ABSTRACT

PLN, the national electricity provider of Indonesia, continues to face persistent challenges from electricity theft, resulting in significant financial losses and operational inefficiencies. Traditional detection approaches, such as manual inspections, have demonstrated low effectiveness, with reported hit rates around 4.16%. Previous research introduced Bidirectional Long Short-Term Memory (Bi-LSTM) models enhanced with L2 regularization and class weighting, which improved detection capability to a hit rate of 6.42% by leveraging temporal patterns in consumption behavior. Expanding on this foundation, the present study proposes a hybrid deep learning architecture that combines Bi-LSTM with Convolutional Neural Networks (CNN) to capture both sequential dependencies and localized usage anomalies. This integrated approach significantly improves performance on highly imbalanced datasets, achieving a hit rate of 25.26% representing a substantial improvement over prior methods. By incorporating temporal and spatial learning components, the model demonstrates increased robustness, scalability, and precision in identifying fraudulent activities within electricity usage data. While this study focuses on postpaid electricity consumption data, characterized by fixed monthly billing cycles, future research should explore more complex and dynamic datasets, such as those from Advanced Metering Infrastructure (AMI) and prepaid customer systems. Unlike postpaid data, prepaid consumption is based on tentative, irregular purchasing behavior, which introduces additional variability and requires more sophisticated temporal modeling techniques. Integrating data from AMI, which offers high-resolution, real-time measurements, could further improve the model's ability to detect subtle anomalies and short-duration fraud patterns. Addressing the unique characteristics of these data types will enhance the generalizability and practical deployment of AI-driven fraud detection models across PLN's broader customer base.

Keywords—Computational intelligence system, Fraud Detection, Artificial Intelligence, Consumption Patterns, Nontechnical loss, pattern classification.