVERSITAS ANDALAS

PADANG

2025

PENERAPAN PEMBELAJARAN MESIN DALAM UPAYA PENCEGAHAN KEJAHATAN SIBER

TUGAS AKHIR

Sebagai Salah Satu Syarat untuk Menyelesaikan Program Sarjana pada Departemen Teknik Industri Universitas Andalas

Oleh:

Nabil Hudiya Rahman

2010933011

Pembimbing:

Ir. Insannul Kamil, M. Eng., Ph. D, IPU, ASEAN Eng., APEC Eng.

DEPARTEMEN TEKNIK INDUSTRI

FAKULTAS TEKNIK

UNIVERSITAS ANDALAS

PADANG

2025

ABSTRAK

Kejahatan siber seperti phishing dan spam telah menjadi ancaman signifikan di era digital, terutama dengan meningkatnya penggunaan internet di Indonesia. Ancaman ini tidak hanya berdampak pada kerugian finansial, tetapi juga pada keamanan data pribadi masyarakat. Penelitian ini bertujuan untuk merancang model machine learning yang mampu mengenali pola kejahatan siber dengan akurasi tinggi, guna mendukung upaya pencegahan kejahatan siber secara efektif.

Penelitian ini menggunakan berbagai algoritma machine learning, seperti LSTM yang diintegrasikan dengan K-fold Cross Validation untuk deteksi email phishing, email spam, dan spam pada platform Twitter. Selain itu, algoritma Random Forest dengan GridSearchCV digunakan untuk mendeteksi web phishing dan spam pada Facebook. Proses pengembangan model ini melibatkan pengolahan data besar dan tuning parameter untuk mendapatkan performa optimal.

Hasil penelitian menunjukkan bahwa model LSTM menghasilkan akurasi sebesar 99.70% untuk deteksi email phishing, 99.06% untuk email spam, dan 89.05% untuk spam pada Twitter. Sementara itu, algoritma Random Forest mencapai akurasi 94.18% pada deteksi web phishing dan 95.83% untuk spam pada Facebook. Penerapan teknologi ini tidak hanya meningkatkan keamanan digital tetapi juga memberikan manfaat bagi efisiensi energi dan keberlanjutan lingkungan. Dengan mengurangi serangan siber, kebutuhan mitigasi dan pemrosesan data tambahan dapat ditekan, sehingga mengurangi konsumsi daya server dan jejak karbon. Selain itu, keberhasilan dalam mencegah serangan web phishing pada infrastruktur kritis, seperti sektor energi, mencegah risiko gangguan besar seperti pemadaman listrik yang dapat berdampak pada aktivitas masyarakat dan ekonomi.

Kata Kunci: *Kejahatan Siber, LSTM, Machine Learning, Phishing, Random Forest, Spam*

ABSTRACT

Cybercrime such as phishing and spam has become a significant threat in the digital era, especially with the increasing use of the internet in Indonesia. This threat not only impacts financial losses, but also the security of people's personal data. This research aims to design a machine learning model that is able to recognize cybercrime patterns with high accuracy, in order to support effective cybercrime prevention efforts.

This research uses various machine learning algorithms, such as LSTM integrated with K-fold Cross Validation for the detection of phishing emails, spam emails and spam on the Twitter platform. In addition, the Random Forest algorithm with GridSearchCV is used to detect phishing and spam websites on Facebook. The process of developing this model involves processing large data and tuning parameters to obtain optimal performance.

The research results show that the LSTM model produces an accuracy of 99.70% for detecting phishing emails, 99.06% for spam emails, and 89.05% for spam on Twitter. Meanwhile, the Random Forest algorithm achieved 94.18% accuracy in detecting web phishing and 95.83% for spam on Facebook. The application of this technology not only improves digital security but also provides benefits for energy efficiency and environmental sustainability. By reducing cyber-attacks, the need for mitigation and additional data processing can be reduced, thereby reducing server power consumption and carbon footprint. Additionally, success in preventing web phishing attacks on critical infrastructure, such as the energy sector, prevents the risk of major disruptions such as power outages that could impact societal and economic activities.

Keyword: Cyber Crime, Machine Learning, LSTM, Phishing, Random Forest, Spam