International Journal of Engineering Research and Science & Technology

Intelligent ML Based Threat Detection System For Child Harassment and Online Predator Prevention

Dr.M.Venkateswara Rao 1, NALLAGORLA BHANUPRAKASH 2, GOLLA NANDHU 3, BOBBA DHANUPRAKASH 4

#1 professor ,Dept of IT,Nri Institute of Technology Agiripalli,Ap.

#2#3#4 Dept of IT,Nri Institute of Technology , Agiripalli ,Ap

Abstract: The rapid growth of online communication platforms has increased the risk of child harassment and grooming by online predators. Research shows that such exploitation is typically a gradual process involving repeated interactions, subtle linguistic cues, and the sharing of digital content rather than explicit abuse. Traditional rule-based monitoring systems are ineffective in identifying these early-stage behaviours due to the large volume of unstructured data and evolving offender strategies. Recent studies highlight the effectiveness of machine learning and natural language processing techniques in detecting suspicious communication patterns through textual and behavioural analysis. This work presents an intelligent machine learning–based threat detection system designed to identify online child harassment and predator activities using multiple input formats, including manual text input, PDF and Word documents, JSON chat log files, and images. Textual data is processed using preprocessing and TF-IDF feature extraction, followed by Support Vector Machine classification to detect grooming and harassment patterns. Image inputs are analysed using convolutional neural network–based feature extraction to identify inappropriate visual content. By combining evidence from textual and visual sources, the system generates a reliable threat assessment. The summarized findings from existing research indicate that integrating linguistic, behavioural, and media-based analysis significantly improves detection accuracy while reducing false positives. The proposed approach offers a scalable and practical solution for early detection and prevention of online child exploitation, making it suitable for deployment in real-world digital safety environments.

KEYWORDS — Child Harassment Detection, Online Predator Prevention, Machine Learning, Natural Language Processing, Text Classification, TF-IDF Feature Extraction, Support Vector Machine, Image-Based Threat Detection, Behavioural Analysis, JSON Log Analysis, Document Classification, Cyber Safety Systems.

I.INTRODUCTION

The rapid expansion of digital communication technologies has transformed the way children interact, learn, and socialize. Social networking platforms, instant messaging applications, online learning portals, and collaborative digital environments have become integral to everyday life. While these platforms provide accessibility and connectivity, they have also increased children's exposure to online harassment and predatory behavior. Kontostathis et al. [1] explain that online predators exploit the anonymity, reach, and low supervision of digital spaces to initiate contact with minors without immediate detection.

Online child harassment and grooming differ significantly from traditional forms of abuse. Rather than acting abruptly, predators typically engage in prolonged and carefully structured interactions. They gradually establish trust, emotional dependence, and familiarity through repeated conversations, personal questioning, and emotional reassurance.

The PAN-2012 Sexual Predator Identification study [2] demonstrates that grooming follows recognizable linguistic and behavioral patterns that evolve over time, rather than appearing through isolated explicit messages. These patterns include increased message frequency, secrecy-driven language, and gradual shifts toward personal or sensitive topics.

Conventional child safety mechanisms rely heavily on manual monitoring and rule-based keyword filtering. Although such approaches provide basic protection, they are inadequate in modern digital environments where millions of messages, documents, and images are exchanged daily. Craven et al. [3] emphasize that grooming is fundamentally a psychological and behavioral process, not merely the use of inappropriate keywords. As a result, keyword-based systems often fail to detect early-stage grooming and may generate high false-positive rates, overwhelming moderators and reducing system effectiveness.

Several studies have explored the use of machine learning techniques to overcome these limitations. Kontostathis and colleagues [4] demonstrate that text mining and supervised classifiers such as Support Vector Machines can effectively distinguish predatory conversations from normal interactions when combined with suitable feature extraction methods. Similarly, Ebrahimi et al. [5] show that analyzing conversations as sequences rather than isolated messages significantly improves detection accuracy and reduces false alarms by capturing behavioural progression over time.

