Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.159920
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Development of a Smartphone-Based Pornography-Related Domain Access Monitoring Application

Alhifny Wahid[1)], Litafira Syahadiyanti[2)*], Bondan Tiur Mahendra[3)]
[1,2,3)] Informatics Department, Universitas Dr. Soetomo, Surabaya, Indonesia
[1)]alhifnywahid@gmail.com, [2)]litafira@gmail.com, [3)]bm333936@gmail.com

Submitted :March 11, 2026 | **Accepted** : April 12, 2026 | **Published** : July 5, 2026

Abstract: The rapid growth of smartphone usage has increased access to various internet content, including pornography-related websites, particularly among adolescents. Existing solutions addressing this issue generally focus on psychological screening or access restriction through parental control systems, which either rely on subjective input or emphasize blocking mechanisms rather than providing insights into actual usage behavior. This study aims to develop MindSafe, a smartphone-based application for monitoring pornography-related domain access activity using a local VPN approach. The proposed system captures domain access activity in real time by intercepting DNS queries at the device level, classifies accessed domains using a blocklist-based approach, and records the results in a structured database. Unlike conventional parental control systems that focus on access restriction, this study introduces a monitoring-oriented approach that emphasizes real-time domain logging and statistical behavior visualization. The system was developed using Agile methodology and evaluated through functional testing and usability assessment. Functional testing confirms that all core features operate as expected. Usability evaluation using the System Usability Scale (SUS) involving 20 respondents resulted in an average score of 76.0, indicating acceptable usability. The results demonstrate that the system provides an objective and privacy-aware monitoring approach, offering a data-driven alternative to existing screening and blocking-based solutions.

Keywords: Mobile Development; Pornography Monitoring; Local VPN; Agile Development; Digital Behavior.

INTRODUCTION

The rapid growth of smartphone usage has significantly increased internet accessibility, particularly among adolescents who rely on mobile devices as their primary medium for digital interaction (Ma'ruf et al., 2024). This increased accessibility enables users to access a wide range of online content, including websites that may contain inappropriate or pornographic material (Tverdokhlib et al., 2025). The ease of access, combined with the private nature of smartphone usage, makes monitoring internet activity increasingly challenging.

Previous studies have primarily addressed pornography-related issues from a psychological perspective, focusing on addiction detection through screening instruments or intervention-based approaches (Muhammad et al., 2024). While these methods provide insights into user conditions, they rely heavily on subjective self-reporting and do not directly capture actual user behavior during internet usage. As a result, there is a limitation in obtaining objective and real-time data regarding how users access online content.

In contrast, a system-oriented approach can provide a more objective perspective by monitoring domain access activities on user devices (Lubis and Handayani, 2022). By focusing on domain-level information rather than webpage content, monitoring can be performed while preserving user privacy (Sim et al., 2024). This approach allows the system to record accessed domains, identify patterns of usage, and provide measurable indicators such as frequency of access and domain categories without involving intrusive content inspection (Silverman, 2023).

Existing solutions such as parental control applications and filtering systems generally emphasize blocking or restricting access to certain websites (Liberato et al., 2025). However, these systems often lack the capability to provide structured monitoring data that enables users to understand their own internet usage patterns (Akter et al., 2022). In addition, research specifically focusing on smartphone-based domain access monitoring using local VPN

* Litafira Syahadiyanti

e-ISSN : 2541-2019
p-ISSN : 2541-044X

mechanisms remains limited, particularly in the context of detecting pornography-related domains through a classification approach.

Based on this gap, this study proposes the development of a smartphone-based application capable of monitoring pornography-related domain access using a local VPN mechanism. The system detects domain access activity in real time, classifies domains based on predefined blocklists, and records monitoring data in a structured manner. The collected data is then presented as statistical information to support users in understanding their internet usage behavior.

