Introduction

The darknet represents a concealed segment of the internet that facilitates anonymous communication through sophisticated encryption and routing protocols, creating substantial challenges for traffic classification in cybersecurity applications[1]. Traditional network traffic analysis methods, particularly deep packet inspection (DPI), prove ineffective against encrypted darknet communications, while centralized data collection approaches raise significant privacy concerns and scalability limitations[2]. Furthermore, the inherent scarcity of properly labeled datasets in darknet environments, combined with severe class imbalance issues where minority classes like Tor traffic represent less than 1% of total traffic, compounds these analytical challenges.

Recent advancements in federated learning have demonstrated promising solutions for privacy-preserving distributed machine learning[3, 4, 5]. However, the application of federated semi-supervised learning specifically to darknet traffic classification remains largely unexplored, representing a critical research gap that this study addresses. The integration of federated learning's distributed privacy-preserving optimization with semi-supervised learning's capacity to effectively utilize both labeled and unlabeled data presents a novel approach to overcome the fundamental limitations of traditional centralized methods[6, 7].

This study proposes a comprehensive federated semi-supervised learning framework for analyzing darknet traffic patterns while maintaining strict privacy preservation requirements. The research approach integrates federated learning's distributed architecture with semi-supervised learning techniques, specifically pseudo-labeling strategies, to address the unique challenges posed by darknet environments including non-independent and identically distributed (non-IID) data distributions and severely limited labeled datasets.

The primary contributions of this work include: (1) development of a novel FSSL framework specifically tailored for darknet traffic classification that addresses privacy, scalability, and data scarcity challenges simultaneously; (2) comprehensive experimental validation using multiple federation scales with detailed justification for experimental design choices; (3) comparative analysis of four distinct federated aggregation strategies under semi-supervised learning conditions; and (4) demonstration of significant performance improvements through strategic pseudo-labeling while maintaining data privacy across distributed environments.

This framework demonstrates potential for enhancing malicious darknet activity detection capabilities while advancing cybersecurity through privacy-preserving approaches. The methodology's applicability extends to other privacy-sensitive domains including IoT networks, healthcare data analysis, and financial fraud detection[8]. Subsequent sections provide comprehensive literature review, detailed methodology description, extensive experimental results, and thorough discussion of implications and future research directions.