Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Real-Time Content Moderation in Gaming Platforms: Technical Frameworks for Child Protection

Naveen Reddy Dendi
Independent Researcher, USA
Corresponding Author: Naveen Reddy Dendi, **E-mail**: naveenrdendi@gmail.com

| ABSTRACT
This article examines the evolving technical frameworks employed by gaming platforms to create safe digital environments for children. As gaming environments have transformed into significant social interaction hubs for young users, the implementation of sophisticated moderation systems has become critical. The examination reveals real-time moderation technologies, including specialized machine learning models, natural language processing algorithms, and automated speech recognition systems designed to identify concerning patterns without disrupting gameplay. Child-specific protection mechanisms include behavior-based classifiers trained to detect grooming behaviors and customizable parental controls, alongside multi-layered approaches combining AI automation with human oversight. Through comparative case studies of major platforms such as Roblox, Minecraft, and Fortnite, the article identifies effective technical strategies, implementation challenges, and emerging best practices. The findings highlight the importance of balancing robust protection with positive user experience and suggest future directions for both technical innovation and policy development in digital child safety.

| KEYWORDS

Content moderation, child safety, machine learning, gaming platforms, real-time detection.

| ARTICLE INFORMATION

ACCEPTED: 01 August 2025 **PUBLISHED:** 28 August 2025 **DOI:** 10.32996/jcsts.2025.7.9.1

1. Introduction to Gaming Platforms as Social Spaces

The landscape of digital gaming has undergone a remarkable transformation, evolving from isolated entertainment systems into dynamic interactive social hubs where players can connect, communicate, and collaborate in real time [1]. This evolution has been accelerated by technological advancements in cloud computing, augmented reality, and human-machine interaction frameworks, creating immersive environments that transcend traditional gaming experiences. Research on spatial augmented reality in projected gaming environments demonstrates how these platforms now facilitate complex social interactions mediated through digital interfaces and virtual personas [1].

For children, these gaming platforms have become particularly significant communication channels, often representing their primary digital social spaces. Digital education applications and gaming environments have become integral to children's social development and learning processes [2]. These platforms offer unique opportunities for creative expression, collaborative problem-solving, and relationship building across geographic boundaries, forming a crucial component of contemporary childhood socialization.

However, the transformation of gaming environments into social spaces introduces distinctive safety challenges. Unlike moderated educational content with predetermined parameters, social gaming involves dynamic, unpredictable interactions between users of varying ages and intentions. These environments must balance open communication with protective measures against inappropriate content, harassment, and predatory behavior. The real-time nature of interactions, coupled with the

multimedia format incorporating text, voice, and visual elements, creates complex moderation scenarios that traditional content filtering approaches cannot adequately address [1, 2].

This article examines how technical moderation approaches are being developed and implemented to protect children in gaming environments while preserving their social and creative benefits. We analyze the integration of machine learning, natural language processing, and automated speech recognition technologies with human oversight to create multi-layered protection systems. Through comparative analysis of implementation strategies across major gaming platforms, we identify effective technical frameworks that balance safety imperatives with engaging user experiences in these evolving digital social spaces.

1.1 Evolution of Gaming Environments into Interactive Social Hubs

The transition of gaming platforms from simple entertainment systems to complex social environments represents a fundamental shift in digital interaction paradigms. These environments now incorporate sophisticated communication tools, collaborative gameplay mechanics, and persistent virtual worlds where users develop ongoing relationships and communities. The integration of spatial augmented reality with robotic interfaces has further expanded the interactive capabilities of these platforms, creating hybrid physical-digital spaces that enhance social presence and engagement [1]. This evolution has transformed gaming from a solitary or limited multiplayer activity into expansive social ecosystems with their own cultures, norms, and interaction patterns.

