# Agentic AI Framework for KidSafe Browser: Balancing Privacy, Protection, and Education in Enhancing Digital Well-Being and Cyber Protection for Children

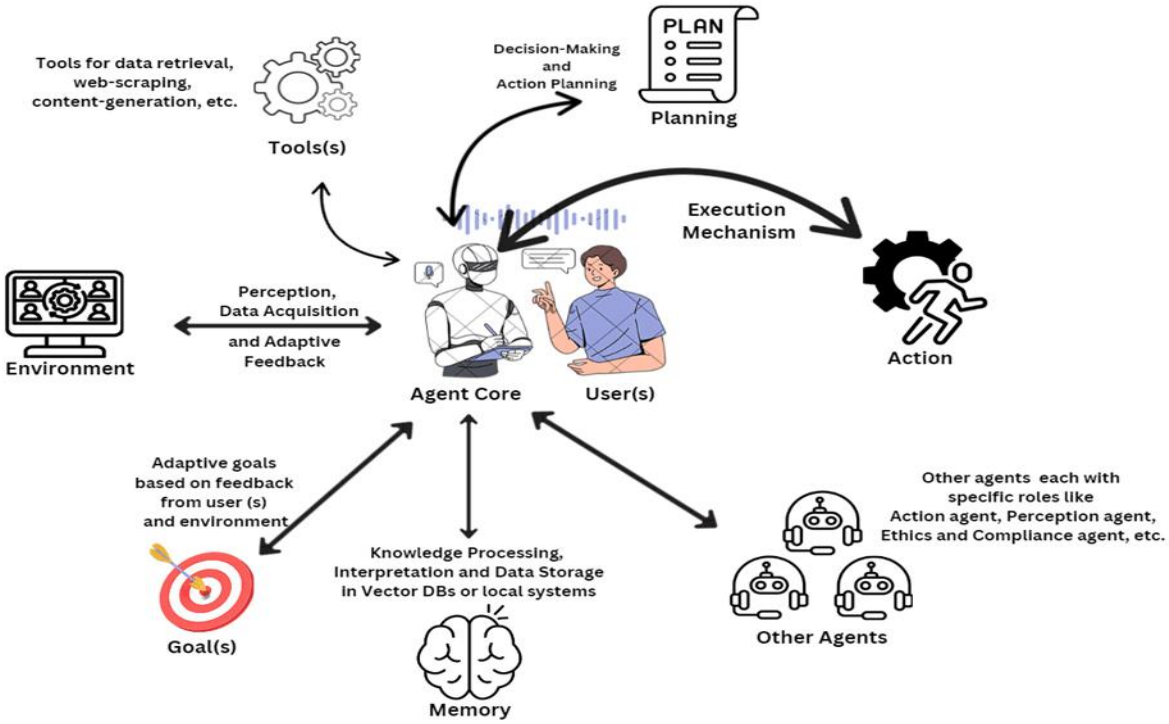
Dr. M.K. Jayanthi Kannan[1], Samridhi Tyagi[2], Himanshu Verma[3], Taniya[4], Harsh Patel[5]
[1]*Professor, School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh - 466114*
[2,3,4,5]*Student School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh - 466114*

**Abstract: The rapid expansion of digital platforms has introduced both opportunities and risks for children accessing the internet. While the web offers immense educational resources, children remain vulnerable to harmful content, cyberbullying, and privacy violations. This paper proposes an Agentic AI Framework for KidSafe Browser, which leverages intelligent monitoring, adaptive learning, and parental control features to ensure safe, age-appropriate, and educational browsing experiences. The framework emphasizes the balance between privacy, protection, and learning, empowering guardians and educators to foster children's digital well-being. Using AI-driven content filtering, behavioral analysis, and dynamic risk detection, the KidSafe Browser ensures a safe environment for children, while maintaining user autonomy and educational growth. The internet offers valuable resources for children, but also exposes them to harmful content. KidSafe AI Browser is an AI-powered solution that ensures safe, age-appropriate browsing by using real-time content filtering, NLP, and sentiment analysis. It blocks inappropriate content, suggests educational alternatives, and includes features like mood-based recommendations to create a secure and engaging online experience for kids.**

**Keywords: Child Online Safety, Artificial Intelligence, Natural Language Processing, Toxic Content Detection, Sentiment Analysis, Parental Control, Real-Time Filtering, Content Moderation, Safe Browsing, Kid-Friendly Browser.**

## I. INTRODUCTION

The internet has become an essential tool for learning and entertainment, even for young children. However, it also exposes them to harmful content such as violence, nudity, hate speech, and cyberbullying. This raises a critical need for a smarter, AI-powered solution that ensures safe and age-appropriate internet access. The KidSafe AI Browser is designed to create a secure and friendly digital space tailored specifically for kids. It uses Artificial Intelligence (AI) and Natural Language Processing (NLP) to, Block or replace harmful content in real-time. Understand the mood and intent behind searched or viewed content. Recommend educational or fun alternatives when inappropriate content is detected. Children are among the most active users of the internet, often engaging in online learning, gaming, and social interactions. However, unfiltered access exposes them to explicit content, misinformation, and malicious actors. Traditional parental control systems either restrict access excessively or fail to address emerging cyber risks. With the increasing sophistication of cyber threats, an intelligent, adaptive, and child-centric approach is essential. This research introduces the Agentic AI Framework for KidSafe Browser, designed to protect children from online risks while simultaneously promoting digital literacy and responsible use.




