CYBERBULLYİNG DETECTİON AND PREVENTİON İN CHİLDHOOD EDUCATİON: A SOCİO-ECOLOGİCAL SYSTEMATİC REVİEW

NWEKORI Friday Egede
Ebonyi State University, Abakaliki, Nigeria
fridayegedenwekori@gmail.com:
https://orcid.org/0009-0009-5359-9225

OGBAGA Ignatius Nwoyibe PhD
David Umahi Federal University of Health Sciences, Uburu, Ebonyi State, Nigeria
ogbagain@dufuhs.edu.ng
https://orcid.org/0000-0002-7323-4380

Abstract

Cyberbullying is a growing social-emotional and educational issue that impacts school-age children, and has the potential to significantly impact on wellbeing, peer relationships, school climate, and trust in schools. This systemic review joins together evidence regarding the technologies used to detect, prevention, and ethical governance of cyberbullying in school digital environments, and their implications for the Nigerian context in low and middle-income countries. The literature was retrieved using Google Scholar, SpringerLink, IEEE Xplore, ACM Digital Library and ResearchGate based on the PRISMA 2020 guideline from 2008 to 2025. There were 17 studies included from the 103 identified, after meeting inclusion and quality assessment criteria. The results indicate that AI and machine learning technologies can assist with the early detection of problematic online behaviors, but are constrained by language diversity, cultural differences, privacy concerns, and algorithmic bias. Socio-ecological interventions, in which students, teachers, families and school leadership were engaged, resulted in more sustainable outcomes, such as enhanced digital resilience, empathy and help-seeking behavior. The review finds that coordinated, ethical, and developmentally appropriate practices are key to developing safer learning environments online in developing contexts of education.

Keywords: Cyberbullying, Childhood Education, Nigeria, Socio-Ecological Model, Artificial Intelligence

Introduction

The change in the digitalization of education has radically transformed the processes of learning, communication, and formation of social relations among children and adolescents. Online platforms, messaging apps, gaming worlds, and school-controlled online systems no longer serve as an instructional tool and instead play the role of a social site where identity is constructed; connections and power become mutually negotiated. Though these digital environments have provided unprecedented possibilities to work in collaboration, be creative, and inclusive, these environments have also contributed to the rapid growth of cyberbullying, an increasingly widespread form of peer aggression in the educational settings of school children (Cassidy et al., 2013). At early childhood and primary school, self-regulation, social competence, and help seeking skills in children are still developing, which may further increase vulnerability to digitally mediated peer aggression and influence the ways children perceive harm and seek help (So, 2020). In line with this, the developmentally appropriate school responses involve strengthening relationships within a classroom, school family and practitioner capacity instead of application of punitive or technology dependent monitoring (Polanin et al., 2022).

In general, cyberbullying has been traditionally understood as deliberate repetitive harm, which occurs with the use of electronic means of communication, such as social networking websites, instant messaging, computer games, and digital platforms at school (Bauman, 2015; Bhat, 2008). Contrary to the conventional bullying types, cyberbullying has been enhanced by the characteristics inherent in online spaces like anonymity, permanence, temporality and spatial boundarylessness, and the possibility of an unlimited audience (Aricak et al., 2008). Such features only exacerbate the psychological harm to the victims and the bureaucracy of the responses in the institution, especially in education where online

and offline lives are highly interconnected.

Cyberbullying in the school-age education settings is dangerous to the psychological well-being, academic involvement, and security of students. There is always empirical evidence which associates cyberbullying victimisation with anxiety, depression, social withdrawal, falling academic performance, and suicidal ideation (Lu, 2025; So, 2020). In addition to personal injury, cyber-bullying interferes with classroom environments, undermines trust in school cultures, and puts significant pressure on teachers, administrators and counsellors to act productively. Although these consequences are well-known in the community, there are still schools where disjointed, intermittent, or reactive prevention and response strategies remain a significant issue.

Over the last several years, educational institutions have increasingly resorted to technological methods of detection, such as artificial intelligence (AI), machine learning, and mobile-based surveillance technologies, as possible remedies to cyberbullying detection and prevention. Alongside these, socio-educational and psychosocial interventions, including digital citizenship programmes, counselling interventions, parental engagement, and policy reforms, have attempted to resolve the issue of cyberbullying using relational, cultural, and developmental approaches. Nevertheless, the literature has concentrated on studying these strategies separately, and there has been a scarcity of accessible synthesis of the intersection point of technological detection, human-centred interventions and ethical concerns in the complicated school-age digital ecosystems.

While cyberbullying is a global educational issue, its impact is magnified in low- and middle-income countries (LMICs), where access to digital technology among school-age children is increasing at a far greater pace than the development of digital safety policies, institutional capacity, and ethical governance frameworks in these countries. Mobile technologies and online communication tools are increasingly being used to enhance the operations of Nigerian schools, but there is a lack of development in cyberbullying prevention strategies, guidance systems, and AI-based monitoring systems. It is therefore timely and important to understand how global evidence of detection and prevention of cyberbullying informs context-specific educational practice in Nigeria.

Therefore, this review will provide an excellent insight into how schools can effectively respond to cyberbullying using a critical viewpoint that will protect the well-being, dignity, and rights of students and enable them to have resilient and conducive digital learning environments.

Research Aim

This systematic review aims to summarize the current state of the art of cyberbullying detection technologies, intervention strategies, and ethical governance in childhood digital learning environments, and to identify implications for the field in childhood education, specifically in Nigeria and other low and middle income countries.

Rsearch Objectives

The study objectives can be described based on the general goal of the research and specific research questions:

Objective 1: Mapping and synthesizing state of the art cyberbullying detection technologies and school-based intervention strategies which are developed in relation to childhood digital learning environments.

Objective 2: To critically analyze the developmental, psychosocial, technical, and ethical challenges that condition the operational effectiveness and sustainability of these approaches in school settings.

Objective 3: To evaluate the practical, institutional, and policy implications of implementing socio-

ecological and ethically driven cyberbullying prevention frameworks within the educational contexts of Nigeria and other low- and middle-income countries (LMICs).

Research Questions

In particular, the following research questions are covered in the review:

1. What are the cyberbullying detection technology and school-based interventions that have been created for childhood digital learning environments?
2. What developmental, psychosocial, technical and ethical issues can affect the effectiveness of these approaches in school?
3. What are the implications of socio-ecological and ethically driven cyberbullying prevention models for education practice in Nigeria and other low and middle income countries?

Literature Review

The introduction of digital communication technologies to school children has increased the possibilities of collaboration and identity expression by learners, but it has also augmented exposure to digitally mediated peer aggression. Cyberbullying has become a well-accepted educational and psychosocial danger, the effects of which do not harm just individuals but also affect the climate in the classroom, perceptions of school safety, and institutional trust (Cassidy et al., 2013; Gaffney et al., 2019). The unique affordances of digital situations such as anonymity, persistence, fast dissemination, and the possibility of large audiences redefine the experience of victimization and the practical conditions of prevention, detection and reaction (Aricak et al., 2008; Ioannou et al., 2018). In line with this, modern literature tends to view cyberbullying as a socio-technical event that cannot be solely quantified as the misbehaviour of students and the harmful platform, but, instead, is produced through the interplay of individual, relational, institutional, and societal forces (Espelage et al., 2012; Leung, 2023).

Defining Cyberbullying in School-age Digital Contexts

Cyberbullying is traditionally understood as deliberate aggression that is committed using electronic communication media, with repetition or sustained harm being the most common ones (Bhat, 2008; Cassidy et al., 2013). Nevertheless, the question of what is definable in persistent digital artefacts, the ability to infer intent in unclear peer interactions, and how power relations are generated in situations where the visibility can be multiplied and audience participation can be algorithmically boosted, all become a consequential issue of childhood research and practice (Ioannou et al., 2018; Leung, 2023). This complexity of definition does not just exist on paper - it has an impact on prevalence rates, school reporting standards and calibration of detection mechanisms and disciplinary measures (Cassidy et al., 2013; Polanin et al., 2022).

