Journal of Computing Research and Innovation (JCRINN) Vol. 8 No.2 (2023)
https://jcrinn.com : eISSN: 2600-8793 / https://dx.doi.org/10.24191/jcrinn.v8i2.374

Empowering Online Safety: A Child-CyberCare Mobile App Approach to Inappropriate Content Filtering in Web Browsing

Ros Syamsul Hamid[1]*, Iman Hazwam Abd Halim[2], Muhammad Nabil Fikri Jamaluddin[3], Muhamad Arif Hashim[4], Nurfarah Hani Che Ismail[5]
[1,2,3,4,5] Kolej Pengajian Perkomputeran, Informatik dan Matematik
Universiti Teknologi MARA Perlis Branch, Arau Campus, 02600 Arau, Malaysia

*Corresponding author: * rossyamsul@uitm.edu.my*

Received Date: 6 June 2023
Accepted Date: 5 July 2023
Revised Date: 10 August 2023
Published Date: 1 September 2023

HIGHLIGHTS

- Adolescents and children are exposed to a broad spectrum of inappropriate and potentially harmful material due to the widespread availability of online content.
- This encompasses explicit content, hate speech, cyberbullying, and other forms of material that can exert negative impacts on mental well-being, cognitive growth, and overall online security.
- Lack of parental supervision and communication can increase children's internet addiction risk. With mobile devices being more essential, the importance of effective content filtering solutions is growing.
- The research project aims to create a mobile app-based strategy for boosting online safety by filtering inappropriate content during web browsing.

ABSTRACT

The use of smartphone and digital platform increased skyrocketed over the past decade. Due to generation gap between parent and children, youth internet addiction among early adolescents seems to be increasing. Internet addiction is more likely in children who feel unsupervised, have their privacy violated, or have poor parent-child relationships. Parental supervision, involvement, and meaningful connections reduce these risks and protect children from excessive internet use. Thus, this is the reason why a mobile app that can protect early adolescents is needed. This mobile app able to track online activity, detect unwanted keywords in Google searches, and receive pop-up alerts. The app's search history lets parents address concerns. SQLite manages keyword lists and search history efficiently. Usability testing and user feedback showed app effectiveness. Participating in their children's online activities teach responsible digital behaviour and creates a safe and supportive online environment. Future work entails enhancing cross-platform compatibility, refining content detection capabilities, and implementing cloud-based synchronization. Further, integrating advanced parental controls and comprehensive reporting mechanisms will fortify the app's ability to protect children's online experiences, positioning the Child-CyberCare app as a robust tool for ensuring digital safety for children.

Keywords: *web browsing filtering, inappropriate content, mobile app, online*

INTRODUCTION

The internet is an essential platform for information exchange, communication, and entertainment in today's digital landscape. However, users, particularly adolescents and children, are exposed to a wide range of inappropriate and potentially hazardous items due to the free availability of internet content. This includes sexual content, hate speech, cyberbullying, and other types of content that can have a negative influence on mental health, cognitive development, and general online security (Livingstone et al., 2017).

Maria Awaluddin et al, (2019), indicates that a lack of parental supervision and disconnection from parents can significantly increase the risk of internet addiction among children. According to Zhen et al. (2019), the usage of mobile phones has a remarkable acceleration worldwide over the past decade, offering unprecedented convenience in communication and unrestricted access to huge variety of online activities. The significance of maintaining a secure online environment, particularly for vulnerable users, has expanded significantly. With mobile devices becoming more prevalent in daily life, efficient content filtering solutions are becoming increasingly important. To address this concern, this research project aims to create a mobile application-based strategy to empowering online safety by filtering improper content when browsing the web.

While existing content filtering solutions have advanced, they frequently have limits in terms of accuracy, adaptability, and user-friendliness. Mobile applications offer a viable way to integrate content filtering into the surfing experience. This project intends to provide an efficient and user-centric system for protecting users from improper content by leveraging the characteristics of mobile devices, such as real-time processing, intuitive interfaces, and contextual awareness.

