This study delves into the realm of anomaly detection, aiming to unlock the capabilities of autoencoders and variational autoencoders (VAEs).

We employed two distinct datasets: the UNSW-NB15 dataset (700,001 cases, 49 features, 6 categorical features) and the NSL-KDD dataset (125,973 cases, 43 features, 5 categorical features) to comprehensively validate our approach.

We meticulously removed duplicate rows and entries with missing data, ensuring the integrity of our dataset.

Categorical variables underwent either label encoding or frequency encoding based on the count of their distinct values. Those with fewer than 50 unique values were subjected to label encoding, while those with 50 or more unique values underwent frequency encoding. After this, all features were scaled using min-max scaling.

Our study involves a comparative analysis of autoencoders and variational autoencoders against the benchmark K-Nearest Neighbors technique. This rigorous evaluation provides a comprehensive understanding of their respective anomaly detection capabilities.

Autoencoders: Strong performance on both datasets, detecting over 80%

of anomalies.

Variational Autoencoders (VAEs): Slightly less effective than autoencoders, excelling in recall but with occasional misclassification (lower F1 score).

K-Nearest Neighbours (KNN): Varies by dataset, underperforms on UNSW-NB15 but outperforms others on KDD. Notably, varied recall suggests generalization challenges across distributions.tasets, indicating a challenge in generalisation across different data distributions.

Acknowledging the intrinsic complexity of autoencoders and variational autoencoders, we incorporated LIME and SHAP techniques. These methods shine a light on these models' often opaque decision-making processes, revealing valuable insights into their anomaly identification mechanisms.

Notably, source/destination IP addresses and port numbers emerged as pivotal factors, revealing vulnerable targets of cyber attacks and potential attackers.

In the context of growing cyber threats, anomaly detection becomes crucial for identifying and mitigating potential attacks.

The findings highlight the effectiveness of Autoencoders and Variational Autoencoders for anomaly detection.

Potential avenues for future research could encompass the utilization of Graph Neural Networks, focusing on anomaly detection through the identification of nodes displaying atypical connectivity patterns within graph-structured data.