1.2 Significance of Gaming Platforms in Children's Communication Landscape

Gaming platforms now occupy a central position in children's digital social lives, often serving as primary venues for peer interaction outside of school settings. These environments provide structured contexts for social exchange through shared activities and goals, creating natural conversation prompts that can help children develop communication skills. The accessibility of digital education applications designed specifically for younger users has expanded the reach of these platforms across diverse age groups and developmental stages [2]. For many children, these gaming spaces represent their first experience with digital citizenship, shaping their understanding of online social norms and digital communication practices.

1.3 Unique Safety Challenges in Digital Gaming Environments

The interactive nature of gaming platforms presents distinct moderation challenges compared to passive media consumption. The combination of real-time communication, avatar-based interaction, and immersive environments creates complex scenarios for content monitoring. Voice chat features, increasingly common in gaming platforms, introduce additional moderation difficulties as they bypass traditional text filtering systems. The pseudo-anonymous nature of many gaming interactions can embolden inappropriate behavior while making user verification more difficult. Furthermore, the global reach of these platforms means they must navigate varying cultural norms and legal frameworks regarding appropriate content and interaction for minors [1, 2].

1.4 Technical Approaches to Child Protection in Gaming Environments

Addressing these unique challenges requires specialized technical approaches to content moderation that can operate effectively in real-time, interactive environments. Advanced systems now employ machine learning algorithms trained on gaming-specific datasets to recognize concerning patterns of interaction beyond simple keyword filtering. These are increasingly integrated with natural language processing capabilities that can assess contextual meaning and intent, rather than merely identifying prohibited terms. Automated speech recognition technologies are being adapted to monitor voice communications, while behavioral analysis systems track interaction patterns that may indicate grooming or exploitation attempts. These technologies form the foundation of comprehensive protection frameworks that combine automated monitoring with human oversight to create safe digital spaces for children's social gaming experiences.

2. Technical Framework of Real-Time Moderation Systems

The effective moderation of gaming platforms requires sophisticated technical frameworks capable of monitoring and evaluating user interactions in real-time. These systems must process massive volumes of data across multiple communication channels while maintaining low latency to ensure both user safety and seamless gameplay experiences. The technical architecture of these moderation systems incorporates several advanced computational approaches working in concert to create comprehensive protective environments for young users.

Technology Type	Key Applications	Technical Challenges	Primary Advantages
Machine Learning Models	Pattern recognition; Behavioral analysis	Training data requirements; Processing latency	Adaptive learning; Contextual awareness
Natural Language Processing	Text filtering; Intent recognition	Gaming vocabulary; Evasion tactics	Semantic understanding; Language adaptation
Automated Speech Recognition	Voice monitoring; Tone analysis	Background noise; Speaker variation	Non-text communication coverage
Multi-modal Analysis	Combined text, voice, behavior monitoring	Integration complexity; Resource requirements	Comprehensive protection

Table 1: Comparison of Real-Time Moderation Technologies in Gaming Platforms [3, 4]

2.1 Machine Learning Implementation in Continuous Interaction Environments

Real-time moderation systems in gaming platforms deploy specialized machine learning models designed to process continuous streams of interaction data. Unlike traditional content moderation for static media, these systems must analyze ongoing exchanges that build contextual meaning over time. The implementation challenges mirror those faced in other continuous monitoring domains, where models must identify patterns across temporal sequences of data. As demonstrated by research in spatiotemporal analysis using machine learning, these systems can effectively process streaming data to identify aberrant patterns when properly trained on domain-specific datasets [3]. In gaming environments, this translates to models that track conversation flows, detect escalation patterns, and identify concerning shifts in interaction dynamics that may indicate harassment or grooming behaviors. The models employ sequential analysis techniques to maintain contextual awareness across extended interactions, rather than evaluating isolated communications.