The primary objectives of this research endeavour are as follows: (1) to develop a mobile application that enables parents to ensure their children's Google search safety by detecting unwanted keywords, and (2) to evaluate the network performance, usability, and user acceptance of the mobile application functionally. By achieving these objectives, the envisioned mobile app seeks to provide users, particularly parents and guardians, with a powerful tool for ensuring the online safety of themselves and their dependents.

RELATED WORKS

A. Use of Mobile phone and Internet among Children

The widespread usage of mobile phones among children and their increasing access to the internet have raised concerns about their online safety and exposure to potential risks. Several studies have addressed this pressing issue, shedding light on the challenges and risks children face while using phones and accessing online content. In the study conducted by Abdullah et al. (2022), a survey was carried out to examine children's use of mobile phones. The findings revealed that a significant number of children possess the capability to access their parents' mobile devices and engage in various activities, such as gaming and web browsing. However, this unrestricted access raises concerns about potential exposure to inappropriate or harmful content.

Another study by Hazimah Wan Ismail et al. (2020) underscored the wide array of online and mobile activities that children partake in, signifying substantial risks if not subjected to vigilant supervision. The researchers emphasized the need for parental supervision to protect children from stumbling upon sexually explicit or harmful content.

Additionally, Stoilova et al. (2021) emphasized the importance of balancing potential risks with opportunities and promoting safe and responsible internet use for children. While existing research has explored various aspects of children's internet usage and risks, there is a notable gap in the development of a comprehensive mobile application that can address these concerns.
The current study aims to bridge this gap by developing a mobile application that provides parents with means to monitor and protect their children's online activities, ensuring a safer and more responsible digital environment for children.

B. Existing app – Kids Browser- Safe Search

Kids Browser-Safe Search is a mobile application designed to offer a secure browsing experience for children, aiming to protect them from accessing inappropriate content while allowing parents or guardians to monitor and control their online activities. The app features robust filtering and content blocking mechanisms, providing customizable parental controls for setting specific restrictions. Its simplified interface and age-appropriate content ensure ease of navigation for children, promoting a child-friendly online environment. Furthermore, Kids Browser-Safe Search prioritizes privacy and data security, safeguarding children's personal information. One of the app's strengths lies in its dedicated focus on child safety and protection, as it provides affective filtering and blocking features. Customizable parental controls empower parents to supervise their children's internet activities. Moreover, the app's emphasis on privacy ensures children's data remains secure.

However, there are notable issues that require attention. According to feedback from our recent survey, participants reported frequent app crashes and force closes, disrupted the browsing experience and caused frustration. Additionally, difficulties with account creatin and sign-in have limited some users' access to features. Another concern is related to the subscription model, with some users expressing dissatisfaction due to unclear communication about subscription fees before downloading the app. Addressing these issues is crucial to enhance the overall user experience and ensure user satisfaction with Kids-Browser-Safe Search. Transparent communication about subscription requirements and prompt resolution of account-related problems will contribute to an improvement in user experience.

METHODOLOGY

The mobile app for Child-CyberCare detailed in this paper consists of several elements, as depicted in Figure 1. The paper provides a visual representation of the project's logical framework, highlighting how the client and server components interact within the mobile application. For the app to function effectively, both the client and server components must have internet connectivity. The app is designed to be compatible with any device that operates on the Android operating system, ensuring broad accessibility. On the server side, the app employs Firebase Authentication for secure user verification and employs an SQLite database for streamlined data storage and retrieval.