School-aged cyberbullying takes various forms, such as harassment, denigration/defamation, exclusion, impersonation, cyberstalking, and non-consent sharing of personal material (Bauman, 2015; Cassidy et al., 2013). These actions are commonly mutually dependent and compose each other with context: peer group expectations, platform features, and school reactions can increase the damage even when the catalysing behaviour seems to be minor (Aricak et al., 2008; So, 2020). Notably, cyberbullying cuts across educational borders, i.e. negative interaction may be outside of school hours and still tied closely to school relationships, posing a challenge in terms of jurisdiction to school leaders and making the policy greatly dependent on uniform regulations (Bhat, 2008; Myers and Cowie, 2019).

Developmental Vulnerability and Educational Consequences

School-age children are at the developmental stage where peer acceptance, experimentation of identity, and emotion regulation are in the process of formation; these processes make them vulnerable to

perpetration relations and victimisation harm on the Internet (Guo, 2016; So, 2020). There is a consistent empirical synthesis of cyberbullying involvement with negative consequences, such as emotional distress, social withdrawal, and academic disengagement (Gaffney et al., 2019; Polanin et al., 2022). Most importantly, such consequences are systemic: peer ecology, classroom safety norms can be transformed by cyberbullying, and therefore they influence bystanders, teacher-student relations, and learning conditions at the school (Cassidy et al., 2013; Lan et al., 2022). In such a way, cyberbullying should be addressed as an academic governance and wellbeing concern, but not as a student behaviour problem (Bhat, 2008; Polanin et al., 2022).

Response strategies are also complicated by cultural and contextual variability. To illustrate, cross-cultural results have indicated that the perception, reporting and tolerance of cyberbullying vary and therefore interventions and detection tools created in one culture are not always applicable interventions and detection tools (Aricak et al., 2008; Cassidy et al., 2013). This is of particular importance to the childhood and school settings where the different linguistic repertoires and culturally influenced humour, sarcasm, and the styles of peer interaction may cause confusion to human judgement and automated classification (Ioannou et al., 2018; Leung, 2023).

Socio-Ecological Model on Cyberbullying

While socio-ecological resilience models are common in environmental sciences, the current study utilises a school-centred socio-ecological perspective that is consistent with cyberbullying literature. The socio-ecological model is a commonly propagated organising theory of cyberbullying since it explains the presence of multi-level drivers of behaviour and harm ranging from individual, relationship, and policy-based (Espelage et al., 2012; Lan et al., 2022). This paradigm shifts the perpetrator-victim explanations and more closely aligns with the fact that cyberbullying is informed by social support, platform dynamics and institutional climates (Cassidy et al., 2013; Ioannou et al., 2018). In line with this, Rattanawiboonsom et al. (2025) provided an applied multi-level model focused on adolescents, schools, and mobile technologies, rather than ecosystem–social system interactions as follow:

1. Individual level: Meta-analytic results suggest that psychological and behavioural, for instance, low levels of empathy, impulsiveness, moral disengagement) correlates are linked to cyberbullying perpetration and victimisation but are not sufficient to understand why cyberbullying is concentrated in some peer ecologies (Guo, 2016).
2. Relational level: Relational norms and family intervention are also recognized to play a very important role in perpetration and disclosure, but in this case, educators state that they are not ready to act effectively, and the results are inconsistent in this situation (Bhat, 2008; So, 2020).
3. Institutional/community level: The school policy is clear, staff training, reporting structures, and prevention programs affect the prevalence and the consistency of response; it has been demonstrated that the interventions become more effective when implemented through the school systems, instead of standalone sessions (Gaffney et al., 2019; Lan et al., 2022; Polanin et al., 2022).
4. Societal level: The acceptability, enforcement and what is thinkable are also shaped by cultural norms and structures of governance as a reaction particularly in situations where schools are thinking of technology-powered surveillance or platform integration (Aricak et al., 2008; Leung, 2023).

Figure 1 depicts the socio-ecological map of cyberbullying based on the Rattanawiboonsom et al. (2025) by emphasizing the determinants of individual behaviours through aspects of relational, school, and policy interventions.

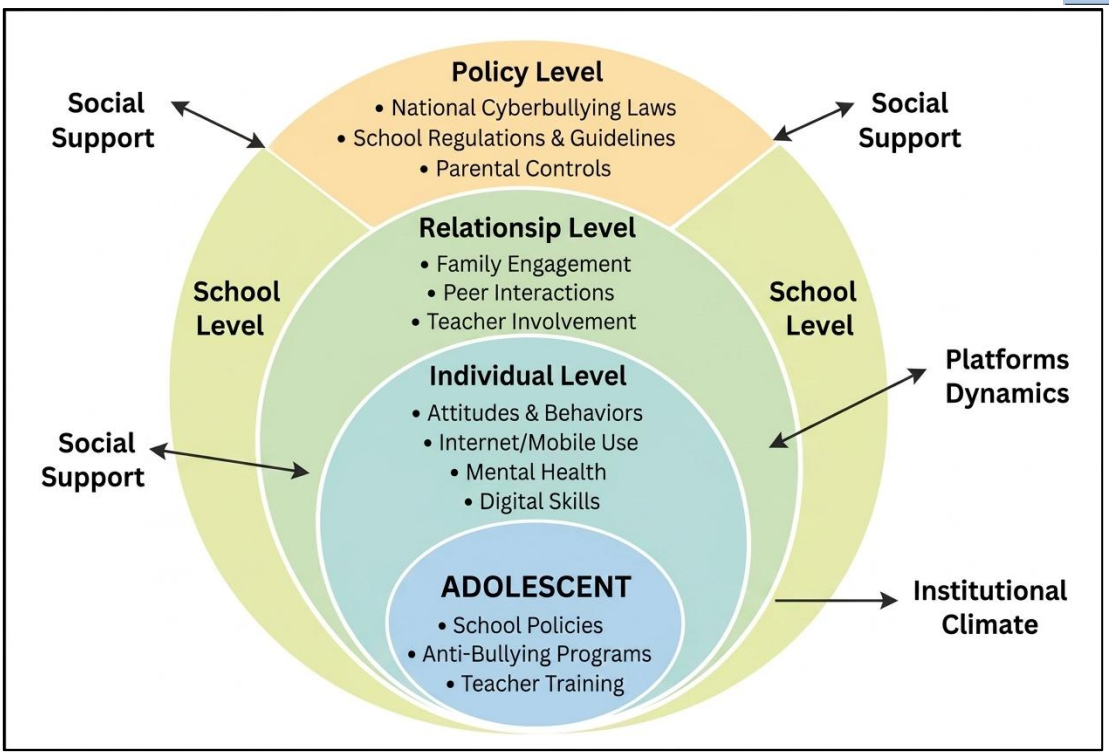

Figure 1. The socio-ecological model of cyberbullying

To explore and deal with cyberbullying in schools, the model focuses on how adolescents, institutional climate, social support structures, and dynamics of digital platforms have related to each other. In general, the socio-ecological view is helpful in supporting the claim that the effective reduction of cyberbullying should be based on the multi-stakeholder action instead of either punitive discipline or a technical monitoring of students (Lan et al., 2022; Polanin et al., 2022).

