ABSTRAK

Webshell yang diklasifikasikan sebagai *trojan scripting* menjadi ancaman serius terhadap integritas infrastruktur keamanan jaringan, untuk mengatasi keterbatasan *Web Application Firewall (WAF*) dalam mendeteksi *webshell* yang telah dikompresi dan disamarkan, pendekatan *artificial intelligence* khususnya melalui teknik *machine learning* dan *deep learning* digunakan untuk mendeteksi, mengenali pola perilaku serta fungsi *webshell*, metode *hybrid CNN-BiLSTM* yang digunakan pada *deep learning* sangat efektif dalam mengolah data teks sehingga dapat memahami struktur temporal model dan data sehingga menghasilkan nilai *precision 0.99*, *recall 0.99*, *f1-score 0.99* serta *accuracy 0.99* pada saat melakukan deteksi *file webshell* dan *non-webshell*, dan juga meminimalisir tingkat kesalahan pada nilai *false positives* dan mencegah *overfitting* pada model data dengan menggunakan fungsi *callback.*

Kata Kunci : *Webshell, Artificial Intelligence, Machine Learning, Deep Learning, CNN-BiLSTM*

ABSTRACT

Webshells, classified as scripting trojans, pose a serious threat to the integrity of network security infrastructure. To address the limitations of Web Application Firewalls (WAF) in detecting compressed and obfuscated webshells, an artificial intelligence approach, particularly through machine learning and deep learning techniques, is utilized. The hybrid CNN-BiLSTM method applied in deep learning proves highly effective in processing text data, enabling the understanding of the temporal structure of the model and data. This results in achieving a precision of 0.99, a recall of 0.99, an F1-score of 0.99, and an accuracy of 0.99 in detecting webshell and non-webshell files. It also minimizes the error rate in false positives and prevents overfitting in the data model by using callback functions.

Keywords: Webshell, Artificial Intelligence, Machine Learning, Deep Learning, CNN-BiLSTM.