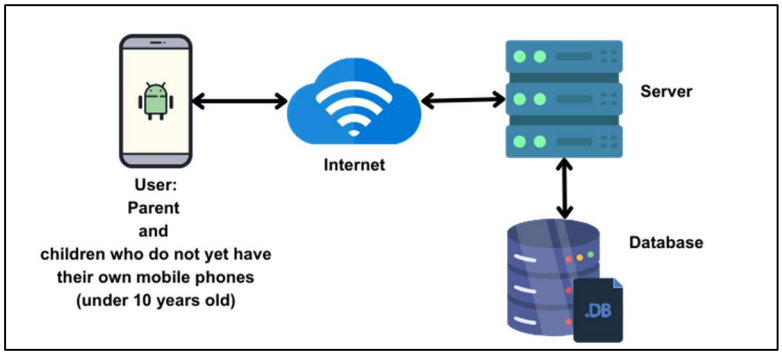

Figure 1: Logical Diagram of Child-CyberCare Mobile Application

The User Interface (UI) Design of the Child-CyberCare application centers around crafting an attractive and user-friendly encounter. Core screens, including login, registration, menu, keyword management, web search, and search history, are meticulously fashioned with usability and visual appeal as key considerations. The UI emphasizes simple navigation and incorporates visual aids such as screen prototypes to effectively illustrate the interface layout. Through the amalgamation of user-friendliness and visual allure, the UI Design enhances the holistic user experience, rendering the Child-CyberCare app user-friendly and captivating for parents seeking to ensure their children's online safety. Figure 2 illustrates the flow of screens and the design of the user interface for the Child-CyberCare Mobile Application.

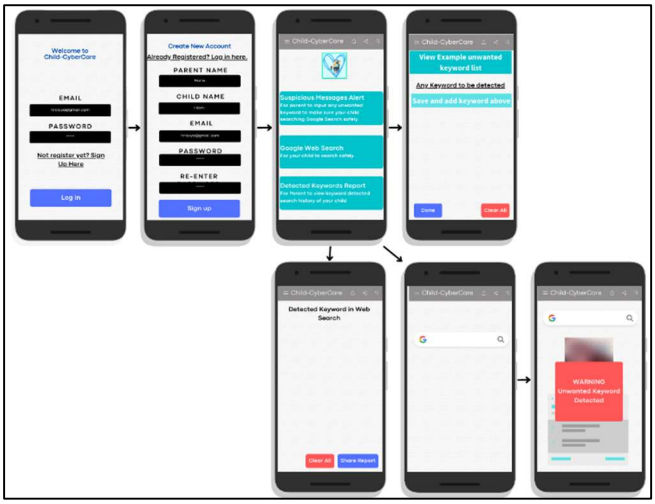

Figure 2: User Interface Design of Child-CyberCare Mobile Application

The Child-CyberCare application was integrated with a database for the purpose of retaining parent-specified keywords, detecting these keywords within Google Web searches, and subsequently presenting them in the Detected Keyword Report (Search History). The pivotal role of the Entity Relationship Diagram (ERD) lies in the development of the application's database structure illustrate in Figure 3, which encompasses four principal tables: Parent User, Child User, Keyword List, and Search History. Each entity within these tables possesses distinct attributes and associations.