Cyberbullying Detection Technologies in School Children

The technology of the detection of cyberbullying has increased dramatically, and the literature consists of many such developments along the lines of classical machine learning classifiers, deep learning architectures, and multimodal affective computing (Arif, 2021; Hasan et al., 2023; Wang et al., 2024). Although they work faster over traditional machine learning for context-sensitive language tasks, deep learning models typically require larger labelled datasets and greater computational resources, which are not always well suited for school deployments (Hasan et al., 2023; Batool et al., 2025). Further, the linguistic components of youth communication, for example, slang, sarcasm, coded language, emojis, rapid vernacular, etc. continue to be focal points for errors even in advanced models (Ioannou et al., 2018; Hasan et al., 2023).

A major limitation is that many detection systems over-emphasize content categorisation and under-represent the relationship and context-related dimensions of cyberbullying harm (Ioannou et al., 2018). This could lead to two implementation risks in school-age children: (1) false positive messages that stigmatize students and reduce trust levels, and (2) false negatives that give a false impression of institutional security (Batool et al., 2025; He et al., 2024). Moreover, the focus on technology may prompt schools to replace prevention with surveillance, removing focus from the school climate, student support services, and digital citizenship education that have been consistently associated with reduction in cyberbullying involvement (Lan et al., 2022; Lim et al., 2023).

Cyberbullying Interventions and Prevention

Meta-analytic data suggests that interventions against cyberbullying, in general, produce modest but

meaningful decreases in perpetration and victimisation, with stronger results when the elements of the intervention are multi-component and socio-ecologically grounded (Gaffney et al., 2019; Lan et al., 2022; Polanin et al., 2022). Awareness and digital citizenship interventions may promote knowledge, norms and help-seeking behaviours, however long-term sustainability may be likely contingent upon institutional support, staff capacity and incorporation into overarching wellbeing strategies (Lim et al., 2023; So, 2020).

But the implementation gap continues to be a stubborn sticking point. The ability of schools to enact interventions with fidelity is highly variable and sporadic enforcement and punishments can inhibit reporting and damage student trust (Polanin et al., 2022; Batool et al., 2025). This underlines the importance of addressing cyberbullying in the context of organization and governance—with staff being trained, processes being made explicit, and support provided to pupils at the centre of an initiative—rather than treating it as events that happen in isolation (Bhat, 2008; Myers & Cowie, 2019).

Ethical Implications

The use of AI and monitoring tools in childhood education contexts involve ethical tensions between protecting students while respecting children's fundamental rights to privacy, autonomy, and non-discriminatory treatment (He et al., 2024). Algorithmic bias, influenced by biased data sets, cultural-linguistic mismatches, or proxy variables, may inequitably affect marginalized learners and lead to inequitable disciplinary outcomes (Batool et al., 2025). Moreover, surveillance of such a scale also runs the risk of normalizing the surveillance of learning spaces, and potentially stifling authentic expression, undermining the trust required for students to report harm (Nee et al., 2023). New development of generative AI issues brings out new governance issues as well: Generative approaches may be conducive toward anticipatory safety design (for instance, training and scenario modelling), but they can also increase potential for misuse and accountability issues when used in the absence of strong governance (Chaudhary et al., 2024). Thus, ethical cyberbullying response in school-age education contexts call for transparent governance, proportionality, explainability where applicable and alignment with whole-school prevention frameworks as opposed to 'detect and punish' logic from the perspective of prevention frameworks (Lan et al., 2022; He et al., 2024).

Research gap

The reviewed literature indicates persistent disciplinary fragmentation despite significant progress in addressing cyberbullying within school-age populations. Existing research is mostly siloed, resulting in a major schism between technological progress, educational initiatives, and ethical governance: Research from the fields of computer science focuses primarily on improving the accuracy and scalability of algorithmic models for identifying possible cyberbullying. These mechanistic frameworks, however, do little to incorporate socio-ecological theories, actual school dynamics (Hasan et al., 2023; Ioannou et al., 2018), or children's developmental environments. On the other hand, the research on socio-ecological interventions and school-based interventions demonstrates the proven effectiveness of multi-level prevention schemes that include students, educators, families, and institutions (Lan et al., 2022; Polanin et al., 2022). However, this body of the literature does not effectively address the AI-powered detection systems introduced into educational contexts. Both in technological and academic research, significant ethical concerns: student privacy, surveillance that becomes routine, algorithmic bias, are widely recognized yet rendered at the periphery rather than considered as foundational design concerns (Batool et al., 2025; He et al., 2024). Such fragmentation highlights considerable gaps in the literature to date. To do so, we need an integrated socio-ecological synthesis, leveraging AI-mediated technology detection as well as developmentally relevant, human-centred interventions grounded in ethical stewardship. These disciplinary silos present a critical need for broad and child-centered cyberbullying approaches in this current digital world of learning.

Conceptual Framework

Based on the synthesis of the literature that has been reviewed, the present study formulates an

integrated socio-ecological conceptual model in explaining the interaction between cyberbullying detection technologies, socio-educational interventions, and ethical governance practices in the school-age digital contexts. The model is not considered a prescriptive framework; rather, it is an interpretive framework which integrates the evidence in the technological, psychosocial, and institutional settings. It outlines the connection of interdependence between automated detection systems, human decision-making in schools, and the multi-level interventions of students, families, and communities. Figure 2 illustrates how ethically governed AI-based detection supports school response frameworks, enabling coordinated, multi-level interventions across students, peers, families, and policy contexts to reduce cyberbullying, strengthen help-seeking, and promote a positive school climate. It is the integrated socio-ecological conceptual model that worked out in this research paper that provides the concept of cyberbullying in childhood digital-based settings as a socio-technical process performed at a variety of levels. Detectors made by AI assist in detecting early signs of harmful online behaviour. However, the results must be interpreted and mediated by humans at a school level to prompt the necessary action. Efficient prevention and intervention are disseminated in the socio-ecological levels such as student support, peer and classroom intervention, family involvement, and institutional policy. The nature of ethical and privacy governance is a cross-cutting dimension that determines the levels of trust, proportionality, and accountability at every level of detection and intervention.

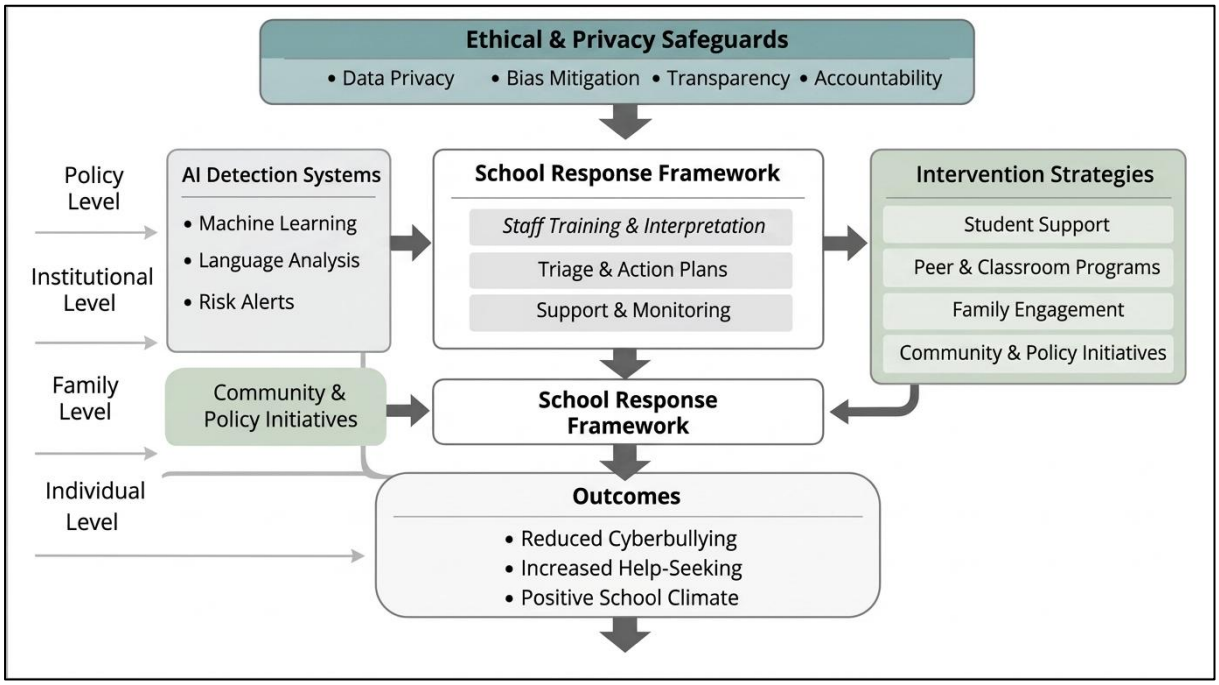

Figure 2. Conceptual model of socio-ecological cyberbullying detection and ıntervention in school-age digital environments