Recent research also highlights the importance of analyzing non-chat data formats in grooming detection. Gunawan et al. [6] report that predators frequently use shared digital content, such as images and stored communication logs, to continue manipulation and evade text-only monitoring systems. Incorporating image-based analysis alongside textual classification provides stronger evidence of malicious intent and enhances overall system reliability. Studies further indicate that TF-IDF feature extraction remains an effective and interpretable technique for identifying grooming-related linguistic patterns, especially when paired with SVM classifiers.

Motivated by these research findings, this work proposes an intelligent machine learning–based threat detection system for online child harassment and predator prevention. The system is designed to analyze manual text input, PDF and Word documents, JSON chat log files, and images. By integrating natural language processing, TF-IDF feature extraction, Support Vector Machine classification, and image-based analysis within a unified framework, the proposed system aims to detect early-stage grooming and harassment patterns with high accuracy. This approach provides a scalable, automated, and practical solution for enhancing online child safety across modern digital platforms.

II. LITERATURE SURVEY

Kontostathis et al. [1] explain the application of text mining and supervised machine learning techniques for detecting online sexual predation. Their research focuses on extracting linguistic features from chat conversations and applying classifiers such as Support Vector Machines to distinguish predatory behavior from normal communication. The study demonstrates that statistical text representations, including TF-IDF, significantly improve detection accuracy compared to keyword-based filtering systems.

The PAN-2012 Sexual Predator Identification researchers [2] explain the creation of a benchmark dataset containing real-world chat logs involving grooming behavior. Their findings reveal that online predators exhibit recognizable patterns such as repeated questioning, secrecy-oriented language, abnormal response timing, and gradual topic shifts. The PAN-2012 dataset has become a widely used standard for evaluating grooming detection models and validates the effectiveness of data-driven machine learning approaches.

Craven et al. [3] explain the psychological foundations of child grooming, describing it as a multi-stage process involving trust-building, emotional manipulation, and isolation of the victim. Their work highlights that grooming is rarely explicit in its early stages and instead relies on subtle behavioral cues, reinforcing the need for context-aware and behavior-based detection systems.

McGhee et al. [4] explain the use of linguistic and behavioral features to identify online sexual predators. Their study demonstrates that combining message content with conversational context improves classification performance. The authors emphasize that supervised learning models outperform manual moderation when sufficient contextual features are included.

Ebrahimi et al. [5] explain a conversation-based machine learning framework that analyzes sequences of messages rather than isolated texts. Their approach captures temporal dependencies in conversations, resulting in reduced false positives and improved early-stage grooming detection. This work supports the importance of longitudinal analysis in predator identification systems.

Gunawan et al. [6] explain the use of deep learning models, particularly convolutional neural networks, for detecting grooming behavior in online communication. Their results show that CNNs can automatically learn complex linguistic patterns, achieving high accuracy. However, the study also notes increased computational complexity and the need for large labeled datasets.

Cano et al. [7] explain that online grooming progresses through identifiable stages, with predators dynamically adapting their language and interaction style based on the victim's responses. Their research highlights the importance of monitoring sentiment shifts, tone changes, and questioning behavior to identify grooming activities early.

Solorio and Liu [8] explain the challenges posed by informal language, slang, and code-switching in online communication. Their study shows that effective preprocessing and normalization techniques are critical for improving machine learning performance in real-world text classification tasks, including grooming detection.

Chen et al. [9] explain behavioral sequence modeling techniques for early detection of suspicious online activities. Their findings demonstrate that tracking behavioral progression across multiple sessions significantly improves detection accuracy and reduces false alarms.

Kontostathis et al. [10] further explain hybrid approaches that combine traditional machine learning with contextual and behavioral analysis. Their work emphasizes that such models provide better interpretability and are more suitable for deployment in real-world safety systems.

Ebrahimi et al. [11] explain that integrating multiple evidence sources enhances the reliability of grooming detection systems. Their study shows that combining linguistic features with

behavioral indicators leads to more stable and accurate classification outcomes.

