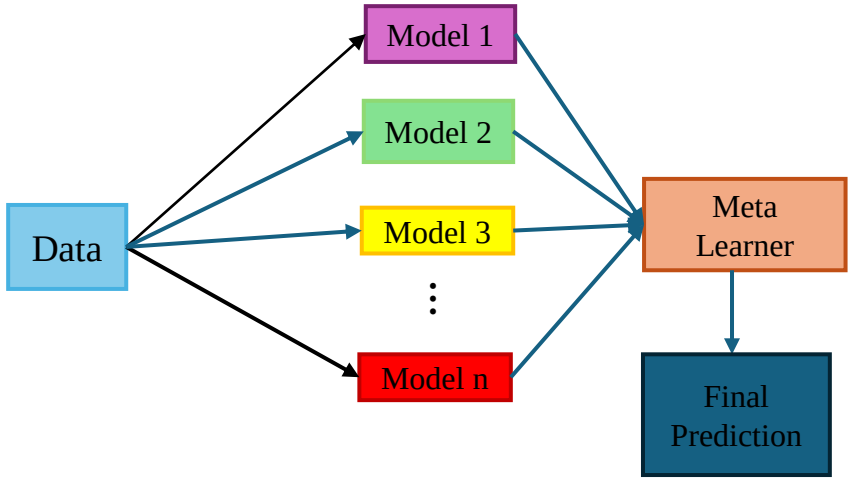
NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

Strengthening Cybersecurity in CPS with Ensemble Learning Techniques

Background

- Ensemble learning involves combining multiple machine learning (ML) models to improve the prediction and detection of complex patterns.
- Enhanced security measures in Water Distribution Systems (WDS) lead to quicker detection and response.

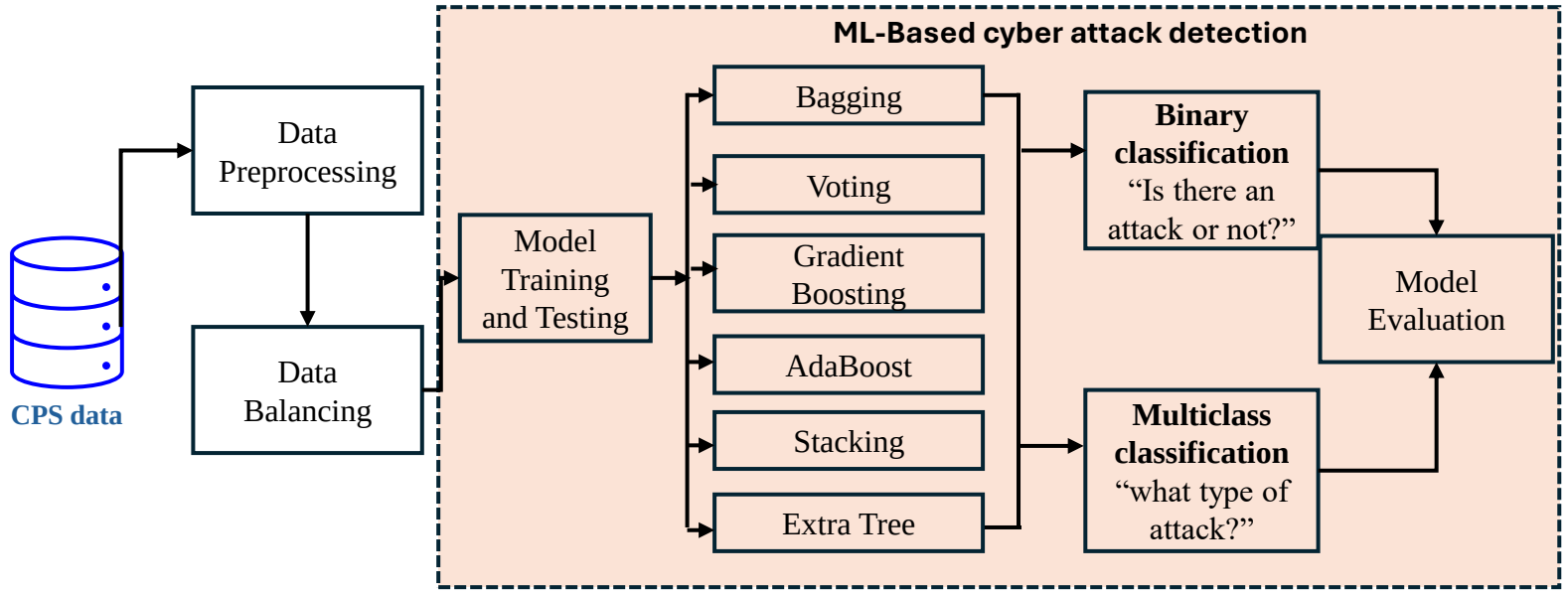


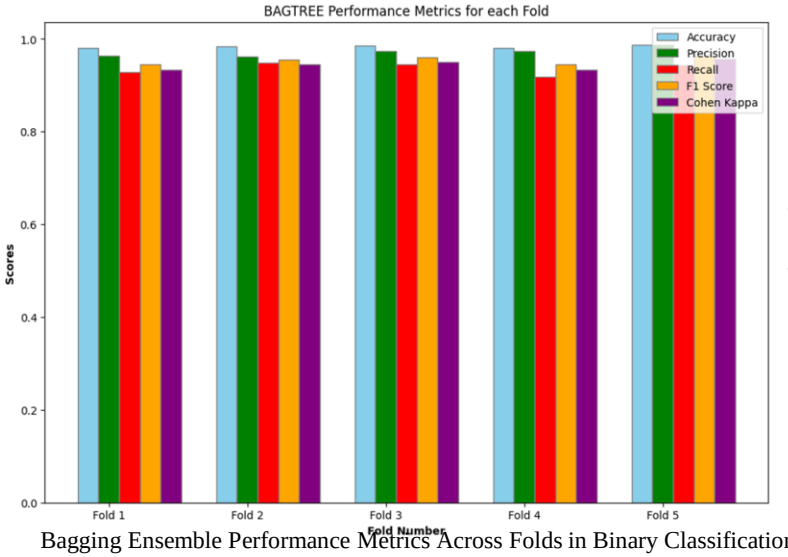
The process of stacking ensemble

Objectives

- To implement ensemble learning methods to detect and mitigate cyber attacks in CPS environments.
- To enhance detection accuracy by leveraging the collective strengths of multiple predictive models.
- To identify effective ensemble methods for WDS CPS cyber attack detection.
- To explore a comparative analysis of ensemble learning methods applied to binary and multiclass classification models in WDS.

Methodology: Water Distribution System CPS Application





Bagging Ensemble Performance Metrics Across Folds in Binary Classification.

Performance of Ensemble Models in Binary and Multiclass Classification.