The model shows that AI-assisted cyberbullying detection can impact school-mediated response and multi-level intervention on the individual, relationship, family, institutional, and policy levels. Cross-cutting governance mechanisms are ethical and privacy protection. The last directional flow constitutes a feedback mechanism whereby the results of the interventions are used to continue to enhance the school practices, policies, and support systems.

Methodology

Research Design

The research followed a literature review approach, to investigate the technologies used in detecting cyber bullies, strategies that can be used to intervene, and ethics in the school-age digital space. To maintain transparency, methodological rigour and reproducibility, the review was based on the Preferred Reporting Items to Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines (Page

et al., 2021). The systematic approach was chosen because of the attribute of interdisciplinary nature of the research on cyberbullying, which covers cyberpsychology, education, computer science, as well as human-computer interaction. The review concentrated on the synthesis of empirical and review-based evidence of both technological detection systems, for example, machine learning, artificial intelligence, mobile monitoring, and social-ecological interventions, and specifically on taking ethical and psychosocial implications into account that could be associated with children and adolescents. To improve reliability and reduce selection bias, study screening and data extraction were independently reviewed and cross-checked. Disagreements were resolved through discussion. The review followed PRISMA 2020 reporting guidance throughout.

Search Strategy

A comprehensive literature search was conducted across the following electronic databases including IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Google Scholar. The search covered publications between 2008 and 2025, capturing both foundational studies and recent advances in artificial intelligence-driven cyberbullying detection and intervention research. The final search string combined multiple keyword groups using Boolean operators: (i) Cyberbullying OR online harassment OR digital aggression, (ii) Detection systems OR machine learning OR deep learning OR artificial intelligence, (iii) Intervention OR prevention OR educational programs OR counselling, (iv) School-age OR school OR children OR adolescents, and (v) Mobile technologies OR apps OR tracking systems. All records were retrieved from academic databases listed above, and only peer-reviewed and methodologically transparent studies were retained during eligibility assessment.

Inclusion and Exclusion Criteria

Studies were selected using predefined inclusion and exclusion criteria.

Inclusion criteria. The inclusion criteria are published articles between 2008 and 2025, focused on school-age populations (ages 5 – 18), examined cyberbullying detection technologies and/or intervention strategies, empirical studies, systematic reviews, or meta-analyses, and published in English.

Exclusion criteria. The exclusion criteria are studies focused exclusively on higher education or adult populations, research addressing traditional (offline) bullying only, opinion pieces, editorials, or commentaries without methodological transparency, and non-English publications.

Study Selection Process

The process of selection was based on PRISMA, and it was conducted in three phases, including identification, eligibility, and inclusion. Titles and abstracts were filtered after elimination of the duplicates. Against the inclusion criteria, the full-text articles were then evaluated, and exclusions were recorded according to population mismatch, unclear methodology, or irrelevance. The search of the database found 103 entries in scholarly databases (Google Scholar, ResearchGate, SpringerLink, and IEEE Xplore, and ACM Digital Library). Once the duplicate records had been eliminated (twenty-five records), seventy-eight records were filtered by titles and abstracts. After this screening, fifty-two records were eliminated. Twenty-six full-text articles were assessed for eligibility, of which thirteen were excluded due to population mismatch, lack of methodological clarity, editorial or opinion-based content, or language restrictions. A total of seventeen studies were incorporated in the study due to the fulfilment of all inclusion criteria. A PRISMA 2020 flow diagram is utilised to describe the process of selecting the study (Figure 3).

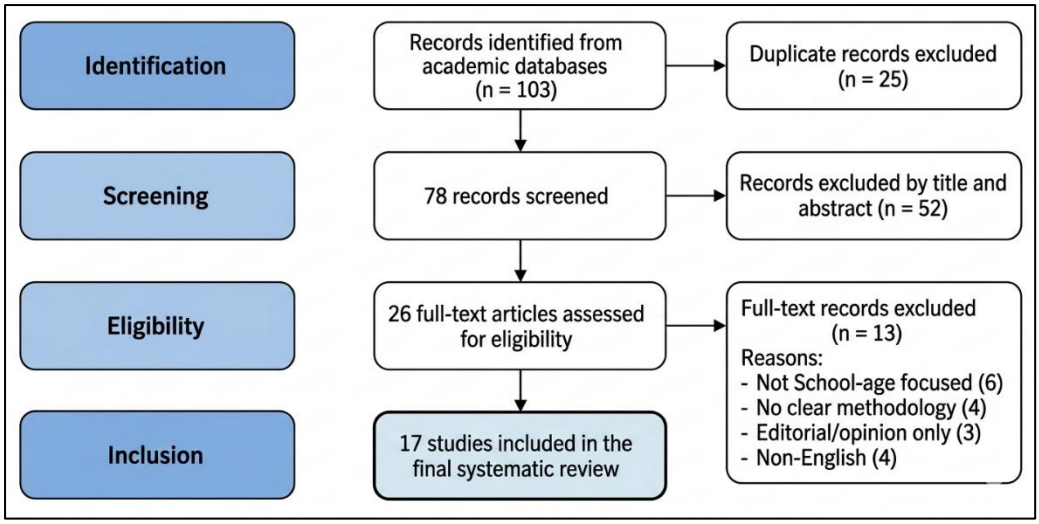

Figure 3. PRISMA 2020 Flow Diagram of Study Selection Process

Data extraction and synthesis

Data were systematically extracted from each included study, capturing publication year and country, study population and educational context, detection or intervention focus, methodological approach, key findings and outcomes, and reported limitations and ethical considerations. Given heterogeneity in study design and outcome measures, a narrative thematic synthesis was conducted. Findings were organised into three analytical domains: cyberbullying detection technologies, intervention and prevention strategies, and ethical, technical and institutional challenges. Additional variables extracted included study location, educational setting, intervention characteristics, and ethical considerations. Where information was unclear or incomplete, interpretations were based on available study descriptions.

Quality Assessment

To guarantee methodological rigour and reliability, the included studies were critically appraised using the Mixed Methods Appraisal Tool (MMAT) 2018, which is suitable for heterogeneous study designs such as empirical studies, systematic reviews and mixed-methods research. The appraisal assessed research studies in terms of clarity of research questions; appropriateness of the methodology; data collection procedures; validity of the findings; and transparency of reporting. The quality (high, moderate, low) of each study was determined separately based on the respective MMAT criteria. In the eligibility stage, studies were excluded if they were rated as low quality for their methodological transparency and/or their evidence reporting. In general, the majority of the studies included showed a moderate to high methodological level, especially the systematic reviews and meta-analyses, which followed reporting standards.

Quality Assessment Table

To ensure reliability, transparency and relevance of evidence synthesized in this review, methodological quality of the studies included was assessed. Each study was assessed for the appropriateness of the research design, clarity of the methodology, procedures for data collection, and validity of the study results using the Mixed Methods Appraisal Tool (MMAT), 2018. Table 1 summarizes the quality assessment of the 17 studies that were included in the review.