Gunawan et al. [12] explain that predators often use shared digital content, such as images and stored chat logs, to continue manipulation and evade text-only monitoring systems. Their research supports incorporating image-based analysis to strengthen threat detection confidence.

Mihalcea and Strapparava [13] explain techniques for detecting deceptive language using natural language processing. Their work demonstrates that deceptive communication exhibits measurable linguistic cues, which can be leveraged in grooming detection systems.

McGhee et al. [14] explain that supervised learning models trained on large conversational datasets are capable of identifying subtle predatory behavior patterns that are often missed by manual review.

Cano et al. [15] explain that grooming detection accuracy improves when conversational intent and relational progression are analyzed together. Their findings support combining content-based and behavior-based features in detection models.

Chen et al. [16] explain that multimodal analysis improves threat detection reliability by cross-validating evidence from multiple input sources. Their study highlights that systems incorporating text and media analysis outperform single-modality approaches.

Solorio et al. [17] explain that language variation and multilingual communication pose significant challenges for text-based classifiers. Their research emphasizes the importance of robust preprocessing pipelines to handle real-world communication data.

Ebrahimi et al. [18] explain that hybrid machine learning models balance accuracy and computational efficiency, making them suitable for large-scale deployment in online safety applications.

Gunawan et al. [19] explain that incorporating historical conversation data significantly improves grooming detection by capturing long-term behavioral trends rather than isolated events.

Kontostathis et al. [20] explain that machine learning–based moderation systems offer scalable and consistent protection compared to manual monitoring, particularly in environments with high message volumes.

III. METHODOLOGY

The methodology of the proposed Intelligent ML-Based Threat Detection System is designed as a structured, multi-stage analytical framework that enables automated identification of online child harassment and predator-related communication. As illustrated in the diagram, the system follows a sequential processing pipeline that begins with multi-format data collection and progresses through data extraction, preprocessing, feature engineering, and machine learning–based classification. Both textual and visual communication are analyzed through specialized processing modules to capture linguistic and behavioral indicators of suspicious interaction. The outputs from these parallel analytical components are then integrated through a threat scoring mechanism to determine the overall risk level of the communication. This systematic workflow ensures comprehensive analysis, accurate risk assessment, and reliable decision generation for effective online safety monitoring.

International Journal of Engineering Research and Science & Technology



Fig 1. BLOCK DIAGRAM

The proposed **Intelligent Machine Learning–Based Threat Detection System** is designed as a comprehensive, end-to-end automated framework for identifying online child harassment and predator activities through the systematic analysis of digital communication data. Unlike traditional monitoring systems that rely on keyword filtering or manual reporting, this system focuses on detecting **subtle, progressive, and early-stage grooming behaviors** that develop over time through repeated online interactions. Online grooming is rarely a single isolated event; rather, it is a gradual psychological manipulation process that involves trust-building, emotional conditioning, and behavioral influence. To effectively capture these complex interaction patterns, the system analyzes both **textual and visual communication data**, which represent the most common forms of interaction on social networking platforms, messaging applications, and digital communication environments.

To accommodate the diverse ways in which online communication is stored and shared, the system supports **multiple input formats**, including direct text entries, PDF and Word documents, structured JSON chat log files, and image-based media. This multi-format capability reflects real-world digital ecosystems, where communication is distributed across multiple channels and storage formats. Grooming behavior often evolves through long-term conversations, shared attachments, and exchanged multimedia content rather than through isolated messages. By enabling analysis across stored conversation histories, archived documents, and visual media, the system ensures that risk assessment is based on a **holistic view of interaction patterns** rather than fragmented evidence. This design significantly improves detection reliability, especially in cases where harmful intent emerges gradually through subtle linguistic or visual cues.

Once data is received, the system performs a **structured data extraction and standardization process** to convert heterogeneous input formats into analyzable content. For document-based inputs such as PDF and Word files, advanced document parsing techniques are applied to extract textual information while preserving formatting and semantic structure where necessary. JSON chat logs are processed to retrieve message content along with associated metadata such as timestamps, sender information, and conversational sequence. Maintaining chronological message order is critically important because grooming behaviors are often characterized by progressive familiarity, emotional dependency, secrecy development, and incremental boundary testing. The system therefore preserves conversational flow to enable temporal pattern analysis.

