Chapter 15
Cybersecurity and Digital Consent: Ensuring Child Safety Through Secure Parental Authorization Systems

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

Priya Matta
Tula's Institute, Dehradun, India

Anand Rajavat
Shri Vaishnav Vidyapeeth Vishwavidyalaya, India

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

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

ABSTRACT

With the growing use of digital platforms, the need for secure parental authorization systems to protect children online has become crucial. This study presents a new framework aimed at enhancing cybersecurity and digital consent for child users. Using the Parental Consent Dataset (PCD), which includes 50,000 anonymized

DOI: 10.4018/979-8-3373-2716-7.ch015

records of user interactions and approvals, the research applies the Authorization System Analysis Method (ASAM) to evaluate the security and effectiveness of parental controls. Key techniques include encryption, behavior monitoring, and real-time consent verification to prevent unauthorized access. Results show a 35% decrease in security risks and an average response time of 0.75 seconds per request. Additionally, the system boosted parental monitoring capabilities by 40%, offering instant updates on children's digital activity. This work emphasizes the importance of secure consent systems in creating safer online spaces for minors.

1. INTRODUCTION

In the rapidly evolving digital landscape (Gupta et al., 2023), ensuring child safety online has become a paramount concern. With children increasingly engaging in online activities, ranging from social media to gaming platforms, there is an urgent need to develop robust parental (Waseem and Koul, 2022) authorization systems that provide secure and real-time monitoring. Digital consent has emerged as a key element in securing these interactions, but the effectiveness of existing systems remains questionable due to gaps in security protocols, user consent management, and unauthorized access prevention (Dick, 2024).

Recent advancements in cybersecurity tools (Chirgaiya and Rajavat,2023), such as blockchain-based consent frameworks and AI-powered parental control systems, have shown promising results in addressing these challenges (Mishra et al., 2024) (Pithawa et al., 2023). The integration of biometric authentication, multi-factor authentication (MFA), and machine learning algorithms (Bhardwaj et al., 2024) has significantly improved the security of authorization systems, enabling more reliable parental oversight of children's online activities.

This study employs the Consent Validation Toolkit (CVT), an advanced tool used to analyze and track consent processes in real-time across multiple platforms. The tool utilizes natural language processing (NLP) (Dhawan et al.,2025) for detecting consent-related discrepancies and encryption algorithms for secure data transmission. We also incorporate a data breach detection framework using AI-driven anomaly detection (Mascari et al.,2025), which can flag potential vulnerabilities (Rawat and Rajavat,2024) and unauthorized access attempts (Nahar et al.,2023).

Our approach involves a comprehensive evaluation of over 60,000 user interactions from the Child Safety Online Dataset (CSOD) (Laranjeira da Silva et al., 2022) (Wang et al.,2024), consisting of anonymized consent approvals, parental consent rejections, and system access attempts. Preliminary findings reveal a 25% reduction in unauthorized access attempts when using the proposed parental authorization model (Rawat et al., 2025), compared to traditional systems, which have an average