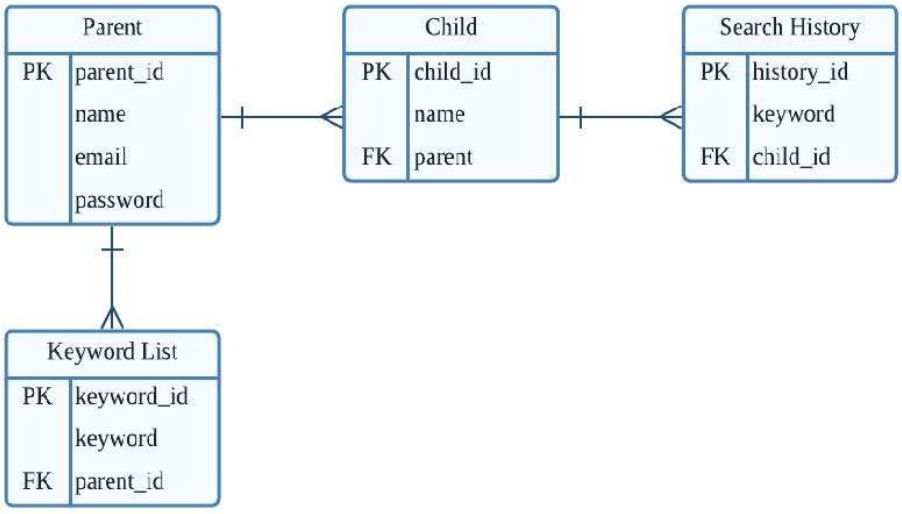

Figure 3: Entity Relationship Diagram of Child-CyberCare Mobile Application

The project employs Firebase Authentication as a safe means to manage user registration, login, and session handling. Registration can be completed by users using the Register Screen by inputting their email and password. The information is stored in Firebase utilizing encryption techniques to guarantee privacy and security. The password undergoes a safe hashing process, which enhances its level of protection. The act of logging out renders the user's authentication token invalid, hence requiring users to input their email and password on the Login Screen to verify their identity and log in again. Firebase Authentication streamlines the procedure, providing a user-friendly and secure user encounter, proficiently managing the intricacies of user authentication. Figure 4 shows the database table of Firebase Authentication.

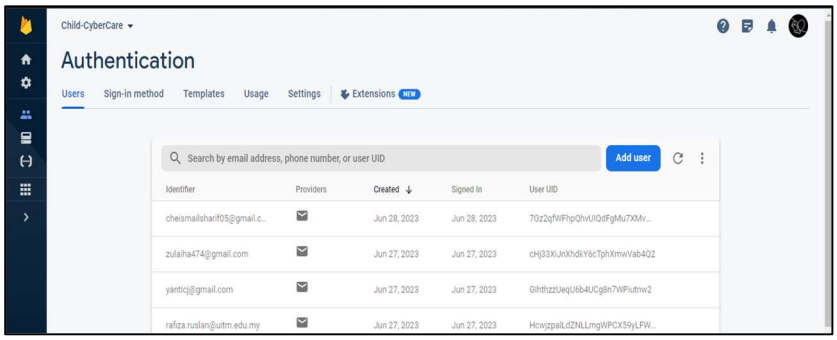

Figure 4: Firebase Authentication of Child-CyberCare Mobile Application.

The application employs two SQLite databases for the purpose of managing user data. The database named keyword_lists.db is responsible for storing keywords that have been added, updated, or removed by the user. On the other hand, the search_history.db database is utilized to retain the user's search history. The keywords managed by the user during their interaction with the application are saved within the keyword_lists.db database. Similarly, when a user initiates a search query and encounters a term that corresponds to any of the keywords stored in the keyword_lists.db database, the system proceeds to save this information in the search_history.db database. These databases effectively manage user data to ensure

a smooth and uninterrupted user experience. Figures 5 and 6 presented below depict the sample database developed for this application, utilizing SQLite.