2.2 NLP Algorithms for Text-Based Communication Filtering

Text communication remains a primary interaction channel in many gaming platforms, particularly those designed for younger users. Natural Language Processing (NLP) algorithms form the backbone of moderation systems for these text-based exchanges. Modern gaming moderation systems have evolved beyond simple keyword filtering to implement sophisticated semantic analysis capabilities. Research in spam classification using NLP illustrates how advanced linguistic processing can effectively distinguish between benign and concerning communications based on contextual patterns rather than isolated terms [4]. In gaming environments, these systems analyze syntactic structures, semantic relationships, and conversational intent to identify problematic communications. Gaming-specific NLP models are trained on datasets that incorporate gaming vernacular, evolving slang, and evasion tactics that attempt to circumvent traditional filters. These specialized algorithms can recognize coded language, intentional misspellings, and context-dependent meanings that characterize communications in gaming environments.

2.3 ASR Technologies for Voice Chat Moderation

The integration of voice chat features in gaming platforms presents unique technical challenges for content moderation. Automated Speech Recognition (ASR) systems must process diverse accents, speaking styles, and audio quality conditions while accurately converting speech to text for analysis. The real-time requirements of gaming interactions necessitate ASR systems with minimal processing delays, even when handling multiple simultaneous speakers. Research in continuous monitoring using sensory data demonstrates the feasibility of real-time processing for streams of information, providing architectural models applicable to voice moderation systems [3]. Modern gaming platforms implement specialized ASR technologies optimized for gaming environments, with acoustic models trained to handle the background noise, overlapping speech, and emotional vocal expressions common in gameplay situations. These systems work in conjunction with NLP algorithms that analyze the transcribed content for policy violations, creating comprehensive voice moderation frameworks.

2.4 Latency vs. Effectiveness in Real-Time Detection Systems

The tension between processing thoroughness and system responsiveness represents a fundamental challenge in real-time moderation. Low-latency detection is essential to prevent exposure to harmful content, but comprehensive analysis requires more processing time. This technical trade-off necessitates carefully optimized architectures that balance these competing demands. Research in spam classification demonstrates how algorithm efficiency impacts detection accuracy under processing

constraints, providing insights applicable to gaming moderation systems [4]. Gaming platforms address this challenge through tiered processing approaches, where lightweight preliminary filters quickly identify obvious violations while more computationally intensive deep analysis runs concurrently for nuanced detection. Edge computing architectures distribute processing loads across network nodes to minimize central server bottlenecks, while pre-trained model deployment reduces inference time for common violation patterns. These architectural optimizations ensure that moderation systems can maintain both protective effectiveness and the real-time responsiveness essential for engaging gaming experiences.

3. Child-Specific Protection Mechanisms

The protection of children in digital gaming environments necessitates specialized technical approaches that address the unique vulnerabilities of young users. While general content moderation systems provide a foundation for safety, child-specific protection mechanisms incorporate additional layers designed to identify and mitigate risks particularly relevant to minors. These specialized systems account for developmental factors, recognize age-specific interaction patterns, and implement safeguards tailored to the needs of children and their guardians.

3.1 Classification of Behavior-Based Machine Learning Models for Child Safety

Behavior-based machine learning models for child safety operate on the principle that harmful interactions with minors often follow identifiable patterns that can be algorithmically detected. These models analyze interaction sequences rather than isolated communications, enabling them to recognize concerning behavioral trajectories that may not trigger conventional content filters. Research in online grooming detection demonstrates how artificial intelligence technologies can effectively identify sequential behavioral markers indicative of predatory interactions [6]. In gaming environments, these systems track multiple behavioral indicators, including conversation patterns, relationship development attempts, topic progression, and efforts to move communication to private channels. The classification frameworks employ various machine learning approaches, including recurrent neural networks that maintain temporal awareness across extended interactions and gradient boosting models that combine multiple weak classifiers to achieve robust detection performance. These specialized models are designed to recognize the subtle progression of manipulative behaviors that traditional keyword filtering might miss.

