Chapter 17
A Federated AI–IoT–Cloud Framework for Enforcing Child Protection Laws Against Digital Crimes in the Modern Cyber Ecosystem

Hitesh Rawat
https://orcid.org/0009-0006-7171-6016
University of Extremadura, Spain

Chandrapal Singh Dangi
Manipal University Jaipur, India

Manoj Dhawan
https://orcid.org/0000-0003-0622-741X
Avantika University, Ujjain, India

Vishwas Dixit
Shri Vaishnav Vidyapeeth Vishwavidyalaya, India

Anjali Rawat
https://orcid.org/0009-0006-7171-6016
University of Extremadura, Spain

ABSTRACT

Amid rising cyber threats targeting minors via smart devices and digital platforms,

DOI: 10.4018/979-8-3373-5132-2.ch017

this study introduces an AI-driven framework to support child protection laws in digital spaces. Using the CSCSD-2024 dataset—containing 2.4 million labeled cases across 15 regions—we analyzed threats such as grooming, cyberbullying, and illicit exposure. The data spans IoT devices (32.7%), social platforms (48.5%), and cloud-based tools (18.8%). A layered AI system integrates CNNs for content analysis, BiLSTM for behavior tracking, and Federated Learning to ensure privacy. Deployed across AWS, Google Cloud, and Azure, it operates in real time with 93 ms latency and 0.78 s inference time. Testing across 4,000 IoT nodes yielded 96.4% precision, 94.9% recall, and 95.6% F1-score, surpassing rule-based models. ROC-AUC and PR-AUC scored 0.982 and 0.955. Legal modules mapped threats to COPPA, GDPR-K, India's IT Act, and Australia's eSafety law with 92.7% accuracy, offering a scalable, cloud-native standard for child safety enforcement.

INTRODUCTION

The digitalization (Nag et al., 2024) of everyday life, accelerated by the widespread adoption of smart devices and interconnected platforms, has led to an alarming surge in cyber threats targeting children. According to a 2024 report by UNICEF (Nag et al., 2024), more than 65% of children aged 8–16 are regularly exposed to online environments, increasing their vulnerability to crimes (Rawat et al., 2025a) (Rajavat et al., 2024) (Rawat and Rajavat, 2024a) such as cyberbullying (Mishra et al., 2024), online grooming (Rawat and Rajavat, 2024b), exposure to illicit content, and digital exploitation. The World Health Organization also reported that nearly 1 in 5 minors globally has experienced some form of online abuse (Bhardwaj et al., 2024) (Dhawan et al., 2025), often originating from unmonitored IoT devices (Srinivasan et al., 2020) or unregulated digital applications.

Despite legislative frameworks (Srinivasan et al., 2020) like COPPA (Children's Online Privacy Protection Act), GDPR-K, and regional acts such as India's IT Act Section 67B and Australia's eSafety Act, the real-time enforcement of these laws remains limited due to a lack of integrated technical infrastructures. Traditional rule-based (Chirgaiya and Rajavat, 2023) systems have demonstrated limited adaptability in detecting evolving threat vectors, typically achieving F1-scores between 71–75%, insufficient for high-risk environments involving children.

To address this gap, the current study proposes a federated AI-IoT-cloud framework (Prathyanga et al., 2024) that leverages modern machine learning algorithms (Prathyanga et al., 2024), edge intelligence, and multi-cloud (Mascari et al., 2025) infrastructures to operationalize child protection laws dynamically. Utilizing the CloudSec-ChildSafe Dataset (Nag et al., 2024) (Srinivasan et al., 2020) (Prathyanga et al., 2024) (Rahman et al., 2024)