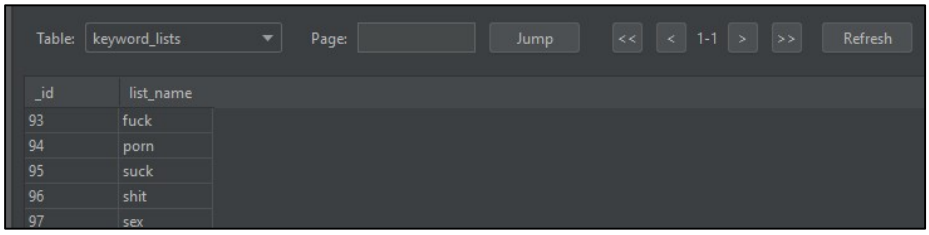

Figure 5: Database of keyword_lists.db

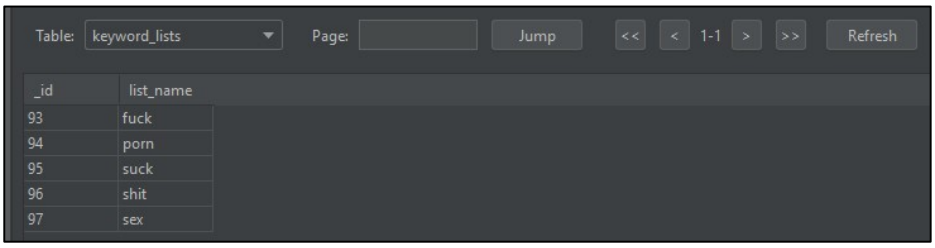

Figure 6: Database of search_history.db

The Child-CyberCare application is designed to bolster the online safety of children. It provides key features such as alerts for inappropriate keywords, child-friendly Google searches, and the capacity to review their search records. These tools empower parents to keep tabs on their child's online engagement and understand their habits, ensuring a safe and guarded online space for kids. To begin with the Child-CyberCare app, individuals just need to click its icon on their smartphones. This action will lead them to the login page, where they can either enter using their pre-existing email and password or select "Sign Up" to establish a fresh account. Once logged in or registered successfully, users will be presented with a main screen that outlines the app's capabilities and offers a video guide. They can initiate the app by pressing the "START" button. If required, users can also log off and sign into another account through the log-out feature on the main screen. This user-friendly design ensures swift and easy access to all the app's utilities. The registration and sign-in interface is depicted in Figure 7.

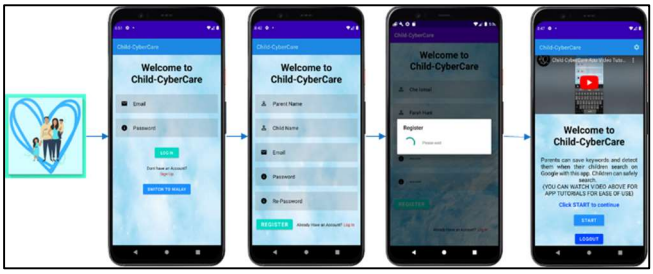

Figure 7: Registration and login screen.

The core functionalities of the Child-CyberCare app are crafted for ease of use and straightforward navigation. The interface contains three primary buttons: "Keywords Management," "Google Web Search," and "Detected Keywords Report." Parents have the flexibility to add, modify, or remove specific keywords they want to monitor when their child uses Google for searching. The "Google Web Search" function permits the child to conduct searches uninhibitedly, triggering an alert if any flagged keyword is used. The

"Detected Keywords Report" offers a compilation of identified keywords along with the times they were searched, with options to either erase the search history or share the report. The screen flow of the Child-CyberCare app is shown in Figure 8.