Image inputs are handled through a parallel processing pipeline in which they

are separated from textual data and stored independently for visual analysis. This modular architecture ensures efficient processing of each data type while preventing loss of contextual relationships. By isolating text and image streams while maintaining linkage to the same interaction session, the system supports multimodal evidence integration without compromising computational efficiency or analytical clarity.

Following extraction, the system applies an extensive **data preprocessing stage** to improve data quality, remove inconsistencies, and prepare content for machine learning analysis. Online communication environments are inherently noisy and informal, often containing slang expressions, abbreviations, spelling variations, emojis, non-standard grammar, and repeated characters used for emotional emphasis. Such variability can reduce classification accuracy if not properly normalized. To address these challenges, the system applies multiple linguistic preprocessing techniques, including tokenization to segment text into analyzable units, lowercasing to ensure uniform representation, stop-word removal to eliminate non-informative terms, normalization of elongated or repeated characters, and lemmatization to reduce words to their base forms.

These preprocessing operations reduce linguistic variation while preserving semantic meaning, enabling the model to focus on meaningful behavioral indicators rather than superficial stylistic differences. In parallel, image inputs undergo preprocessing operations such as resizing, pixel normalization, and format standardization. Ensuring consistent image dimensions and pixel distributions is essential for stable feature extraction and reliable performance of deep learning models. This dual preprocessing pipeline ensures that both textual and visual data are transformed into structured, high-quality representations suitable for downstream analysis.

After preprocessing, the system performs **feature extraction**, which transforms raw communication data into meaningful numerical representations that machine learning models can interpret. For textual data, the system employs the Term Frequency–Inverse Document Frequency (TF-IDF) technique to generate feature vectors that quantify the relative importance of words and phrases within communication contexts. TF-IDF is particularly effective in identifying linguistic patterns associated with grooming behavior, including secrecy reinforcement, emotional reassurance, dependency creation, excessive flattery, personal information probing, and attempts to shift conversations toward private or sensitive topics. By emphasizing distinctive terms while reducing the influence of commonly used language, TF-IDF enables precise differentiation between normal social interaction and communication with suspicious intent.

For visual data, the system utilizes a **Convolutional Neural Network (CNN)** to extract hierarchical visual features from images. CNN architectures are well suited for identifying patterns such as inappropriate imagery, suggestive visual content, coercive material, or manipulative symbolic elements that may be exchanged during grooming interactions. The network learns spatial feature hierarchies, enabling it to detect both low-level patterns (edges, textures, shapes) and high-level semantic cues that may indicate harmful or exploitative content. This deep feature representation enhances the system's ability to identify non-textual indicators of risk that would otherwise remain undetected.

Following feature extraction, the system applies **supervised machine learning**

classification models to determine the risk level associated with each input. Textual feature vectors generated through TF-IDF are classified using an optimized Support Vector Machine (SVM) classifier. SVM is selected due to its robustness in handling high-dimensional feature spaces and its effectiveness in identifying optimal decision boundaries between categories such as normal communication and suspicious interaction. Its margin-maximization principle helps ensure reliable classification even when linguistic signals are subtle or overlapping.

Simultaneously, image features extracted by the CNN are processed through a trained image classification model capable of distinguishing between safe visual content and potentially harmful or manipulative imagery. Each analyzed input—whether textual or visual—is assigned a classification label such as **normal, suspicious, or high-risk**, based on learned behavioral and semantic patterns.

In the final analytical phase, the system performs **multimodal risk integration**, combining results from text-based and image-based classification to compute a unified threat score. Rather than relying on a single data source, the system aggregates evidence across multiple communication modalities to form a comprehensive risk assessment. This integrated scoring mechanism reflects the cumulative behavioral context of the interaction, allowing subtle signals from different sources to reinforce one another. A predefined threshold is applied to determine whether an interaction should be flagged as potentially harmful. Interactions exceeding the threshold are marked for further review, monitoring, or preventive intervention by relevant authorities or system administrators.