3.2 Dataset Development and Training Methodologies for Detecting Grooming Patterns

The effectiveness of child protection systems depends heavily on the quality and specificity of the datasets used to train detection models. Developing appropriate training datasets for grooming detection presents significant challenges, requiring careful curation of examples that represent genuine risk patterns while maintaining ethical standards and privacy protections. Research in intelligent grooming detection systems illustrates methodologies for creating representative datasets that capture the linguistic and behavioral markers of inappropriate interactions [6]. These approaches often combine anonymized real-world data from moderated platforms with synthetic data generated through expert simulation of concerning interaction patterns. Training methodologies typically employ supervised learning with carefully labeled examples of both benign and concerning communications, supplemented by semi-supervised approaches that can leverage larger volumes of unlabeled data. Advanced training regimes incorporate adversarial examples to improve resilience against evasion tactics, while transfer learning techniques adapt general language models to the specific domain of child safety in gaming environments.

3.3 Comparative Analysis of Automated Age Verification Technologies

Automated age verification represents a critical component of child protection frameworks, enabling age-appropriate content filtering and interaction limitations. Modern gaming platforms implement various technical approaches to age verification, each offering different balances of accuracy, privacy, and usability. Research in touch behavior-based age estimation demonstrates how interaction patterns can serve as behavioral biometrics for approximate age determination [5]. These behavioral approaches analyze user interaction with the interface, including touch dynamics, navigation patterns, and gameplay behaviors to estimate age ranges without requiring explicit personal information. Alternative approaches include voice analysis systems that estimate age ranges based on vocal characteristics during voice chat interactions. Multi-factor age estimation combines multiple behavioral indicators to improve accuracy while maintaining privacy, providing gaming platforms with non-intrusive methods to verify appropriate age-gated content access and interaction permissions.

3.4 Technical Architecture of Parental Control Interfaces and Their Customization Capabilities

Parental control systems represent the front-line of child protection, enabling guardians to establish appropriate boundaries for their children's gaming experiences. The technical architecture of these systems must balance comprehensive protection with usability and customization flexibility. Modern parental control interfaces implement multi-layered permission structures, allowing granular configuration of content access, communication permissions, and gameplay time limits. Research in touch behavior-based systems demonstrates how user interface design impacts the effectiveness of protective technologies [5]. Contemporary parental control frameworks incorporate dashboard architectures that provide visual analytics of children's gaming activities, real-time notification systems that alert guardians to potential policy violations, and progressive permission

models that adapt restrictions based on age and demonstrated responsibility. These interfaces increasingly implement machine learning to suggest appropriate settings based on similar user profiles, while maintaining guardian override capabilities for customization to individual family values and child development needs.

4. Multi-layered Moderation Approaches

The complexity of child protection in gaming environments necessitates multi-layered approaches that combine various technical and human elements into cohesive protection frameworks. These integrated systems leverage the complementary strengths of automated technologies and human judgment to create comprehensive safety mechanisms that can adapt to evolving challenges. By implementing defense-in-depth strategies, gaming platforms can address the diverse range of potential risks while maintaining engaging user experiences.

Moderation Layer	Technical Components	Integration Points	Effectiveness Factors
Automated Detection	AI classifiers; Real-time filtering	Primary screening	Processing efficiency
Human Moderation	Review interfaces; Escalation systems	Complex case review	Consistency; Response time
Community Reporting	User interfaces; Evidence collection	Violation identification	Accessibility; Reporter protection
Cross-Platform Coordination	Data sharing APIs; Standard taxonomies	Threat intelligence exchange	Implementation consistency

Table 2: Multi-layered Moderation Components [7, 8]

4.1 Integration of AI-driven Automated Detection with Human Oversight

Modern gaming platforms have developed sophisticated hybrid moderation systems that combine the scalability of AI-driven detection with the nuanced judgment of human moderators. This integration creates moderation workflows where automated systems handle initial content screening and flag potential violations for human review. Research in cloud security demonstrates how balanced approaches combining automation with human oversight create more effective compliance systems than either component alone [7]. In gaming environments, this translates to tiered moderation architectures where AI systems process massive volumes of routine communications while specialized human moderation teams focus on ambiguous cases, appeals, and emerging threat patterns. These human-in-the-loop systems implement carefully designed escalation protocols, ensuring that potentially harmful content receives appropriate review while maintaining operational efficiency. The feedback from human moderators continuously refines automated detection models through supervised learning cycles, enabling systems to adapt to evolving communication patterns and evasion tactics.