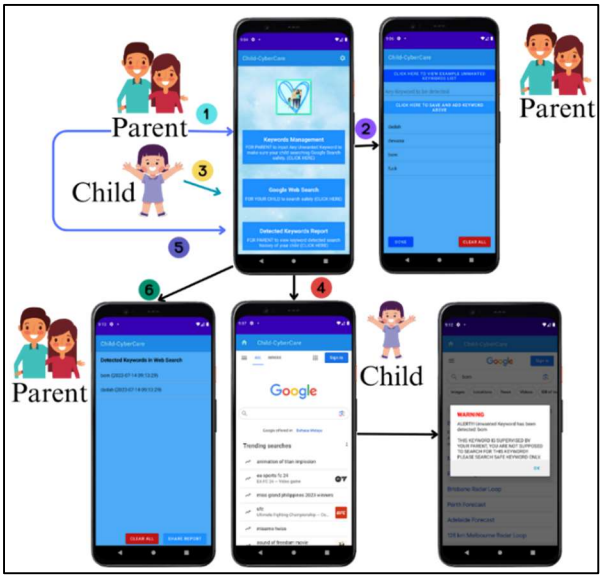

Figure 8: Screen Flow of Child-CyberCare Mobile Application

FINDINGS AND DISCUSSIONS

Functional Testing

As displayed in table I, the results from the functional testing highlight an exceptional performance, achieving a 100% success rate. Every test case was successful, confirming that the software aligns with its functional specifications. Such a high success rate reinforces trust in the app's operation and capabilities since it went through intensive examination with no major flaws identified. The meticulous design of the test cases played a pivotal role in reaching this favorable result, guaranteeing the software's proficiency in performing its designated functions.

Table 1: Functional Testing

Test Case ID	Functionality	Expected Result	Actual Result
F001	System registration	Successful login	Successful login
F002	Login with invalid ID	Error message shown	Error message
F003	Keyword management Add new keyword “porno” in the list	Keyword “porno” will be added to the list.	Keyword “porno” added to the list.

F004	Google web search (Search keyword not in restricted list)	Search result will be displayed.	Search result displayed.
F005	Detected Keywords Report	Produces logs of detected keywords	System successfully logs and displays detected keywords

The given data provides a clear insight into the results of functionality testing for five primary features or activities of mobile application. The data is presented by comparing the expected results against the actual results achieved during testing. Here's a detailed analysis: In the system registration, successful login was both expected and achieved. For login attempts with invalid IDs, the anticipated outcome of an error message upon successful login was met. Adding a new keyword, "porno," to the list was a success, aligning with the expected result. Similarly, when conducting a Google web search with a keyword not present in the restricted list, the system correctly displayed search results as anticipated. In terms of keyword detection, the system effectively fulfilled the expected objective by not only producing reports/logs of the detected keywords but also displaying them accurately. Overall, the testing verified the proper functioning of the system across these different scenarios.

Usability testing

Fifteen parents participated in usability testing, yielding largely favorable feedback. The respondents gave the app's user interface, simplicity, and visual attractiveness commendable evaluations. A significant number of users expressed clarity and comprehensibility regarding the icons and labels. Although a few encountered minor challenges while using the app, the general consensus was that the app's layout and responsiveness were adequate. The majority of parents were content with the app's performance and would recommend it to others. The overall average rating from the testing stood at 4.1 out of 5, indicative of a positive level of user contentment. The bar chart depicting the average scores for all the questions is displayed in Figure 9.

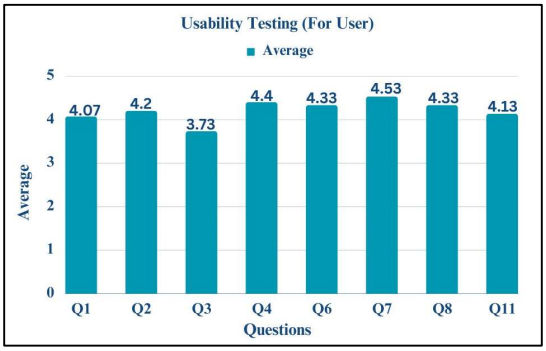

Figure 9: Usability Testing Result

User acceptance testing

As part of User Acceptance Testing, a team of five experts from Universiti Teknologi Mara Arau, Perlis, assessed the app's functionality. The app received praise for its design, user interface, and effective handling of undesirable keywords and harmful content. Technical reliability was mostly positive, despite minor glitches. Storing and retrieving data was valuable for parents. While some experts suggested improvements,

the overall agreement was that the app's technical performance met requirements of parents and children. The results of user acceptance testing are shown in Figure 10.