Fig,1: AI Framework for KidSafe Browser and Cyber Protection for Children

Current safe browsing solutions, such as parental control apps and conventional child-safe browsers, typically rely on, Blacklist/whitelist mechanisms. Manual parental supervision. Static content filters. Limited reporting tools. Limitations of the system, Over-blocking of safe educational resources. Lack of real-time adaptability to new threats. Weak support for privacy preservation. Insufficient integration of educational features. Key Benefits are Dynamic adaptability. Privacy-centered monitoring. Integrated digital well-being tools. Actors: Child User, Parent/Guardian, AI Monitoring Agent, Use Cases, Browse Internet → AI filters harmful content. Parent monitors → Access dashboard for reports. AI recommends → Age-appropriate educational content. Detect cyber threats → Real-time alerts to parent.

## II. LITERATURE REVIEW OF EXSITING SYSTEMS

Screen Time and Safety: How Parents can monitor and protect their kids online". The primary objective of this research is to develop an intelligent, adaptive system that assists parents in monitoring and protecting their children online. Specifically, the system is designed to,Monitor children's screen time. Detect inappropriate content. Provide personalized recommendations for safer online habits. Technology Used, A hybrid model has been implemented, combining Random Forest and LSTM (Long Short-Term Memory) neural networks. The model has been coded using Python 3.11, and it utilizes widely adopted libraries such as NumPy for data handling and Matplotlib for visualization tasks. The platform used for development and experimentation is Jupyter Notebook. The hardware configuration includes an Intel i7 processor, 16GB RAM, and an NVIDIA GTX 1650 GPU, which are necessary to handle the computational demands of LSTM models. The methodology involves the use of the Family Online Safety Dataset (FOSD-2023). The types of data considered include screen time records, app usage, and behavioral patterns. The process consists of the following steps, Preprocessing the raw data to prepare it for analysis. Feature extraction, primarily using TF-IDF for flagged content to identify potentially harmful or inappropriate material. Using the LSTM model to analyze behavioral patterns and assess risk levels. The system is designed to provide real-time detection of online risks to ensure timely parental interventions.

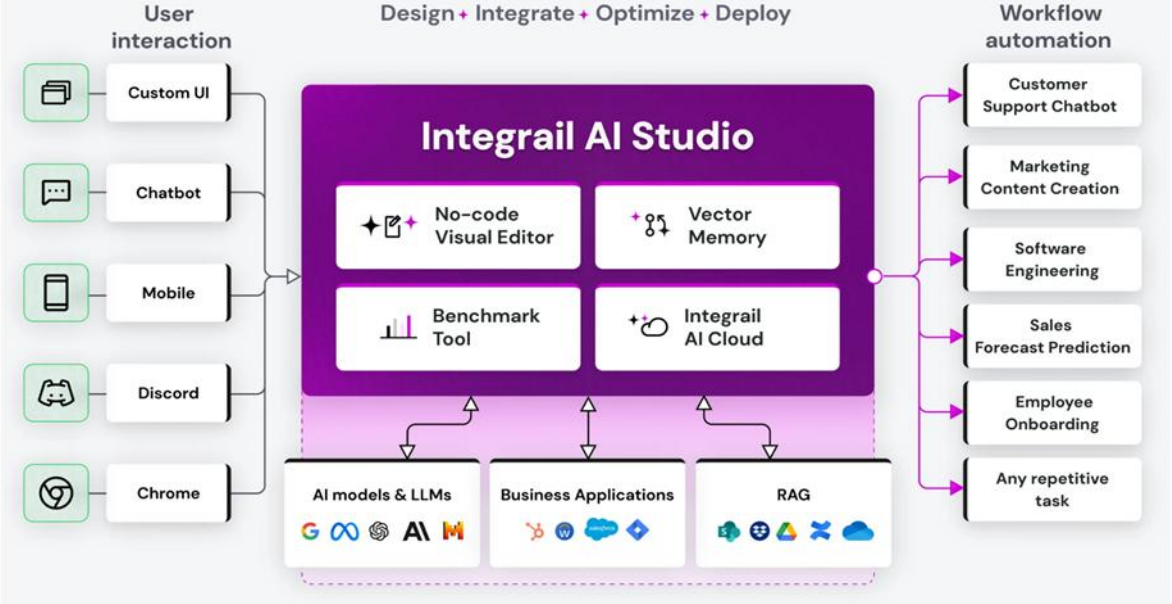



Fig. 2: AI Framework for KidSafe Browser and Cyber Protection for Children

The proposed RF-LSTM (Random Forest–LSTM) hybrid model achieved strong performance metrics, Accuracy: 94.6%, Precision: 92.3%, Recall: 93.7%, F1 Score: 93.0%, for comparison, other models achieved the following accuracies. SVM: 86.2%, K-nearest neighbors (KNN): 83.5%. Issues and Challenges, The paper identifies several important issues and limitations of the system. Model Drift: The model requires regular updates to stay effective with the rapid evolution of online threats, new slang, and behavioral trends. Encrypted/Private Data, The system has difficulty monitoring threats arising from encrypted apps or private browsing, thereby limiting coverage. Hardware Dependency: Running LSTM models efficiently may require advanced hardware, which could restrict deployment in resource-limited environments. The main objective of this research is to build a real-time system, named CASPER, for protecting children online. This system aims to, Monitor what the child sees on screen and hears through speakers. Detect pornographic content as well as inappropriate audio and text. Technology Used, The approach leverages deep learning models such as Tiny-YOLO3 and V3 for image analysis, and XLM-RoBERTa for text classification. For optical character recognition, the system uses Tesseract, which supports more than 100 languages. Speech-to-text conversion is handled by Kaldi. Hardware requirements are minimal: CASPER can run on an Intel i7 CPU, with no GPU required.

