Chapter 9
Privacy-Preserving AI Framework for Child Suspicious Activity Recognition With Parental Control and Digital Protection

Vinod Mahor
https://orcid.org/0000-0002-2187-6920
Maulana Azad National Institute of Technology, India

Jaytrilok Choudhary
Maulana Azad National Institute of Technology, India

Dhirendra Pratap Singh
Maulana Azad National Institute of Technology, India

ABSTRACT

Ensuring child safety in more and more linked digital contexts provides a double difficulty: properly monitoring questionable behavior while maintaining user privacy and allowing adaptive parental control. Facilitating real-time identification of abnormalities in children's digital activities, the framework uses a hybrid CNN-BiLSTM model to precisely capture both spatial and temporal behavioral patterns. hence addressing important privacy issues., hence delivering real-time notifications and risk evaluations customised to the environment and intensity of the identified actions. Achieving 95% accuracy and good precision, recall, and F1-score, exper-

DOI: 10.4018/979-8-3373-2716-7.ch009

imental tests using the Kinetics-700 dataset confirm the efficacy of the suggested model. With improved computational efficiency appropriate for real-time applications, the model shows better performance than traditional methods. The inclusion of privacy-preserving technologies does not noticeably affect performance, hence stressing the framework's appropriateness for use in actual digital platforms.

1. INTRODUCTION

The proliferation of digital technologies and ubiquitous internet access has fundamentally transformed the lives of children, reshaping how they communicate, learn, and entertain themselves. (Kanda et al., 2009) With the increasing reliance on smart devices, online education platforms, social media, and interactive digital content, children are spending a significant portion of their time online. While these advancements offer numerous educational and developmental benefits, they have also introduced unprecedented risks, (Sul-Ain et al., 2024) including exposure to inappropriate content, online predators, cyberbullying, and other forms of digital abuse. In this evolving landscape, the safety and well-being of children have become a critical area of concern for parents, educators, and policymakers alike.

(Al-Rammah et al., 2022) Artificial Intelligence (AI) has emerged as a powerful enabler of intelligent monitoring systems that can identify abnormal or suspicious behavior in real time. Leveraging advancements in computer vision, natural language processing, and behavioral analytics, AI-based solutions can detect and respond to potential threats much faster than traditional rule-based systems. (Yang et al., 2025) These capabilities have led to the integration of AI into surveillance systems, content filtering tools, and parental control applications. However, the deployment of AI in child activity monitoring raises significant privacy concerns. The collection and processing of sensitive personal data, including video footage, audio streams, chat logs, and biometric information, pose a substantial risk to the child's privacy and can lead to misuse if not handled responsibly, and Classification of frames from dataset are shown in Fig.1.