4.2 Community Reporting Systems: Technical Implementation and Effectiveness

Community participation forms a critical component of comprehensive moderation frameworks, extending monitoring capabilities beyond automated systems. The technical implementation of reporting mechanisms must balance accessibility with accuracy to effectively leverage user contributions. Research in community engagement through information and communication technologies demonstrates how properly designed reporting interfaces can significantly enhance participation in collective safety efforts [8]. In gaming contexts, these systems implement streamlined reporting workflows with categorized violation types, contextual evidence capture, and appropriate urgency flags for immediate threats. Advanced implementations incorporate reporter reputation systems that weight reports based on previous accuracy, reducing the impact of malicious reporting while prioritizing credible alerts. Technical challenges include preventing report flooding, ensuring reporter anonymity protection, and providing appropriate feedback loops without revealing sensitive moderation details. Effectively designed community reporting systems create multiplier effects for moderation teams while fostering community investment in maintaining safe environments.

4.3 Cross-platform Moderation Standards and Interoperability Concerns

As children frequently participate across multiple gaming environments, the fragmentation of moderation approaches presents significant safety challenges. Cross-platform coordination has been proposed as a future goal in moderation research, with various stakeholders exploring technical standards for safe and privacy-preserving information sharing while respecting privacy constraints and competitive boundaries. Research in cloud security frameworks highlights the importance of standardized compliance approaches across interconnected systems [7]. In the gaming ecosystem, these challenges manifest in efforts to develop shared taxonomies of harmful content, standardized reporting formats, and secure information-sharing protocols for

user safety alerts. Technical implementations include federated trust networks that enable platforms to share threat intelligence without exposing proprietary algorithms or user data, API-based alert systems for coordinated responses to emerging threats, and industry-wide hash-matching databases for known harmful content. These interoperability frameworks must navigate complex legal jurisdictions, varying platform policies, and technical integration challenges while working toward the shared goal of creating consistently safe environments across the gaming ecosystem.

4.4 Balancing User Experience with Safety Protocols in Moderation Design

The technical design of moderation systems must carefully balance protective measures with the core interactive experiences that make gaming platforms engaging for children. Overly restrictive systems can undermine social connection and creative expression, while insufficient protections expose children to unacceptable risks. Research in community engagement applications demonstrates how user-centered design approaches can create protective technologies that complement rather than obstruct core functionalities [8]. In gaming environments, this balance manifests in context-sensitive moderation systems that adjust filtering thresholds based on activity type, adaptive protection levels that correspond to detected risk factors, and transparent feedback mechanisms that help users understand moderation decisions. Technical implementations include progressive permission models that gradually expand communication options as users demonstrate responsible behavior, game-integrated reporting interfaces that minimize disruption to gameplay flow, and educational nudges that guide users toward positive interactions rather than simply blocking negative ones. These balanced designs aim to make safety an enabling feature that supports positive experiences rather than a restrictive layer that diminishes engagement.

5. Case Studies: Implementation in Popular Gaming Platforms

The theoretical frameworks and technical approaches to content moderation find their practical application in the systems implemented by major gaming platforms. By examining these real-world implementations, we can better understand how protective technologies operate in production environments with massive user bases. Each platform has developed unique approaches tailored to their specific user demographics, interaction models, and technical architectures, providing valuable insights into effective moderation strategies.