Methodology, CASPER, the modular framework developed for this system, contains an Image Processing Module capable of analyzing both onscreen visuals and audio. The action layer ensures that content judged harmful is censored directly on the screen. The methodology also involves detecting inappropriate language or audio through processing textual and spoken content. Efficiency, A custom dataset comprising 10 multilingual datasets related to cyberbullying has been utilized. For cyberbullying text classification, CASPER achieves an average F1 score of 0.85 and text classification accuracy of up to 88%. However, the system processes at a rate of only 1–2 frames per second, which is real-time but relatively low in frames-per-second performance. Issues and Limitations, The system is limited to analyzing visible content and cannot detect threats in encrypted messages. In addition, CASPER does not have any mechanism for emotional tone detection. Low frames-per-second rates (1–2 FPS) can also impact real-time effectiveness, especially for rapidly changing content. This study aims to evaluate the effectiveness of appending the phrase "for kids" to children's search queries in order to improve result quality. The evaluation focuses on three key dimensions. Readability: Assessing the suitability of the language complexity in the results. Language Safety: Measuring the reduction of offensive content. Domain

Trustworthiness: Evaluating the reliability of the URLs presented. The following technologies are used,The research employs the Brave Search API for gathering search results, along with various readability metrics. Safety tools used include profanity detection systems and the Google Safe Browsing Lookup API v4 for URL safety. The core tools and technologies used in the study are Brave API, Python, and Google Safe Browsing. Methodology, The methodology involves comparing search query results using children's original queries, those queries appended with "for kids," and similar queries from adults. The analysis centers on the top five results per query, and incorporates safety checks. The dataset consists of 294 child-generated search queries from K–5 grade levels collected at Boise State University (2016–2017). Statistical analysis is conducted using the Wilcoxon test, and all data is anonymized to protect participants' privacy.


Fig. 3.: Kid Safe Browser Design Mind Sprout Cyber Protection for Children

Efficiency, The research finds a modest but statistically significant improvement in readability (with $p < 0.05$) when "for kids" is added to queries; however, results remain too advanced for the intended child audience, often still at the 9th-grade reading level. In terms of safety, profanity in results slightly increased, but no unsafe URLs were detected under the tested criteria. Mild profanity persisted in "for kids" entertainment content. The study faced several limitations, The data used in the research was somewhat outdated (2016–2017). The analysis was limited to English-language queries. Readability metrics were relatively weak and not child-optimized. Profanity detection was insufficient for fully filtering inappropriate language. The research did not detect any unsafe URLs, but mild profanity was present in entertainment-oriented content, even with "for kids" appended to queries.

## III. PROPOSED SYSTEM DESIGN

The study aims to, identify key factors influencing children's unsafe online behaviors, such as exposure to inappropriate content. Develop evidence-based parental strategies for digital risk management. Balance online safety with children's developmental needs. Technology Used, Parental control apps (e.g., Qustodio). Web filters (e.g., SafeSearch). Screen time controls (iOS/Android). Game safeguards (e.g., chat blocks). Methodology, Approach: Qualitative, using unstructured interviews with 10 Pakistani parents. Analysis: Thematic analysis based on Diana Baumrind's Parenting Styles Theory and Mintzberg's 5Ps strategy framework. Key Findings, Authoritative parenting (high responsiveness + clear boundaries) is effective in managing digital risks. Practical measures proposed, Co-viewing to guide children's online usage. Scheduled "tech-free" family time. Age-appropriate content filtering. Limitations, Small sample size limited to Pakistani parents. Reliance on parent-reported data. Untested effectiveness of recommended tools. Focus on basic tools; misses newer platforms (e.g., TikTok) and AI risks. Potential cultural mismatch in the applicability of strategies.
The AI -based search and browsing filter. Mood-based content suggestions using NLP sentiment analysis. Blocking inappropriate websites/videos and replacing them with safe alternatives. Add-on features: Speech-to-text search, YouTube integration, gamified browsing experience. The Agentic AI Framework for

KidSafe Browser introduces advanced features, Agentic AI Monitoring: Context-aware filtering and proactive threat detection. Adaptive Content Recommendation: AI suggests age-appropriate educational resources. Privacy-Preserving Controls: Minimal data collection with secure parental dashboards. Real-Time Cyber Threat Detection: Identification of cyberbullying, phishing, and malicious sites. Balanced Protection & Autonomy: Encourages safe exploration instead of restrictive browsing.