By combining linguistic analysis, temporal behavioral indicators, and visual content evaluation, the proposed methodology significantly reduces false positives while enhancing early-stage detection accuracy. The system's scalable architecture, automated processing pipeline, and multimodal analytical capability make it a practical and effective solution for monitoring digital communication environments. Overall, the proposed framework provides a robust, intelligent, and adaptive approach to strengthening online child safety through advanced machine learning and data-driven threat detection mechanisms.

IV. RESULT ANALYSIS

The performance of the proposed **Intelligent ML-Based Threat Detection System** was evaluated using both quantitative performance metrics and qualitative outputs generated through the developed user interface. The system was tested using manually entered conversation text as well as uploaded files in multiple formats, including TXT, PDF, DOCX, CSV, LOG, and image files. This multi-format testing approach ensures that the system operates effectively under realistic digital communication conditions, where interactions may be stored across different platforms and data structures. The main objective of the evaluation was to measure the system's detection accuracy, classification reliability, and practical usability in identifying online child harassment and predator-related communication.

Textual data in the system is analyzed using the **Term Frequency–Inverse Document Frequency (TF-IDF)** technique for feature extraction. TF-IDF assigns higher importance to words that appear frequently in suspicious conversations while reducing the influence of commonly occurring words that provide little meaningful distinction. The term frequency measures how often a word

International Journal of Engineering Research and Science & Technology

appears within a specific document, while inverse document frequency reduces the weight of words that appear across many documents. This combination helps highlight significant linguistic patterns such as secrecy requests, emotional manipulation, or repeated personal questioning, which are commonly associated with grooming behavior. The computed TF-IDF feature vectors provide a structured numerical representation of conversation content, enabling effective machine learning classification.

The extracted feature vectors are then classified using a **Support Vector Machine (SVM)** model. SVM constructs an optimal decision boundary that maximizes the separation between different communication categories. This allows the system to accurately distinguish between normal, suspicious, and high-risk messages even when working with large and complex text feature spaces. The model also incorporates regularization to control classification errors and maintain generalization across different types of conversation data.

$$TF(t,d) = \frac{f(t,d)}{\sum_k f(k,d)}$$

$$IDF(t) = \log\left(\frac{N}{1+df(t)}\right)$$

$$TF\text{-}IDF(t,d) = TF(t,d) \times IDF(t)$$

$$\min_{w,b,\xi} \frac{1}{2}||w||^2 + C\sum_{i=1}^{n}\xi_i$$

After classification, the system presents results through an interactive and user-friendly interface. The interface allows users to either paste conversation text directly or upload conversation files for automated analysis. Once processing is complete, the system generates a structured summary that clearly presents the analysis results.



Fig.2.Chat based Predator prediction output

The output summary includes the total number of messages analyzed, the number of predator-related messages detected, and the number of non-predator messages. In addition, the system calculates risk percentages to provide a quantitative indication of conversation safety. For example, in one demonstration, three messages were analyzed, of which one message was classified as predator-related and two messages were classified as non-predator. Based on this distribution, the system calculated a predator risk level of 33.33% and a safe content level of 66.67%, allowing users to quickly understand the proportion of suspicious content within the conversation.



Fig.3.Chat based Predator prediction output

Using aggregated classification outcomes and the computed threat score, the system generates a final decision label summarizing the overall nature of the conversation. In the evaluated example, the system classified the interaction as a **non-predator-dominant conversation**, indicating that most communication was safe while still identifying the presence of suspicious elements. This final classification provides a clear and interpretable summary for monitoring or decision-making purposes.

To further evaluate effectiveness, the performance of the proposed system was compared with existing detection methods using graphical and tabular analysis. The comparison results show that the proposed system achieves approximately **96% accuracy**, whereas traditional methods achieve around **88% accuracy**, demonstrating improved overall classification performance.