5.1 Technical Examination of Roblox's Moderation Infrastructure

Roblox presents a particularly challenging moderation environment due to its user-generated content model and predominantly young user base. The platform has implemented a multi-layered moderation infrastructure that combines automated filtering, human review, and developer tools to create a comprehensive protection framework. At the technical core of Roblox's system is a text filtering architecture that applies age-appropriate standards based on user accounts, with more restrictive filters applied to younger users. This system employs machine learning classifiers trained on platform-specific datasets to recognize problematic patterns in both standard communications and the specialized vocabulary that emerges within gaming communities. Beyond text filtering, Roblox implements proactive image and audio scanning systems that evaluate uploaded assets before they enter the platform ecosystem. The platform's moderation architecture extends to game experiences themselves, with automated systems that analyze game mechanics and environments for potential safety issues. This comprehensive approach enables Roblox to maintain protective boundaries while supporting the creative expression central to its platform identity.

5.2 Minecraft's Approach to Safe Creative Environments Through Moderation

Minecraft has pioneered approaches to creating safe creative environments through a combination of technical tools and community governance structures. Research on youth-centered moderation in Minecraft demonstrates how technical architecture decisions shape the governance possibilities within gaming environments [9]. The platform's server-based multiplayer model creates distinct moderation challenges and opportunities, as individual server operators maintain significant control over their environments. Minecraft's technical approach includes providing server administrators with robust moderation tools, including customizable permission systems, logging capabilities, and plugin architectures that enable community-developed moderation extensions. At the platform level, Minecraft implements account-level protections and reporting systems that create baseline safety standards while allowing server-specific community norms to develop. This federated approach to moderation enables the platform to support diverse play communities with varying values and standards while maintaining core safety protections. The effectiveness of this approach depends on both the technical tools provided and the social infrastructure that enables community governance to function effectively within technical boundaries.

5.3 Fortnite's Solutions for Managing Large-Scale Concurrent User Interactions

Fortnite represents one of the most challenging moderation environments due to its massive concurrent user base and real-time interaction model. The platform has developed specialized technical solutions to manage safety in this high-volume, fast-paced environment. Fortnite has reportedly implemented voice chat filtering systems adapted for gaming contexts, likely involving acoustic models capable of handling gameplay-specific audio conditions such as background noise and overlapping speech, based on common practices in the industry. The platform employs behavioral analysis systems that track interaction patterns

across sessions, identifying concerning behaviors that might not be apparent in isolated communications. Fortnite's technical architecture includes regionalized moderation systems that can apply culturally appropriate standards while maintaining global platform policies. The scale of Fortnite's user base necessitates highly optimized detection algorithms capable of processing millions of simultaneous interactions with minimal latency. These technical solutions are complemented by community features that allow players to establish trusted social circles with customized communication permissions, creating layered protection that balances open interaction with safety considerations.

5.4 Comparative Effectiveness Metrics Across Platforms and Moderation Methodologies

The diverse approaches to moderation implemented across gaming platforms provide an opportunity to evaluate the relative effectiveness of different technical strategies. While direct comparison is challenging due to the proprietary nature of moderation systems and the varying contexts in which they operate, certain patterns emerge when examining available metrics. Minecraft's community governance model demonstrates particular strengths in fostering positive community cultures but faces challenges in ensuring consistent protection across diverse server environments [9]. Centralized moderation systems like those employed by Roblox offer more consistent policy enforcement but may struggle to accommodate the contextual nuances of diverse player communities. The effectiveness of moderation systems can be evaluated along multiple dimensions, including false positive rates that measure how often legitimate content is incorrectly flagged, response latency that tracks the time between violation and moderation action, user satisfaction with moderation decisions, and community health indicators that assess the overall safety of the environment. These comparative metrics help identify successful approaches that might be adapted across platforms, while highlighting the importance of tailoring moderation systems to the specific technical and social characteristics of each gaming environment.