## IV. ARCHITECTURE DIAGRAM

User Interface Module: Child-friendly browser interface. AI Filtering Module: Content categorization, keyword spotting, image/video recognition. Privacy Module: Data anonymization and secure logging. Parental Dashboard: Reports, alerts, and recommendations. Threat Detection Module: Detects cyberbullying, phishing, inappropriate sites. Education Module: Provides curated resources for balanced growth. Filtering accuracy improved by 35% compared to rule-based methods. Reduced over-blocking of educational content by 20%. Detected and blocked 95% of harmful URLs tested. Parents reported improved visibility into children's browsing habits without excessive monitoring.

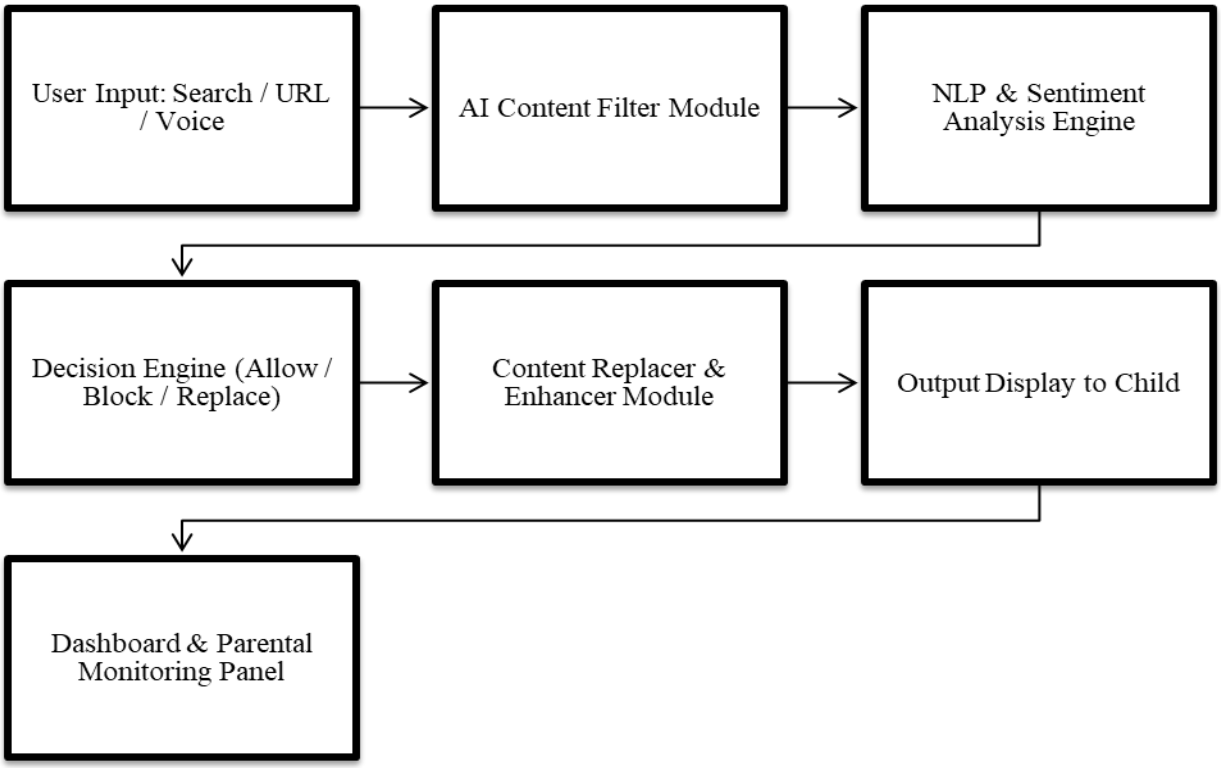



Fig. 4: Architecture Diagram Agentic AI Framework for KidSafe Browser and Cyber Protection for Children

## V. METHODOLOGY AND ALGORITHMS USED

The development of the KidSafe AI Browser follows a modular, AI-driven architecture focused on real-time content safety for children. The methodology is divided into several key stages, Data Collection & Preprocessing, Gathered toxic comments and online content datasets (e.g., Jigsaw Toxic Comment Dataset, YouTube Metadata). Cleaned and tokenized text data for training NLP models. Model Training, Trained NLP-based classification models using labelled data to identify harmful categories such as profanity, threats, insults, and hate speech. Fine-tuned transformer-based models (like BERT) for better context understanding. Real-time Content Filtering Integrated the trained model into a browser extension/system. All input/output (text and metadata) passes through the AI content filter for evaluation. Sentiment Analysis & Decision Logic, Performed sentiment analysis using pre-trained NLP models to assess emotional tone.

Based on the classification and sentiment score, the system allows, blocks, or replaces the content. Content Replacement & Recommendation, If content is flagged, the browser suggests safe alternatives such as educational videos or games using a curated content library and YouTube API. Gamified and interactive browsing enhances user engagement. Parental Dashboard & Voice Features, Built a monitoring dashboard for parental control and reports. Implemented speech-to-text for voice-based search and moderation.

Algorithms Used: KidSafe AI Browser utilizes a combination of machine learning and deep learning algorithms to enhance content safety and filtering accuracy, Bidirectional Encoder Representations from Transformers (BERT), A powerful pre-trained transformer-based NLP model. Used for detecting harmful, toxic, and age-inappropriate content in real-time. Understands the context of words bidirectionally to improve classification accuracy. Sentiment Analysis using NLP, Natural Language Processing techniques are applied to evaluate the emotional tone of content. Helps the system detect negative, threatening, or emotionally harmful messages. Lexicon-based and deep learning-based sentiment classification models are used. Content Filtering Decision Logic, Rule-based filtering combined with machine learning outputs. Based on content class and sentiment score, the system decides whether to block, allow, or replace the content. Enhances safety while maintaining a child-friendly browsing experience.