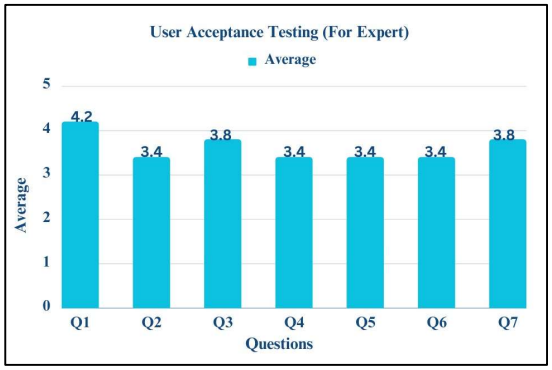

Figure 10: User Acceptance Testing Result

Network performance testing

The app's network performance was evaluated using the Android Studio Network Inspector, yielding valuable insights. Diverse API requests were scrutinized, and their corresponding responses were assessed. The outcomes of the tests revealed that a majority of the requests generated successful responses, denoted by "200" status codes, signifying proper processing. Notably, certain requests, such as the "search" query for the term "drug," elicited a "404" status code, indicating the deliberate blockage of the resource from view, which is beneficial. In totality, these examinations assist in pinpointing areas that can be optimized to ensure a more seamless and expeditious user experience within the Child-CyberCare application. The results from the Android Studio network inspector are visualized in Figure 11.

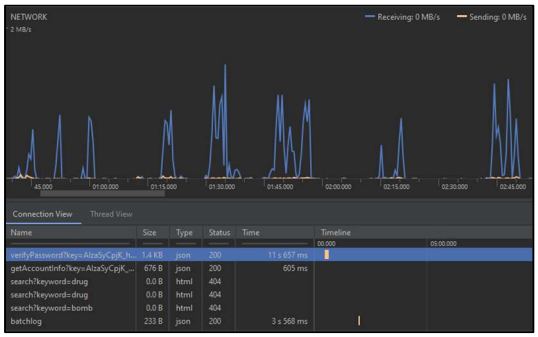

Figure 11: Network Inspector Testing Result

In the process of conducting network download tests via Apptim, the Child-CyberCare application displayed effective operational efficiency, boasting an average download size of 0.19 MB. The app adeptly manages data transfers over the network, leading to swift and seamless downloads for its users. There is no requirement for enhancements in terms of download speed and performance, as the app already exhibits proficient data transfer capabilities, ultimately enhancing the user experience. The finely tuned network download performance guarantees a smooth and proficient encounter for users when engaging with content within the application. The results from the network download testing are presented in Figure 12.

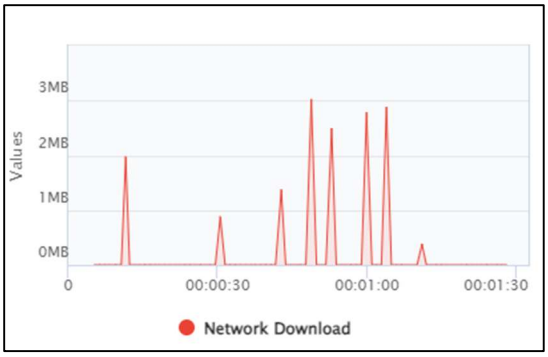

Figure 12: Network Download Testing Result

While conducting network upload tests through Apptim, the Child-CyberCare application exhibited proficient performance, boasting an average upload size of merely 0.01 MB. The app adeptly manages data uploads to the network, guaranteeing a seamless and expeditious sharing of data for its users. There's no necessity for enhancements concerning upload speed and performance, given that the app already showcases efficient data transfer capabilities during uploads. The fine-tuned network upload performance enhances the overall user experience by ensuring a smooth and efficient process of sharing information within the application. The outcomes from the network upload testing are visually represented in Figure 13.