Platform	Primary Technical Approach	Unique Protection Features	Target Demographic Considerations
Roblox	Multi-layered filtering	Age-appropriate filtering; Asset screening	Younger users; User-generated content
Minecraft	Community governance tools	Customizable permissions; Plugin architecture	Diverse age ranges; Server-based play
Fortnite	High-volume processing	Voice chat optimization; Trusted circles	Large-scale concurrent users

Table 3: Comparative Analysis of Moderation Approaches in Major Gaming Platforms [9]

6. Conclusion

The technical frameworks for content moderation in gaming platforms represent a crucial frontier in child safety for digital environments. Effective protection systems must integrate multiple technological approaches—from machine learning and natural language processing to automated speech recognition and behavioral analysis—while balancing automated detection with human oversight. The case studies of major gaming platforms illustrate that successful moderation architectures adapt to the specific interaction models and user demographics they serve, with customized solutions for different communication channels and creative environments. Cross-platform coordination and standardization efforts, though challenging, offer promising pathways for creating consistent safety experiences across the fragmented gaming ecosystem. The integration of parental controls and age verification technologies provides essential customization layers that accommodate varying developmental stages and family values. Moving forward, the evolution of content moderation systems will require continued innovation in real-time processing capabilities, improved detection of nuanced harmful behaviors, and greater interoperability between platforms. By advancing these technical approaches while maintaining commitment to child-centered design principles, the gaming industry can create environments that balance the tremendous social and creative benefits these platforms offer with the robust protections necessary to ensure children's wellbeing in these increasingly important digital social spaces.

Funding: This research received no external funding

Conflicts of interest: The authors declare no conflict of interest

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers

References

[1] Aswathi P and Amritha N, et al. (2023). ICT Significance for Community Engagement during COVID in Rural India: An Application Suite, in 2023 IEEE Global Humanitarian Technology Conference (GHTC), December 20, 2023. https://ieeexplore.ieee.org/document/10354703

[2] Deepak S A (2024). Cloud Security in the Age of AI: Balancing Automation and Human Oversight for Effective Compliance, *International Journal of Intelligent Systems and Applications in Engineering,* January 30, 2024. https://ijisae.org/index.php/IJISAE/article/download/7064/5994/12318

[3] Farhana S E, and Khan S N, et al. (2021). SPAM EMAIL CLASSIFICATION USING NLP, *JCRES Journal*, 2021. https://psvpec.in/jcres/2021_2/JCRES_2020_Volume%204,Issue%202_Paper%2011.pdf

[4] Giovanni P, and Andrea S, et al. (2017). Spatial Augmented Reality meets robots: Human-machine interaction in cloud-based projected gaming environments, in 2017 IEEE International Conference on Consumer Electronics (ICCE), January 8-10, 2017. https://ieeexplore.ieee.org/abstract/document/7889276

[5] Hilda B R M and Margarita R R, et al. (2018). Digital education using apps for today's children, in 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), June 13-16, 2018. https://ieeexplore.ieee.org/document/8399329

[6] KATIE S T and KRITHIKA J (2021). Designing for Youth-Centered Moderation and Community Governance in Minecraft, ACM Transactions on Computer-Human Interaction (Volume 28, Issue 4), July 2021.https://dl.acm.org/doi/fullHtml/10.1145/3450290

[7] Md Shafaeat H, and Carl H (2020). Touch Behavior Based Age Estimation Toward Enhancing Child Safety, in 2020 IEEE International Joint Conference on Biometrics (IJCB), September 28–October 1, 2020. https://ieeexplore.ieee.org/document/9304913

[8] Philip A, and Zheming Z, et al. (2019). An Intelligent Online Grooming Detection System Using AI Technologies, in 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), June 23–26, 2019. https://researchportal.northumbria.ac.uk/en/publications/an-intelligent-online-grooming-detection-system-using-ai-technolo

[9] Ton T. H. D, and David U. (2022). Ecological Validation of Machine Learning Models for Spatiotemporal Gait Analysis in Free-Living Environments Using Instrumented Insoles, IEEE Robotics and Automation Letters (Volume: 7, Issue: 4), October 2022. https://ieeexplore.ieee.org/abstract/document/9816101