ABSTRACT

Signature-based botnet detection struggles to detect new threats or undocumented botnet variants. This detection method often suffers from a high false positive rate. This type of detection is less reliable in a network environment due to its reliance on known patterns. This study used a deep learning-based approach by integrating Variational Autoencoder (VAE) and Transformer to detect botnets in computer networks using the CTU-13 dataset. VAE enables learning of probabilistic latent representations of network traffic, while Transformer, with its self-attention mechanism, improves the model's ability to capture long-range dependencies in complex network data. Experimental results show that the VAE-Transformer model has an accuracy of 88.98% for botnet detection and a false positive rate of 1,560. Parameter optimization results for batch size usage show that using a batch size of 32 is better with an accuracy of 88.98%.

.

.

Keywords: *Botnet, Variational Autoencoder-Transformer (VAE-Transformer), Anomaly Detection, Deep Learning, Computer Network, False Positive.*