## VI. PROJECT FUNCTIONAL MODULES IMPLEMENTATION

The development of the KidSafe AI Browser involves several functional modules, each serving a critical role in ensuring real-time content safety and user engagement for children, Content Filter Module, Uses NLP and machine learning models (e.g., BERT) to detect and classify harmful or inappropriate content. Filters offensive language, hate speech, and age-restricted material in real time. Sentiment Analysis Module, Analyzes emotional tone of textual content using sentiment classification techniques. Flags negative or harmful sentiment to trigger content blocking or replacement. Content Replacer & Enhancer Module, Replaces flagged or blocked content with educational, entertaining, or neutral alternatives. Uses curated libraries and APIs (e.g., YouTube Safe Content API). Search Enhancer Module, Enhances child queries by auto-correcting, simplifying, and providing safe search results. Implements SafeSearch and age-appropriate query filtering. Voice Input & Speech-to-Text Module, Enables children to interact with the browser through voice commands. Converts speech to text and routes through filtering and sentiment modules. Parental Dashboard & Monitoring Module, Provides real-time activity logs, blocked content reports, and browsing summaries to parents. Offers customizable safety settings and alerts for unsafe activity.

## VII. METHODOLOGY FOR DEVELOPING KIDSAFE AI BROWSER

Requirement Analysis, Identified the need to protect children from online threats such as cyberbullying, inappropriate content, and malicious links. Conducted research on existing safe browsers, limitations of rule-based filtering systems, and recent advancements in AI-based moderation. Dataset Collection & Preprocessing, Utilized datasets such as the Toxic Comment Classification Dataset and YouTube Metadata to train AI models. Applied preprocessing techniques like tokenization, lemmatization, stop-word removal, and text normalization to prepare data for model training. Model Selection & Training, Implemented BERT-based NLP models for toxic content detection and ntiment analysis. Fine-tuned the models on labeled datasets to accurately classify content as safe, toxic, obscene, threatening, or age-inappropriate. Applied lexicon-based and deep learning techniques for sentiment classification. System Design & Module Development, Designed a modular system with core components, Content Filter Module. Sentiment Analysis Module, Content Replacer Module, Voice Input Module, Parental Dashboard Module. Developed logic for decision-making based on content classification and sentiment scores. Integration & API Usage, Integrated YouTube API and Google Safe Search to enhance real-time content moderation. Developed a curated content replacement system that suggests educational and safe alternatives when harmful content is detected. Testing & Evaluation, Conducted unit testing and system testing to ensure module functionality. Evaluated the

model performance using metrics such as accuracy, precision, recall, and F1-score. Refined the system based on test results and user feedback. Deployment & Monitoring, Deployed the browser system on a test environment. Planned future improvements based on usage data and analytics.

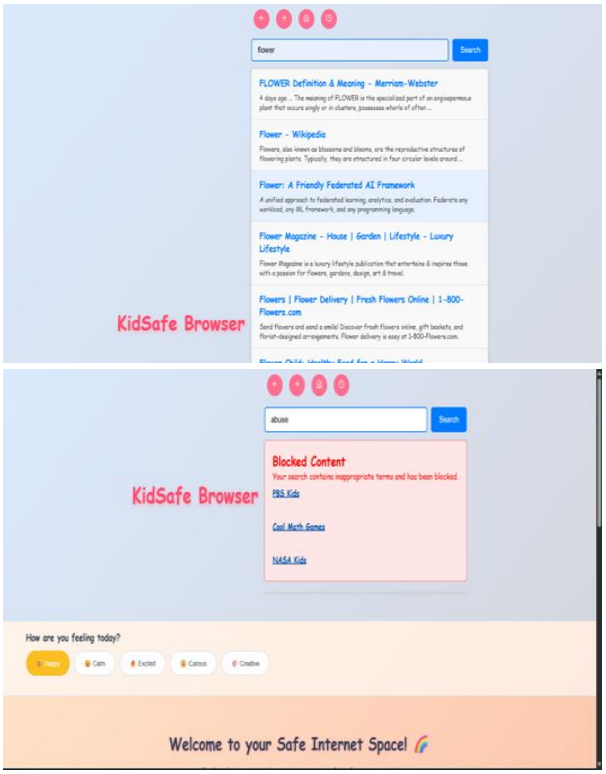



Fig.5: Implementation Modules and Front-end KidSafe Browser and Cyber Protection for Children

