



Federated Learning for Privacy-Preserving Cyberbullying Detection: A Comprehensive Review of Challenges, Technologies, and Privacy Considerations in Child Protection

Don Simon Patabadi Shashitha Udesch De Silva¹, Ranaweerage Sithumi Bhagya²,
Thulani Thanuvinie Magedara³

*Department of statics and computer science
Faculty of Science, University of Kelaniya
Dalugama, Sri Lanka*

Abstract

The threat of cyberbullying is also emerging as an issue more serve than bullying and psychologies harassment, as it alters the child's welfare in distinct ways. Centralized detection mechanisms also fail due to privacy violating, on-scalability, and data silos that are heterogeneous data problematic. Federated Leaning(FL) can be a potential solution as it allows for collaborative model training across distributed devices without exposing sensitive user data. The significant contribution of this review is the discussion of how federated learning in all the cyberbullying detection system for children can be combined smoothly. We contract the current best models such as deep Convolution Neural Networks(CNN), Recurrent Neural Networks(RNN) long short term memory and other transformer-based models such as BERT. This survey also comes with various privacy-protecting secure methods such as aggregation, differential privacy, and blockchain that may be used to aid federated learning in its ability to process otherwise non-IID data from multiple heterogeneous sources. The obtained results show that FL based solution allow for attaining detection accuracies from around 74% up to more than 90% with competitive quality and under user privacy preservation. Hybrid architectures and transformer based state of the art models achieve considerable gain over baseline with computation communication overhead tradeoff. Addressing current technical limitations through continued research on hybrid deep learning approaches and enhanced security protocols will be crucial to move these innovations towards real world applications that ensure online environment online environments are safer for vulnerable populations.

Keywords: Blockchain; Convolution Neural Network; Deep Learning; Long-short term memory; Recurrent Neural Network