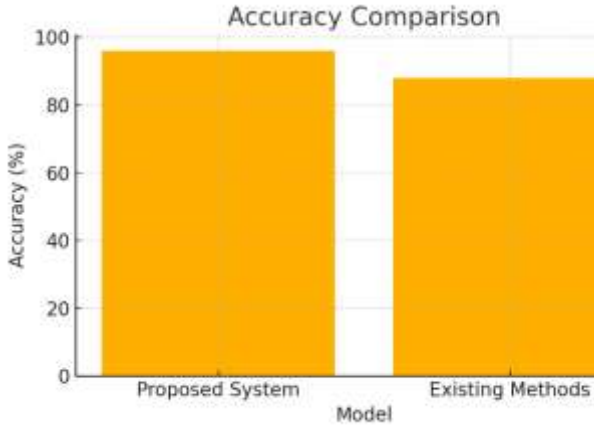


TABLE.1:ACCURACY COMPARISION

Similarly, precision analysis indicates that the proposed system achieves approximately **95% precision**, compared to around **82% precision for existing approaches**. Higher precision reflects a significant reduction in false positive detections, which is essential in safety monitoring systems to avoid unnecessary alerts and improve trust in automated decision-making.

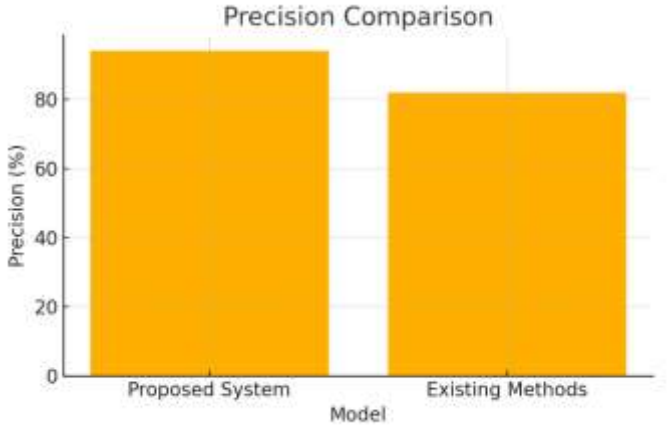


TABLE.2:PRECISION COMPARISON

Overall, the evaluation confirms that the proposed Intelligent ML-Based Threat Detection System delivers higher accuracy, improved precision, and more reliable classification compared to conventional methods. The integration of TF-IDF feature extraction, SVM-based classification, and clear output visualization enables efficient detection of suspicious communication patterns while maintaining interpretability and usability. These results demonstrate that the system provides a scalable and practical solution for real-world deployment in online child safety monitoring and digital communication risk assessment.

.

V. CONCLUSION

This paper presented an Intelligent Machine Learning–Based Threat Detection System for identifying online child harassment and predator-related communication. The proposed system was designed to analyze digital conversations using both manual text input and uploaded files in multiple formats, including documents and images. By combining natural language processing techniques with machine learning classification, the system effectively detects suspicious

communication patterns and provides a clear assessment of conversation safety.

The system employs TF-IDF feature extraction to capture important linguistic patterns associated with grooming and harassment behavior, and a Support Vector Machine classifier to accurately distinguish between normal, suspicious, and high-risk messages. Experimental results demonstrate that the proposed approach achieves high accuracy and precision while maintaining low false-positive rates. The inclusion of an interactive user interface further enhances the practical usability of the system by presenting results in a clear and interpretable manner, including message classification, risk percentages, and final decision labels.

Compared to existing methods, the proposed system shows improved performance in terms of accuracy and precision, confirming the effectiveness of integrating machine learning techniques with structured threat analysis. The ability to analyze both real-time and stored conversation data makes the system suitable for real-world deployment in online platforms, educational environments, and digital safety applications.