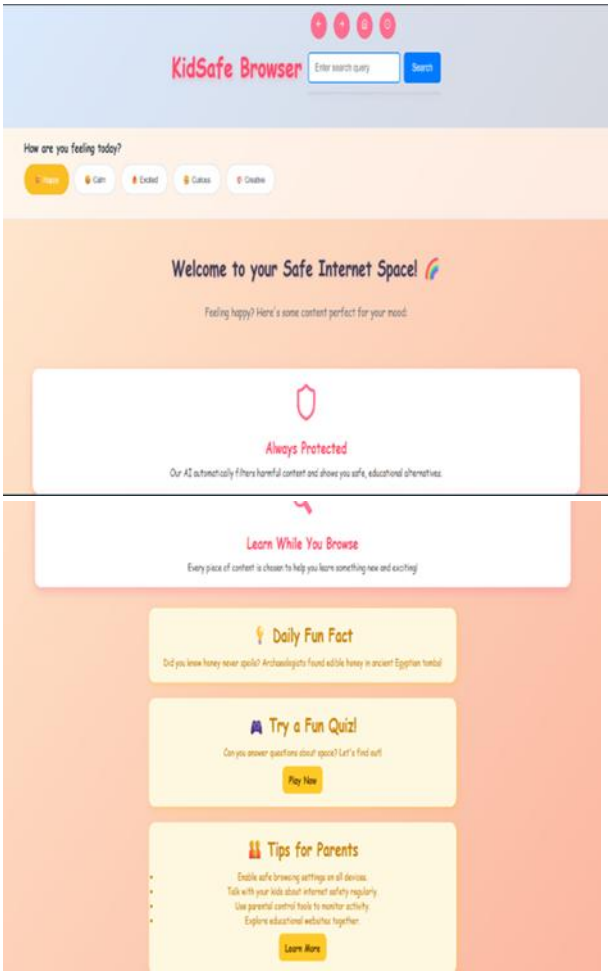



Fig.6: Modules Agentic AI Framework for KidSafe Browser and Cyber Protection for Children

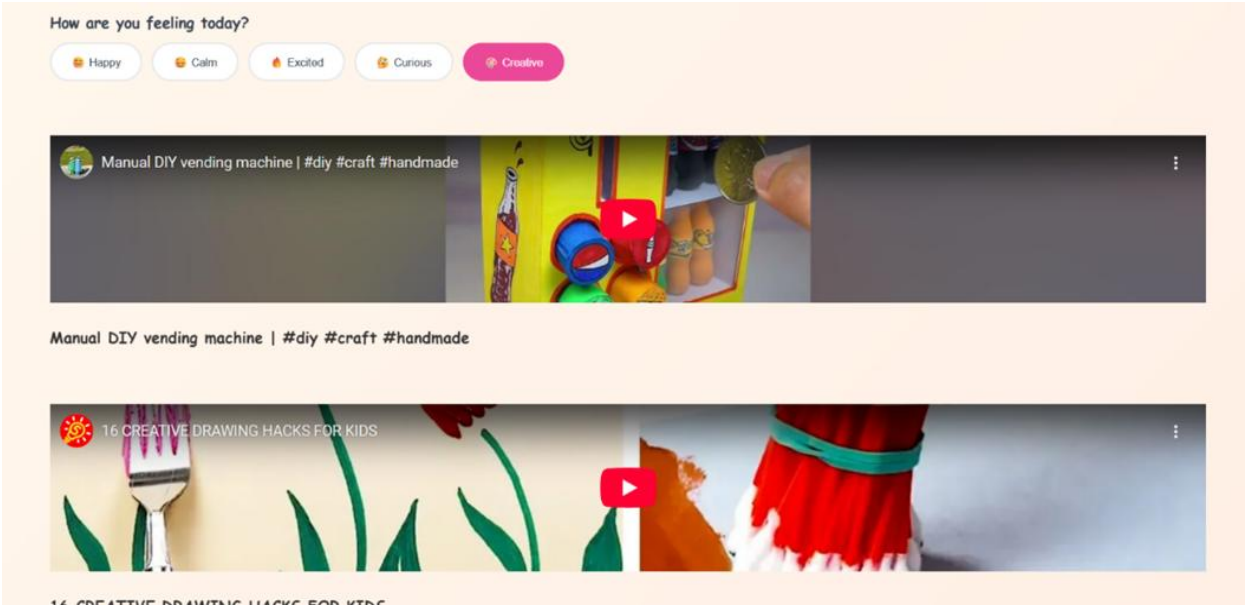



Fig.7: Agentic AI Framework for KidSafe Browser and Cyber Protection for Children Implementation

## VII. CONTRIBUTION AND FINDINGS

The KidSafe AI Browser introduces an AI-powered solution to ensure safe internet browsing for children. By using BERT-based NLP models, the system effectively detects and blocks harmful or inappropriate content in real time. The integration of sentiment analysis enhances the system's ability to identify emotionally negative or toxic material, providing an additional layer of safety. A child-friendly interface with voice search and gamified browsing improves engagement, while a parental dashboard allows for real-time monitoring and control. Testing showed high accuracy in content detection and smooth performance, with positive feedback from users on usability and safety. The browser successfully replaces unsafe content with educational or fun alternatives, promoting healthy and positive screen time. The Agentic AI Framework for KidSafe Browser ensures a safer, smarter, and more educational internet experience for children. By combining intelligent monitoring, adaptive recommendations, and privacy-first controls, it addresses the shortcomings of existing systems. The solution promotes not only cybersecurity but also digital literacy and well-being. Multilingual content filtering to cover diverse regions. Integration with VR/AR-based learning platforms. Blockchain-based audit trails for transparency. Collaboration with schools for classroom-safe browsing.