Table 1. Quality Assessment of Included Studies

Author	Study Type	Appraisal Tool	Quality Rating
Aricak et al. (2008)	Empirical survey	MMAT	Moderate
Arif (2021)	Systematic review	MMAT	High
Batool et al. (2025)	Systematic review	MMAT	High
Bhat (2008)	Narrative review	MMAT	Moderate
Cassidy et al. (2013)	Systematic review	MMAT	High
Chaudhary et al. (2024)	Empirical AI study	MMAT	Moderate
Gaffney et al. (2019)	Meta-analysis	MMAT	High
Guo (2016)	Meta-analysis	MMAT	High
Hasan et al. (2023)	Systematic review	MMAT	High
He et al. (2024)	Literature review	MMAT	Moderate
Ioannou et al. (2018)	Conceptual synthesis	MMAT	Moderate
Lan et al. (2022)	Systematic review/meta-analysis	MMAT	High
Lim et al. (2023)	Systematic review	MMAT	High
Nee et al. (2023)	Systematic review	MMAT	High
Polanin et al. (2022)	Meta-analysis	MMAT	High
Rattanawiboonsom et al. (2025)	Empirical study	MMAT	Moderate
Wang et al. (2024)	Systematic review	MMAT	High

Results

Research Question One: What are the cyberbullying detection technology and school-based interventions that have been created for childhood digital learning environments?

The results of the research questions indicate that technological and socio-educational solutions have been developed to address cyberbullying in childhood digital learning environments. Artificial intelligence-based detection systems, machine learning models, deep learning approaches, and multimodal detection systems were all identified as being effective in the reviewed studies, as were school-based interventions like counselling, digital citizenship education, peer-support strategies, and coordinated family-school strategies.

Cyberbullying Detection Technologies

According to the reviewed literature, studies on the detection of cyberbullying in childhood school settings have largely emphasized the use of computational methods. Commonly reported were traditional machine learning models such as Support Vector Machines, Naive Bayes classifiers, and

Random Forest algorithms. These strategies proved useful in detecting overt abusive words only but scarred in detecting context sensitive abusive words like sarcasm, slang, and coded peer communication. Table 2 summarises the principal cyberbullying detection approaches reported across the included studies, highlighting typical techniques, strengths, limitations, and implications for implementation.

Table 2. Summary of Cyberbullying Detection Technologies in School-Age Digital Settings

Detection Approach	Typical Techniques / Data	Evidence Base (from included studies)	Strengths	Key Limitations	Implications for School Use
Traditional Machine Learning (ML)	Text features (e.g., bag-of-words, n-grams); SVM, Naïve Bayes, Random Forest	ML detection trends and pipelines (Arif, 2021; Ioannou et al., 2018; Nee et al., 2023)	Efficient; interpretable; low compute cost	Limited contextual understanding; weak on sarcasm/slang; low generalisability (Ioannou et al., 2018; Arif, 2021)	Suitable for baseline monitoring with human oversight
Deep Learning (DL)	CNN, RNN/LSTM, Transformers (text-based)	Reviews of DL performance and trends (Hasan et al., 2023; Nee et al., 2023)	Improved contextual accuracy	High data and compute demands; limited explainability; bias risk (Hasan et al., 2023; Batool et al., 2025)	Adoption depends on governance, resources, and transparency
Multimodal Detection	Text + emotion, behavioural, or media cues	Multimodal emotion-based detection reviews (Wang et al., 2024)	Captures non-text signals	Privacy risks; complexity; cultural/contextual variability (Wang et al., 2024; Batool et al., 2025)	Requires strong ethical safeguards in child settings
Hybrid / Context-Enriched Models	Text + behavioural, relational, or institutional data	Proposals linking detection with intervention context (Ioannou et al., 2018; He et al., 2024)	Higher ecological validity	Implementation complexity; privacy and surveillance concerns (He et al., 2024; Batool et al., 2025)	Best embedded within whole-school response frameworks
Generative AI–Enabled Approaches	Generative AI for detection support and scenario modelling	Emerging empirical evidence (Chaudhary et al., 2024)	Adaptive and proactive potential	Governance, accountability, and misuse risks (Chaudhary et al., 2024; He et al., 2024)	Experimental; use cautiously with institutional oversight
School-Centred Feasibility & Governance *(cross-*	Privacy, consent, bias mitigation, staff training	Reported implementation and governance issues (Nee et al., 2023; He et	Builds trust and accountability	Weak safeguards undermine trust and safety	Essential for ethical and sustainable school deployment

cutting)	al., 2024; Batool et al., 2025)

More recent research stated the application of deep-learning constructions, such as convolutional and recurrent neural networks as well as transformer-based networks. These methods were more contextually sensitive and more accurate at classification but needed large, labelled datasets and high levels of computational resources which hampered their practical application in school settings. A few investigations suggested composite detection models that combined linguistic analysis with behavioural or institutional information. The models sought to include relational and contextual data besides text-based classification. Nevertheless, the issues associated with data privacy, interpretability, and the possibility of its implementation were continuously reported. Figure 4 presents an analytical visualisation of cyberbullying detection approaches, illustrating trade-offs between developmental suitability, institutional feasibility, and ethical risk in school-age digital contexts.

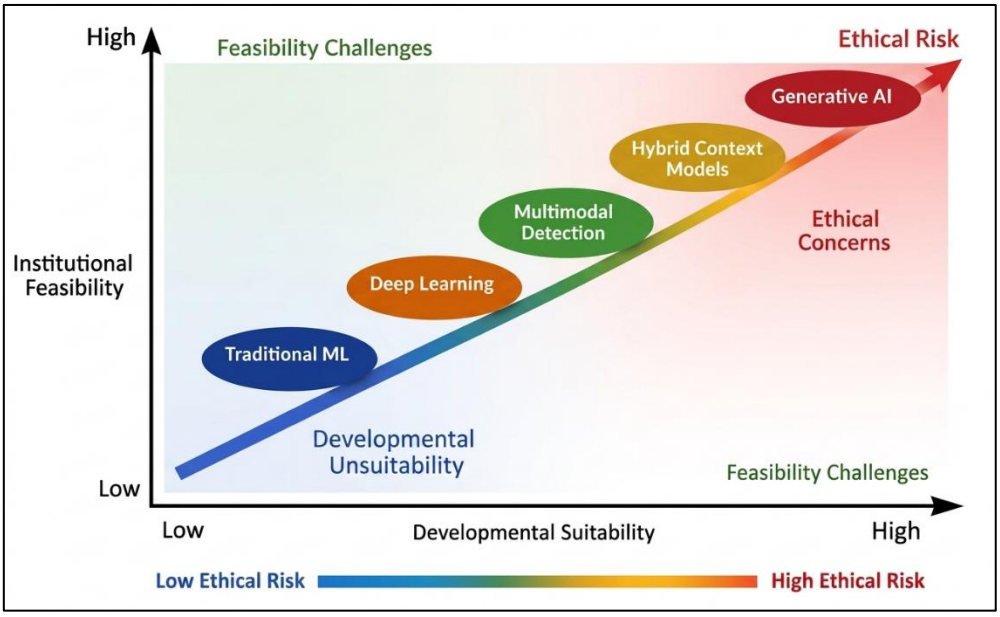

Figure 4. Analytical Mapping of Cyberbullying Detection Approaches in School-Age Digital Contexts.

In figure 4, the diagram summarises cyberbullying detection approaches by mapping them across developmental suitability, institutional feasibility, and ethical risk in school-age contexts. While more advanced AI methods offer greater contextual sensitivity, they also introduce increased ethical and implementation challenges. Generally, the visual highlights that technical sophistication alone is insufficient for school settings unless detection systems are supported by ethical safeguards and integrated within human-centred, socio-ecological response frameworks.