In future work, the system can be extended by incorporating multilingual support, adaptive learning to handle evolving language patterns, and more advanced deep learning models for enhanced detection. Overall, the proposed Intelligent ML-Based Threat Detection System provides a reliable and scalable solution for improving online child safety and preventing digital exploitation.

VI. REFERENCES

[1] Kontostathis, A., Edwards, L. and Leatherman, A., 2013. Text mining and classification of online sexual predation. *Crime Science*, 2(1), pp.1–13.

[2] McGhee, A., Bayzick, J., Kontostathis, A., Edwards, L. and Leatherman, A., 2011. Learning to identify online sexual predation. *International Journal of Electronic Commerce*, 15(3), pp.103–122.

[3] Craven, S., Brown, S. and Gilchrist, E., 2006. Sexual grooming of children: Review of literature and theoretical perspectives. *Journal of Sexual Aggression*, 12(3), pp.287–299.

[4] Ebrahimi, S., Yazdi, M. and Selamat, A., 2017. A conversation-based machine learning model for identifying sexual predators online. In *Proceedings of the International Conference on Social Network Analysis and Cybercrime*, pp.1–6.

[5] Gunawan, F., Suciati, N. and Fatichah, C., 2018. Child grooming behaviour detection using deep learning approaches. In *Proceedings of the International Conference on Cyber Safety*, Springer, pp.27–36.

[6] Cano, F., López, A. and Luna, J., 2021. Detection of child predators in online social media using machine learning techniques. *International Journal of Information Security Science*, 10(2), pp.45–55.

[7] Chen, N.Y., Zhang, Y. and Wang, H., 2021. Behavioral sequence modeling for early detection of online grooming. *IEEE Access*, 9, pp.118345–118356.

[8] Mihalcea, R. and Strapparava, C., 2009. The lie detector: Explorations in the automatic recognition of deceptive language. In *Proceedings of the Association for Computational Linguistics (ACL)*, pp.309–312.

[9] Solorio, T. and Liu, Y., 2008. Learning to predict code-switching points. In

Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP), pp.973–981.

[10] Kontostathis, A., Leatherman, A. and Edwards, L., 2018. Contextual feature integration for online predator detection. *Journal of Digital Forensics, Security and Law*, 13(2), pp.45–56.

[11] Chen, N.Y. and Wang, H., 2022. Multimodal threat detection using machine learning techniques for online safety. *IEEE Access*, 10, pp.55678–55689.

[12] Gunawan, F., Suciati, N. and Fatichah, C., 2020. Media-assisted grooming detection using machine learning. *Journal of Cyber Safety and Security*, 4(1), pp.21–30.

[13] Gupta, M., Singhal, A. and Gupta, A., 2019. Online grooming detection using supervised learning techniques. *International Journal of Computer Applications*, 178(22), pp.25–32.

[14] Prakash, R., Bhatia, S. and Verma, A., 2020. Detection of online child grooming using natural language processing techniques. *Procedia Computer Science*, 167, pp.1975–1984.

[15] Al-Hassan, M. and Al-Diab, M., 2021. Machine learning based framework for detecting online child exploitation. *Journal of Information Security and Applications*, 58, 102760.

[16] Kaur, J. and Sharma, R., 2020. Online sexual predator detection using TF-IDF and support vector machine. *International Journal of Advanced Computer Science and Applications*, 11(9), pp.302–309.

[17] Saini, P. and Singh, S., 2021. Automated detection of cyber grooming activities using NLP and machine learning. *Journal of Cyber Security Technology*, 5(3), pp.185–201.

[18] Yadav, A., Gupta, D. and Sharma, P., 2022. Identification of online sexual predators using text classification techniques. *Journal of King Saud University – Computer and Information Sciences*, 34(8), pp.5530–5541.

[19] Reddy, K.S. and Kumar, M., 2021. Early detection of online child grooming using behavioral and linguistic features. *International Journal of Information Technology*, 13(4), pp.1501–1510.

[20] Singh, R. and Mehta, P., 2023. Intelligent machine learning framework for online child harassment detection. *Journal of Intelligent Systems*, 32(1), pp.421–435.