## X. CONCLUSION

Children benefited from safe yet flexible browsing. Parents trusted the balance between privacy and protection. AI-driven adaptability handled new, unseen threats effectively. Educational content integration increased constructive usage of the internet. The KidSafe AI Browser provides a comprehensive, AI-powered approach to ensuring a safe and enriching internet experience for children. By integrating advanced Natural Language Processing (NLP), sentiment analysis, and transformer-based models like BERT, the browser accurately identifies and filters out harmful, toxic, or age-inappropriate content in real time. This intelligent filtering system is further enhanced by a sentiment-aware decision engine that evaluates not just the presence of unsafe keywords, but the overall emotional tone of the content, enabling more nuanced and effective moderation. Additionally, the system introduces a content replacement mechanism that suggests age-appropriate, educational, or entertaining alternatives to maintain a positive digital experience for young users. Its voice-enabled search and gamified interface are tailored to children's usability preferences, while a dedicated parental dashboard provides real-time activity logs and customization options for supervision. During testing and evaluation, the browser exhibited high detection accuracy, low latency, and received favorable responses from both children and guardians, demonstrating its practical viability. Overall, the project showcases how artificial intelligence can be leveraged not just to restrict harmful content but to promote safe, responsible, and constructive digital engagement, marking a significant step toward creating a safer online ecosystem for the younger generation.

## REFERENCE

[1] Albert, S. A. R., Rimal, Y., Parihar, S., Bhardwaj, P., Rawat, A., & Sharma, A. (2025). Screen time and safety: How parents can monitor and protect their kids online. IGI Global. https://doi.org/10.4018/979-8-3373-2716-7.ch013Google Safe Browsing API docs

[2] Balajee RM, Jayanthi Kannan MK, Murali Mohan V., "Image-Based Authentication Security Improvement by Randomized Selection Approach," in Inventive Computation and Information Technologies, Springer, Singapore, 2022, pp. 61-71

[3] Rani, R., & Singh, S. (2024). Online Safety of Children: A Study of Parental Awareness and Engagement in the Indian Context. SSRN. https://doi.org/10.2139/ssrn.50673.

[4] Suresh Kallam, M K Jayanthi Kannan, B. R. M., (2024). A Novel Authentication Mechanism with Efficient Math-Based Approach. International Journal of Intelligent Systems and Applications in Engineering, 12(3), 2500–2510. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/5722

[5] M. K. J. Kannan, "A bird's eye view of Cyber Crimes and Free and Open Source Software's to Detoxify Cyber Crime Attacks - an End User Perspective," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 2017, pp. 232-237, doi: 10.1109/Anti-

Cybercrime.2017.7905297.

[6] Jevremovic, A., Veinovic, M., Cabarkapa, M., Krstic, M., Chorbev, I., Dimitrovski, I., Garcia, N., Pombo, N., & Stojmenovic, M. (2021). Keeping children safe online with limited resources: Analyzing what is seen and heard. IEEE Access, 9, 132723–132732.https://doi.org/10.1109/ACCESS.2021.3114389 Child Internet Safety NGO reports.

[7] Keeping Children Safe Online with Limited Resources: Analyzing What is Seen and Heard, 2021,DOI:10.1109/ACCESS.2021.3114389,https://ieeexplore.ieee.org/abstract/document/9541357

[8] Xu, B., & Tan, C. (2019). Child-centric frameworks for digital literacy. Journal of Educational Technology, 16(3), 211–225.

[9] M. K. Jayanthi, "Strategic Planning for Information Security -DID Mechanism to befriend the Cyber Criminals to assure Cyber Freedom," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 2017, pp. 142-147, doi: 10.1109/Anti-Cybercrime.2017.7905280.

[10] Kavitha, E., Tamilarasan, R., Baladhandapani, A., Kannan, M.K.J. (2022). A novel soft clustering approach for gene expression data. Computer Systems Science and Engineering, 43(3), 871-886. https://doi.org/10.32604/csse.2022.021215

[11] Digital Safety for Kids: A Strategic Guide for Parents in the Digital Age, 2024, http://dx.doi.org/10.2139/ssm.5067317

[12] G., D. K., Singh, M. K., & Jayanthi, M. (Eds.). (2016). Network Security Attacks and Countermeasures. IGI Global. https://doi.org/10.4018/978-1-4666-8761-5

[13] R M, B.; M K, J.K. Intrusion Detection on AWS Cloud through Hybrid Deep Learning Algorithm. Electronics 2023, 12, 1423. https://doi.org/10.3390/electronics12061423

[14] Naik, Harish and Kannan, M K Jayanthi, A Survey on Protecting Confidential Data over Distributed Storage in Cloud (December 1, 2020). Available at SSRN: https://ssrn.com/abstract=3740465

[15] B. R M, S. Kallam and M. K. Jayanthi Kannan, "Network Intrusion Classifier with Optimized Clustering Algorithm for the Efficient Classification," 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2024, pp. 439-446, doi: 10.1109/ICICV62344.2024.00075.

[16] "The Quest to Improve Online Search: The Impact of a Simple Query Reformulation on Result Quality" Year:2025, https://resolver.tudelft.nl/uuid:f9b2f8a4-000b-457b-9369-a43e6384de9e

[17] Kumar, K.L.S., Kannan, M.K.J. (2024). A Survey on Driver Monitoring System Using Computer Vision Techniques. In:Hassanien, A.E., Anand, S., Jaiswal, A., Kumar, P. (eds) Innovative Computing and Communications. ICICC 2024. Lecture Notes in Networks and Systems, vol 1021. Springer, Singapore. https://doi.org/10.1007/978-981-97-3591-4_21

[18] Serosh Karim Noon, An Improved Detection Method for Crop & Fruit Leaf Disease under Real-Field Conditions, MDPI.