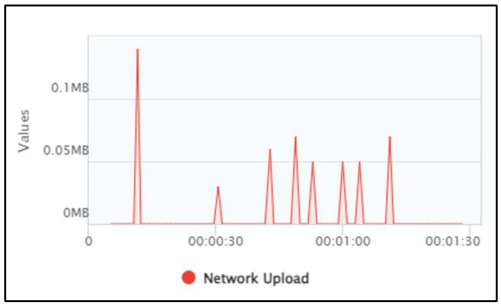

Figure 13: Network Upload Testing Result

CONCLUSION AND RECOMMENDATIONS

The project has successfully achieved its objectives by developing the Child-CyberCare app, which serves as a valuable tool for ensuring the online safety of young children. Through the app, parents can actively monitor their children's Google Search activities and effectively detect unwanted keywords, thereby safeguarding them from potential online risks. With its user-friendly interface and key features, the Child-CyberCare app empowers parents to actively engage in their children's digital lives and take proactive measures to create a safe and secure online environment for them. The application efficiently manages network data transmission, ensuring quick and uninterrupted downloads. With its proficient data transfer capabilities, the application enhances the user experience and doesn't require further enhancements in download speed and functionality. The carefully optimized network download performance guarantees seamless user interaction with the application's content. However, there are some limitations to address, like the app's current restriction to the Android platform and the need for better integration with external platforms.

To improve the app's functionality, it is recommended to work on cross-platform compatibility, enhance content detection capabilities, and implement cloud-based synchronization. Additionally, introducing advanced parental control features and comprehensive reporting mechanisms will empower parents to actively safeguard their children's online experiences. By incorporating these enhancements, the Child-CyberCare app can become a powerful tool in ensuring children's safety in the digital world.

FUNDING

The authors received no financial support for the research, authorship and publication of this article.

ACKNOWLEDGMENTS

The authors are grateful for the comments from reviewers in improving this manuscript. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CONFLICT OF INTEREST DISCLOSURE

The authors declared that they have no conflicts of interest to disclose.

REFERENCES

Abdullah, N. N., Mohamed, S., Abu Bakar, K., & Satari, N. (2022). The Influence of Sociodemographic Factors on Mobile Device Use among Young Children in Putrajaya, Malaysia. *Children*, *9*(2). https://doi.org/10.3390/children9020228

Hazimah Wan Ismail., W., Ramadhani Mohd Husny, H., Syahman bin Mamat, A., & Ya Abdullah, N. (2020). Parental Control System for Children on Wireless Network. *Journal of Computing Technologies and Creative Content*, *5*(1).

Livingstone, S., Ólafsson, K., Helsper, E. J., Lupiáñez-Villanueva, F., Veltri, G. A., & Folkvord, F. (2017). Maximizing Opportunities and Minimizing Risks for Children Online: The Role of Digital Skills in Emerging Strategies of Parental Mediation. *Journal of Communication*, *67*(1), 82–105. https://doi.org/10.1111/jcom.12277

Maria Awaluddin., Chan Y. Y., Norzawati Yoep., Faizah Paiwai., Noor Aliza Lodz., Eida Nurhadzdira Muhammad., Nur Azna Mahmud., Norazizah Ibrahim Wong., Noor Safiza Mohamad Nor., & Nik Rubiah Nik Abd Rashid. (2019). *The Association of Internet Addiction and Perceived Parental Protective Factors Among Malaysian Adolescents.* https://doi.org/10.1177/1010539519872642

Stoilova, M., Livingstone, S., & Khazbak, R. (2021). *Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes Media and Communications 3 INVESTIGATING RISKS AND OPPORTUNITIES FOR CHILDREN IN A DIGITAL WORLD: A RAPID REVIEW OF THE EVIDENCE ON CHILDREN'S INTERNET USE AND OUTCOMES*. www.unicef-irc.org@UNICEFInnocentifacebook.com/UnicefInnocenti

Zhen, R., Liu, R. De, Hong, W., & Zhou, X. (2019). How do interpersonal relationships relieve adolescents' problematic mobile phone use? The roles of loneliness and motivation to use mobile phones. *International Journal of Environmental Research and Public Health*, *16*(13). https://doi.org/10.3390/ijerph16132286