**2. Review of Existing Research**

**2.1 Machine Learning and Optimization for Intrusion Detection**  
Aziz & Alfoudi (2023) presented a summary of various ML models and optimization methods in IDS. The research mentions supervised and unsupervised learning techniques, with a focus on feature selection and hyperparameter optimization for enhanced detection rates. Their discussion focuses on hybrid models that integrate conventional ML with optimization methods for better performance.

**2.2 TF-IDF and Singular Value Decomposition for HIDS**  
Subba & Gupta (2021) introduced a feature extraction framework based on Term Frequency-Inverse Document Frequency (TF-IDF) and Singular Value Decomposition (SVD) for HIDS. Their method effectively performs dimensionality reduction while preserving essential information, resulting in enhanced anomaly detection. The framework is tested on real system process data, showing dramatic improvements in detecting malicious activities.

**2.3 Context-Aware Feature Extraction in CNN-Based IDS**

Shams et al. (2021) presented a new context-aware feature extraction approach for Convolutional Neural Network (CNN)-based Intrusion Detection System (IDS). The proposed approach enriches system behavior representation with the addition of contextual information. It is evident from the research that CNNs with enriched feature extraction are superior to conventional ML techniques and yield more accurate results in identifying complex intrusion patterns.

**2.4 Stacking Ensemble-Based HIDS Using Word Embeddings**  
Kumar & Subba (2023) discussed a stacking ensemble approach for Windows-based HIDS using multiple word embeddings to identify abnormal processes. The research combines multiple deep learning methods to improve feature representation, which results in more accurate identification of malicious activities. The research shows the superiority of stacking ensembles in enhancing classification accuracy.

**2.5 Stacking Ensemble Models on ADFA Dataset**  
Satilmiş et al. (2025) constructed several stacking ensemble models that are trained on the ADFA dataset, a standard dataset for HIDS research. The research compares different ML algorithms put together in an ensemble framework, showing enhanced detection performance compared to individual models. Their work confirms the significance of ensemble learning in intrusion detection