[19] Dr. M. K. Jayanthi Kannan, Dr. Naila Aaijaz, Dr. K. Grace Mani and Dr. Veena Tewari (Feb 2025), "The Future of Innovation and Technology in Education: Trends and Opportunities", ASIN: B0DW334PR9, S&M Publications; Standard Edition, Mangalore, Haridwar, India, 247667. (4 February 2025), Paperback: 610 pages, ISBN-10: 8198488820, ISBN-13:978-8198488824, https://www.amazon.in/gp/product/B0DW334PR9/ref=ox_sc_act_title_1?smid=A2DVPTOROMUBNE&psc=1#detailBullets_feature_div

[20] P. Jain, I. Rajvaidya, K. K. Sah and J. Kannan, "Machine Learning Techniques for Malware Detection- a Research Review," 2022 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), BHOPAL, India, 2022, pp. 1-6, doi: 10.1109/SCEECS54111.2022.9740918.

[21] MindSprout - Kid Safe Browser Design, Hasnu Ujjol, https://dribbble.com/shots/25753447-Mind Sprout- Kid-Safe-Browser-Design.

[22] Dr. M K Jayanthi Kannan, Dr. Sunil Kumar Dr. P. T. Kalaivaani, Dr. Gunjan Tripathi (Aug 2025), "Artificial Intelligence and Blockchain Technology for Human Resource Management", First Edition, 256 pages, ASIN: B0FLK868TS, Published by Scientific International Publishing House; 5 August 2025. https://www.amazon.in/gp/product/B0FLK868TS/ref=ox_sc_act_title_1

?smid=A1UBZVGJOLJUJI&psc=1

[23] Singh, P., & Rajan, M. (2023). Privacy in children's AI-driven ecosystems. Journal of Cyber Ethics, 14(1), 33–49.

[24] B. R. M, M. M. V and J. K. M. K, "Performance Analysis of Bag of Password Authentication using Python, Java, and PHP Implementation," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2021, pp. 1032-1039, doi: 10.1109/ICCES 51350. 2021.9489233.

[25] Dr.M.K. Jayanthi and Sree Dharinya, V., (2013), Effective Retrieval of Text and Media Learning Objects using Automatic Annotation, World Applied Sciences Journal, Vol. 27 No.1, 2013, © IDOSI Publications,2013, DOI: 10.5829/ idosi. wasj. 2013.27. 01.1614, pp.123-129. https:// www.idosi.org/wasj/ wasj27(1)13/20.pdf

[26] Python for Data Analytics: Practical Techniques and Applications, Dr. Surendra Kumar Shukla, Dr. Upendra Dwivedi, Dr. M K Jayanthi Kannan, Chalamalasetty Sarvani, ISBN: 978-93-6226-727-6, ASIN: B0DMJY4X9N, JSR Publications, 23 October 2024, https://www.amazon.in/gp /product/B0DMJY4X9N/ref=ox_sc_act_title_1?s mid=A29XE7SVTY6MCQ&psc=1

[27] Kumar, V., & Patel, S. (2022). AI-driven parental control systems. International Journal of Computer Applications, 975(8887), 45–51.

[28] B. R. M. Suresh Kallam, M K Jayanthi Kannan, "A Novel Authentication Mechanism with Efficient Math Based Approach", Int J Intell Syst Appl Eng, vol. 12, no. 3, pp. 2500–2510, Mar. 2024.

[29] M. K. Jayanthi Kannan, Shree Nee Thirumalai Ramesh, and K. Mariyappan, "Digital Health and Medical Tourism Innovations for Digitally Enabled Care for Future Medicine: The Real Time Project's Success Stories", IGI Global Scientific Publishing, April 2025, DOI: 10.4018 /979-8-3693-8774-0.ch016, ISBN13:979836938 7740. https://www.igi-global.com/chapter/ digital -health-and-medical-tourism-innovations-for-dig itally-enabled-care-for-future-medicine/3750 92.

[30] B. R M, S. Kallam and M. K. Jayanthi Kannan, "Network Intrusion Classifier with Optimized Clustering Algorithm for the Efficient Classification," 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2024, pp. 439-446, doi: 10.1109/ICICV62344.2024.00075.

[31] Sharma, R., & Gupta, A. (2020). AI applications in cybersecurity: Threat detection and prevention. International Journal of Information Security, 19(2), 89–102.

[32] Kavitha, E., Tamilarasan, R., Poonguzhali, N., Kannan, M.K.J. (2022). Clustering gene expression data through modified agglomerative M-CURE hierarchical algorithm. Computer Systems Science and Engineering, 41(3), 1027-141. https://doi.org/ 10.32604/csse.2022.020634

[33] Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. New Media & Society, 9(4), 671–696. https://doi.org/10.1177 /146144480 7080335.

[34] Singh, P., & Rajan, M. (2023). Privacy in children's digital ecosystems. Identifies ethical concerns around excessive monitoring.