Intervention and Prevention Strategies

The multi-component and school-based interventions based on the socio-ecological framework were the main sources of intervention studies. These interventions usually include students, educators, parents, and institutional policies. In various reviews and meta-analyses, multi-level interventions were linked to significant yet similar effects in reducing cyberbullying perpetration and victimisation. Table 3 summarises intervention strategies reported across the included studies, mapped to socio-ecological levels, and highlighting associated benefits and implementation challenges in school contexts.

Table 3. Socio-Ecological Cyberbullying Intervention Strategies and Reported Challenges in School Contexts

Socio-Ecological Level	Intervention Strategies	Evidence Base (from included studies)	Reported Benefits	Key Challenges
Individual (Child-Focused)	Counselling, coping skills, social-emotional learning (SEL)	School-based and counselling-focused reviews (Bhat, 2008; Guo, 2016; Gaffney et al., 2019)	Improved coping, resilience, and disclosure	Access to trained staff; stigma around help-seeking
Peer / Classroom	Peer support programs, digital citizenship education	Educational and awareness-based interventions (Cassidy et al., 2013; Lim et al., 2023; Lan et al., 2022)	Reduced perpetration and victimisation; improved peer norms	Variable teacher training; inconsistent implementation
Family	Family engagement, parent awareness and guidance	Socio-ecological and school–family intervention reviews (Cassidy et al., 2013; Lan et al., 2022)	Stronger support continuity across home and school	Uneven parental participation; digital literacy gaps
School / Institutional	Clear policies, reporting systems, coordinated response pathways	Policy- and school-level intervention evidence (Polanin et al., 2022; Gaffney et al., 2019)	More consistent and timely responses	Resource constraints; inconsistent policy enforcement
Digital / Technological Support	Reporting apps, monitoring tools, trend analysis platforms	Reviews of technology-assisted interventions (Nee et al., 2023; Rattanawiboonsom et al., 2025)	Extends support beyond classroom; improves visibility	Effectiveness depends on human follow-up and governance
Ethical & Governance (Cross-Cutting)	Safeguarding policies, privacy protection, proportional monitoring	Ethical and implementation-focused reviews (Batool et al., 2025; He et al., 2024)	Builds trust, accountability, and child safety	Privacy, surveillance, consent, and bias concerns

From Table 3, digital citizenship, awareness, social-emotional learning educational programs were quite often reported. The interventions based on counselling were determined especially relevant to assist the affected students in terms of disclosure, coping, and resilience. At the organizational level, more uniform responses to cases of cyberbullying were linked to the fact that clear policies and reporting mechanisms were in place. More exploration of mobile and digital platforms as a more supplementary tool to report, monitor trends, and peer support was done. Although such systems expanded intervention outside the classroom, they required a combination of human-centred support systems to be effective.

Research Question Two: What developmental, psychosocial, technical and ethical issues can affect the effectiveness of these approaches in school?

The literature reviewed reveals a complex mix of developmental, psychosocial, technical, and ethical issues in each of which cyberbullying paradigms in education are systematically limited in effectiveness. All of these hurdles pose significant risks to the credibility of technology surveillance systems, the long-term maintenance of school-based prevention programs, and the integrity of current response systems. The main ones found in the literature are grouped as follows:

Technical and Computational Limitations: While the automated detection algorithms, which are mostly based on traditional machine learning and advanced deep learning architectures, have proven to be very effective at processing mature texts, they are less effective in respect of youth-specific linguistic nuances. These systems often fail to distinguish between the meaning of slang, sarcasm, emojis, quick speech and coded communication between peers, reducing generalizability to a variety of school communities. The current technological systems tend to focus on the discrete categorization of content and to not capture the important relational and contextual aspects of cyberbullying. This reductionist approach produces false positive alerts which may lead to stigmatizing learners, or false negative which create a false sense of security within the institution. Highly accurate deep learning models require large amounts of training data that has to be labeled and significant computational resources, which limits their use for most educational settings.

Ethical and Governance Considerations: The adoption of AI and digital monitoring tools raises significant ethical and governance dilemmas regarding the balancing of the need for protection and the rights of children to privacy, informed consent, and autonomy. Detection systems trained on skewed populations or that do not align with a certain cultural-linguistic context risk inaccurately penalizing the behaviors of marginalized learners and thus creating inequitable disciplinary results. Extensive use of digital surveillance risks to normalize surveillance in learning ecologies. This can stunt true student expression and undermine institutional trust needed for voluntary self-disclosures of harm.

Developmental and Psychosocial Factors: Developmentally, children in school-age years are more vulnerable to digitally mediated aggression, owing to the continued development of their ability to regulate themselves, develop an identity and use peer relationships. In addition to the inherent social stigma attached to help-seeking behaviors, barriers to Disclosure are also the apprehension of punitive institutional repercussions.

Institutional and Implementation Barriers: Structural constraints such as limited financial resources, pedagogical inadequacies of staff members, and a general lack of proactivity in adopting intervention strategies as opposed to reacting to their needs are considered to be institutional and implementation barriers. Resource and competency barriers are the lack of appropriate resources and pedagogical skills of staff members to successfully implement multi-component intervention strategies. Anti-cyberbullying policies are not consistently enforced, and there are no clear reporting mechanisms that are coordinated, which affects the continuity of care and reduces student confidence in the consistency of the student support process.

Therefore, the study as a whole suggests that relying solely on a computational approach to detection is not enough to reduce cyberbullying in the school context. Developmentally appropriate, morally responsible and place- and context-specific approaches that integrate technologized affordances into holistic, human-scale socio-ecological systems are required for sustainable effectiveness.

Research Question Three: What are the implications of socio-ecological and ethically driven cyberbullying prevention models for education practice in Nigeria and other low and middle income countries?

The synthesis of the literature reviewed indicates that while the detection of cyberbullying using technology alone is a viable option, it is not as effective when compared against the socio-ecological and ethically driven models for prevention of cyberbullying in educational practice in Nigeria and LMICs. In such cases, the use of AI solutions that require a heavy use of resources is less likely to be feasible, and will require considerable adaptation. In Nigeria and other LMIC settings, the adoption of high-tech AI surveillance systems is often hindered by logistical and technological challenges, such as poor ICT infrastructure and limited electricity availability, as well as technological expertise among teachers. However, solutions that are over-reliant on technology just don't seem to have an equal investment in institutional capacity and teacher training are not likely to be sustainable.

Cyberbullying is a very context-sensitive and psychosocial phenomenon. In Nigeria, community values, relationships and extended families are highly relevant to socio-ecological interventions because they have a strong impact on child development. Moreover, traditional forms of AI systems (which are typically developed using western data) often struggle to align culturally rooted communication styles, local slang and subtle forms of peer aggression. This means that human-centred strategies such as family engagement and digital citizenship education are not only more culturally responsive, but are also easily integrated with the current priorities in education for character and moral development.

In schools with limited formal guidance systems, building up of the foundational counselling units and embedding digital safety measures into the formal school curriculum are key priority areas. The research shows that whole-school initiatives, which encourage interactivity between students, teachers, families and community representatives, result in a more resilient and supportive school culture than reactive, monitoring that focuses on technology. The application of detection technologies in areas where digital regulatory environments are emerging, presents significant ethical questions about privacy, surveillance and algorithmic bias. However, if monitoring is not accompanied by clear and transparent policies, it can have unexpected consequences including loss of institutional trust, stigmatization of learners, and active discouragement of learners reporting victimization due to fear of punitive disciplinary responses. Thus, prevention models need to be anchored in context-sensitive ethical governance, which should be aligned with ethical frameworks such as the Nigeria Data Protection Act that strike the balance between the protection goals and students' fundamental rights to privacy and autonomy. Overall, the evidence supports the use of hybrid developmental and non-developmental approaches in LMICs. Educational practitioners can design culturally relevant, scalable, and sustainable cyberbullying prevention strategies by combining the effective use of technology to prevent cyberbullying with human mediation and ethical protection measures that are accessible and affordable.

Discussion

The present systematic review summarized the evidence about the detection technologies of cyberbullying, intervention strategies, and ethical considerations in digital environments of school-age through a socio-ecological approach. The results indicate that there is the sustained lack of connection between the relatively fast-paced development and implementation of artificial intelligence-based detection systems (AI) and the relatively slow development and implementation of multi-level, human-centred interventions. Although this gap is also observable on a global scale, it is still more pronounced in Nigeria where the integration of educational technology is still developing and limited by many infrastructural, institutional, and socio-cultural factors. The growth of mobile internet connectivity and social media usage among school-going children has surpassed the progress that has been made in relation to establishing formal digital safety protocols in schools. Despite the opportunities related to early detection of dangerous online behaviours, the applicability of AI-powered detection systems in primary and secondary schools in Nigeria is limited due to limitations like inadequate ICT

infrastructure, unstable electricity supply, limited access to devices, and low level of technical knowledge among teachers. Consequently, direct application of the technologically intensive solutions in the high-resource environments directly to the Nigerian schools might not produce the desired results without a significant adaptation to the local circumstances.

Socio-ecologically, the results support the idea that cyberbullying is not just a simple individual behavioural problem but a multifaceted psychosocial phenomenon that is conditioned by interactions at various levels such as peer relationships, school climate, family structures, and other broader societal norms. These relational and cultural processes are especially affecting in Nigeria, where communal values, respect of authority and extended family are important factors in child development. However, most of the present-day detection technologies are primarily focused on classifying the content, and do not capture such a contextual subtlety as the culturally entrenched patterns of communication, local slang, and indirect forms of aggression that are prevalent in peer interactions. The limitation begs the question of the accuracy as well as the cultural sensitivity of AI-based systems in application within the Nigerian school context. The review also shows that interventions based on coordinated actions of students, teachers, families, and school leadership are more sustainable and adaptable to the context. In such a country as Nigeria, where the formal structures of guidance and counselling often lack sufficient development or necessary resources, enhancement of guidance and counselling units becomes paramount. Also, a transformational role can be played in terms of promoting empathy, responsible online behaviour and awareness of the consequences of cyberbullying by incorporating digital citizenship education in the curriculum. This makes them culturally relevant and practically feasible as they are compatible with the existing educational priorities related to the moral teaching and the formation of the character.

Notably, the results indicate that technological tools ought to be framed as a helpful tool and not as a substitute to professional judgement, pastoral care, and teacher-student relationships. In a Nigeria classroom where teacher authority and interpersonal interaction are still the main focus of learning environments, excessive dependence on automated systems can only be detrimental to trust and to create meaningful intervention. Rather, hybrid solutions that integrate simple technological-support solutions with human controls and relational strategies will be more likely to be effective. The notion of ethical considerations becomes a significant aspect of cyberbullying detection and intervention. The concern of privacy, surveillance, bias in algorithms, and student autonomy are especially relevant in the context when regulatory frameworks and data protection practices remain in their infancy. Misuse of student data, loss of trust, and opposition by students and parents may be some of the unintended consequences of the implementation of monitoring technologies in Nigeria without clear policies, transparency, and accountability mechanisms. This underlines the importance of context sensitive ethical governance that is consistent with national policies such as the Nigeria Data Protection Act, but also recognises the realities of an implementation at the school level.

A cyberpsychological perspective of the results warns against the development of school conditions, which are overly dependent on surveillance and data collection. In the Nigerian setting where stigma and fear of disciplinary measures may already discourage students to report harmful experiences, such methods may also lead to discouragement of disclosure and undermine informal support systems. Developing trust, thus, becomes a primary ingredient of successful cyberbullying prevention. The schools need to put on the front burner safe reporting mechanisms, confidentiality and supportive response that will make the students seek help without fear of punishment or victimisation. Moreover, early childhood and primary education are important intervention points in Nigeria where the fundamental social-emotional skills, moral reasoning and help-seeking behaviours are still underdeveloped. Its integrated socio-ecological framework suggests the necessity of developmentally appropriate strategies that integrate relationship building in classrooms, family engagement and policies that are institutionally supported. Since educational contexts across Nigeria are as varied as the urban-based private schools and the under-resourced rural public schools, flexibility and scalability of interventions are critical factors.

The study outlines the need to balance cyberbullying intervention plans with the overall school wellbeing and digital education frameworks to educational technology practitioners and policy makers. Instead of viewing cyberbullying as the isolated technological problem, it should be embedded into the whole-school strategies that would combine the protection, digital literacy, educator training, and community involvement. The combination of the two will not only promote effectiveness but also make sure that interventions are culturally appropriate, ethically sound, and sustainable in the Nigerian educational environment.

Limitations and Future Directions

One of the drawbacks of this review is that none of the empirical studies examined were from Nigeria, and there were relatively few studies from low and middle income educational settings. Thus, the results from this study must be treated with a certain level of caution for application in Nigerian schools because of the variations in the technological infrastructure, implementation of policy, digital literacy, and socio-cultural settings. The omission of non-English and informal learning studies might also have left out local knowledge. Future studies ought to be geared towards studies context-specific to Nigerian schools, especially the prevalence and dynamics of cyberbullying. It is necessary to create low-cost, mobile-friendly, and culturally sensitive AI-based detection systems with strong ethical protection. Moreover, it is suggested that more research should be done to investigate the potential of integrating digital citizenship and socio-emotional learning into the Nigerian curriculum and the alignment of research, policy, and school-level practice to ensure sustainable cyberbullying prevention.

Implications of the Study

The need is for schools and policymakers in Nigeria to get out of the one-size-fits-all and technology-focused approaches in response to cyberbullying and instead towards integrated, holistic and socio-ecological approaches that address both detection and responses including psychosocial and ethical governance. In the Nigerian setting, where school-aged children are receiving digital access on an exponential scale, acknowledging mobile devices and through social media, cyberbullying is increasingly becoming a significant yet under-regulated public issue in education. Even though AI-based detection tools have the potential to detect harmful online behaviour at an early stage, their implementation in Nigerian schools is affected by several contextual factors such as poor technological infrastructure, digital literacy gaps between teachers, and inequality in access to digital resources in urban and rural settings. Given that reliance on purely technological solutions could be inadequate and even impractical without corresponding funding to educate teachers; develop institutional capabilities; or develop digital policies. The result of this study emphasizes the need to mainstream cyberbullying prevention into the formal school curriculum by adopting a whole school approach.

In Nigerian schools, this involves building guidance and counselling facilities, embedding digital citizenship and online safety training programmes in curricula and encouraging teachers, parents, and community members to work together. Considering the social and cultural context of Nigeria, family engagement and community sensitization programs may be especially important to influence responsible online behaviour and facilitating the reporting of cyberbullying incidents. Policy wise, frameworks at the national and institutional levels with the explicit inclusion of cyberbullying in educational policies are scarce. Nigeria has larger cybersecurity and child protection frameworks in place, but its implementation in the shape of policy and implementation at schools is still lacking. Therefore, study findings suggest that it is required to create locally responsive guidelines which weigh between students' safeguarding and their rights to privacy, autonomy, and freedom of expression. Additionally, the ethical aspects are even more relevant to Nigerian context regarding trust in organizational systems that could bias reporting behaviour. When implementing monitoring or AI based systems, it is necessary to consider the transparency, proportionality and accountability to avoid potential unintended consequences (e.g. students not trusting their system, or misuse of the surveillance systems). Integrating technology, education and ethics as evidence sources, our research offers an organized approach for educators, school principals and policymakers in Nigeria to develop

developmentally sensitive, user-friendly and sustainable cyberbullying interventions. In practice, the findings recommend that cyberbullying prevention be considered part of wellbeing policies in whole schools instead of as a technology-only solution or a separate one, the focus should be on responding in ways that are inclusive, locally grounded and designed to meet the needs of the child holistically.

Conclusion

Cyberbullying in the context of the education of children is a multi-layered socio-educational phenomenon that requires an integrated and people-centred response. As shown in this review, AI powered detection systems have dynamic capabilities for online harm detection, but they are only as effective as the supporting psychosocial intervention, strong ethical governance, and institutional readiness. The development of digital resilience, empathy and inclusive learning practices are essential to sustainable prevention and depend on the seamless combination of technological innovation and multi-level socio-ecological intervention. This paper calls for action to foster critical interdisciplinary collaboration among education, families, policy makers, and technology developers, as a synthesis of evidence in the technological, educational, and ethical areas. Finally, it is important that these integrated frameworks are incorporated into culturally responsive and context-specific policies since this is essential not just in creating safer digital learning environments, but also in preparing the next generation of resilient and ethically responsible digital citizens.

Competing Interests Statement

The authors declare that there are no known financial, professional, personal, or institutional competing interests that could have appeared to influence the work reported in this systematic review. The research was conducted independently for academic purposes as part of an MSc programme, and no external funding or commercial sponsorship was received.

References

Aricak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Ciplak, S., Yilmaz, N., & Memmedov, C. (2008). Cyberbullying among Turkish adolescents. *Cyberpsychology & Behavior, 11*(3), 253–261. https://doi.org/10.1089/cpb.2007.0016

Arif, M. (2021). A systematic review of machine learning algorithms in cyberbullying detection: Future directions and challenges. *Journal of Information Security and Cybercrimes Research, 4*(1), 1–26. https://doi.org/10.26735/GBTV9013

Batool, I., Shah, M., Dhawankar, P., & Gonul, S. (2025). Behind the screens: A systematic literature review on barriers and mitigating strategies for combating cyberbullying. *Information, 16*(4), Article 263. https://doi.org/10.3390/info16040263

Bauman, S. (2015). Types of cyberbullying. In *Cyberbullying: What counselors need to know* (pp. 53–58). American Counseling Association. https://doi.org/10.1002/9781119221685

Bhat, C. S. (2008). Cyber bullying: Overview and strategies for school counsellors, guidance officers, and all school personnel. *Journal of Psychologists and Counsellors in Schools, 18*(1), 53–66. https://doi.org/10.1375/ajgc.18.1.53

Cassidy, W., Faucher, C., & Jackson, M. (2013). Cyberbullying among youth: A comprehensive review of current international research and its implications and application to policy and practice. *School Psychology International, 34*(6), 575–612. https://doi.org/10.1177/0143034313479697

Chaudhary, P. K., Yalamati, S., Palakurti, N. R., Alam, N., Kolasani, S., & Whig, P. (2024). Detecting

and preventing child cyberbullying using generative artificial intelligence. In *Proceedings of the 2024 Asia Pacific Conference on Innovation in Technology (APCIT)* (pp. 1–5). IEEE. https://doi.org/10.1109/APCIT62007.2024.10673710

Espelage, D. L., Rao, M. A., & Craven, R. G. (2012). Theories of cyberbullying. In *Principles of cyberbullying research* (pp. 49–67). Routledge.

Gaffney, H., Farrington, D. P., Espelage, D. L., & Ttofi, M. M. (2019). Are cyberbullying intervention and prevention programs effective? A systematic and meta-analytical review. *Aggression and Violent Behavior, 45*, 134–153. https://doi.org/10.1016/j.avb.2018.07.002

Guo, S. (2016). A meta-analysis of the predictors of cyberbullying perpetration and victimization. *Psychology in the Schools, 53*(4), 432–453. https://doi.org/10.1002/pits.21914

Hasan, M. T., Hossain, M. A. E., Mukta, M. S. H., Akter, A., Ahmed, M., & Islam, S. (2023). A review on deep-learning-based cyberbullying detection. *Future Internet, 15*(5), Article 179. https://doi.org/10.3390/fi15050179

He, Z., Li, Y. J., & Lee, M. K. (2024). IT solutions for tackling cyberbullying: A literature review. In *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*. https://aisel.aisnet.org/pacis2024

Ioannou, A., Blackburn, J., Stringhini, G., De Cristofaro, E., Kourtellis, N., & Sirivianos, M. (2018). From risk factors to detection and intervention: A practical proposal for future work on cyberbullying. *Behaviour & Information Technology, 37*(3), 258–266. https://doi.org/10.1080/0144929X.2018.1432688

Lan, M., Law, N., & Pan, Q. (2022). Effectiveness of anti-cyberbullying educational programs: A socio-ecologically grounded systematic review and meta-analysis. *Computers in Human Behavior, 130*, Article 107200. https://doi.org/10.1016/j.chb.2022.107200

Leung, A. N. M. (2023). Cyberbullying research among children and adolescents: Suggestions for future directions. In *Cyberbullying and values education* (pp. 192–210). Routledge.

Lim, W., Lau, B. T., & Islam, F. M. A. (2023). Cyberbullying awareness intervention in digital and non-digital environment for youth: Current knowledge. *Education and Information Technologies, 28*(6), 6869–6925. https://doi.org/10.1007/s10639-022-11472-z

Lu, L. (2025). Understanding cyberbullying: Causes, consequences and comprehensive intervention strategies. *Trends in Sociology, 3*(1), 1–20. https://doi.org/10.61187/ts.v3i1.203

Myers, C. A., & Cowie, H. (2019). Cyberbullying across the lifespan of education: Issues and interventions from school to university. *International Journal of Environmental Research and Public Health, 16*(7), Article 1217. https://doi.org/10.3390/ijerph16071217

Nee, C. N., Samsudin, N., Chuan, H. M., Mohd Ridzuan, M. I. B., Boon, O. P., Mohamad, A. M. B., & Scheithauer, H. (2023). The digital defence against cyberbullying: A systematic review of tech-based approaches. *Cogent Education, 10*(2), Article 2288492. https://doi.org/10.1080/2331186X.2023.2288492

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Polanin, J. R., Espelage, D. L., Grotpeter, J. K., Ingram, K., Michaelson, L., Spinney, E., Valido, A., Sheikh, A. E., Torgal, C., & Robinson, L. (2022). A systematic review and meta-analysis of interventions to decrease cyberbullying perpetration and victimization. *Prevention Science, 23*(3), 439–454. https://doi.org/10.1007/s11121-021-01259-y

Rattanawiboonsom, V., Sikandar, H., Thatsaringkharnsakun, U., & Khan, N. (2025). The role of mobile technologies in tracking cyberbullying trends and social adaptation among teenagers. *International Journal of Interactive Mobile Technologies, 19*(1). https://doi.org/10.3991/ijim.v19i01.52747

Sidhu, M. S., & Sidhu, K. K. (2025). AI strategies for handling disciplinary and cyber bullying in schools. In *Current and future trends on AI applications* (Vol. 1, pp. 207–229). Springer Nature Switzerland.

So, A. (2020). *Exploring cyberbullying in K–12 education in Canada to promote cyberbullying awareness and prevention measures* (Doctoral dissertation, University of Ottawa). http://dx.doi.org/10.20381/ruor-24909

Wang, S., Shibghatullah, A. S., Iqbal, T. J., & Keoy, K. H. (2024). A review of multimodal-based emotion recognition techniques for cyberbullying detection in online social media platforms. *Neural Computing and Applications, 36*(35), 21923–21956. https://doi.org/10.1007/s00521-024-10371-3