The objectives of this study are: (1) To design and develop a smartphone-based domain access monitoring application using a local VPN mechanism; (2) To implement domain classification for pornography-related websites using a blocklist-based approach; (3) To present domain access activity in the form of statistical information to support understanding of internet usage patterns.

This study contributes to the development of a privacy-aware monitoring system that provides objective insights into domain access activity without diagnosing user behavior. The proposed application is intended as a monitoring tool to support data-driven understanding of internet usage rather than as a diagnostic or intervention system.

LITERATURE REVIEW

Research on pornography-related online behavior has generally been approached from psychological and behavioral perspectives, especially through exposure studies, risk screening, and intervention-oriented applications. Studies on adolescent exposure to pornographic content show that smartphones and social media increase the likelihood of repeated access due to ease of use, privacy, and continuous internet connectivity (Allison et al., 2024). This indicates that mobile devices are not only communication tools, but also major gateways for accessing sensitive online content, making objective monitoring mechanisms increasingly relevant in digital safety research (Meilani et al., 2023; Turvey et al., 2024). However, most of these studies emphasize behavioral impact and prevention strategies rather than technical monitoring of actual access activity on user devices.

Several previous studies have developed applications related to pornography problems, but many of them focus on self-assessment or intervention rather than direct monitoring. For example, mobile systems based on screening instruments are designed to identify the level of pornography-related risk using questionnaire responses, which depend on subjective user input and do not capture real access activity in real time (Muhammad et al., 2024). This creates an important gap between behavioral assessment and technical observation. In the context of information systems, a monitoring approach based on actual network activity can provide more objective evidence of user interaction with online domains than self-reported responses alone (Barata et al., 2023).

From a technical perspective, smartphone-based monitoring can be implemented through local VPN mechanisms that intercept domain requests at the device level without inspecting webpage content directly (Kohli et al., 2025). This architecture is relevant because it enables the application to capture domain-level traffic while maintaining a more privacy-aware approach than full packet inspection. In practice, such an approach is closely related to DNS or domain filtering systems, where accessed domains are identified and matched against predefined rules or domain lists (Rose et al., 2025). Compared with conventional filtering tools that primarily block access, a monitoring-oriented system focuses on logging, categorization, and statistical reporting of access activity. This distinction is important because the purpose of the present study is not to prevent all access automatically, but to provide structured information about pornography-related domain access patterns.

Related work in web filtering and parental control systems also shows that many existing solutions are designed around restriction, supervision, or safe browsing enforcement (Puvvadi, 2025). Although such systems are useful for content control, they often provide limited transparency regarding how access behavior is recorded, categorized, and analyzed from the user side. A domain-based monitoring architecture can therefore offer a different contribution by combining real-time detection, structured logging, and usage statistics in a mobile environment (Namrutha et al., 2025). This is particularly relevant for smartphone-based implementation, where lightweight monitoring is needed due to device resource limitations and privacy concerns.

Another important aspect in this area is blocklist-based classification. Instead of analyzing webpage content directly, blocklist-based approaches classify domain access by comparing observed domains with predefined categorized lists (Li et al., 2024). This approach is practical for mobile systems because it reduces processing complexity and supports near real-time decision making. However, its effectiveness depends on the quality, relevance, and maintenance of the blocklist used. Therefore, the use of categorized domain lists in a monitoring system should be accompanied by clear rules for classification and transparent reporting of detected domain categories.

Based on these previous studies, it can be seen that current literature still leaves a gap in the development of smartphone-based systems that specifically integrate local VPN monitoring, domain-level detection, blocklist-based classification, and structured statistical presentation for pornography-related access. Therefore, this study contributes by developing a smartphone-based monitoring application that emphasizes objective domain access

* Litafira Syahadiyanti

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.159920
e-ISSN : 2541-2019
p-ISSN : 2541-044X

recording, privacy-aware monitoring, and data-driven presentation of pornography-related access activity rather than psychological diagnosis or intervention.

METHOD

This study adopts a combined approach consisting of system development methodology and research evaluation methodology. The system development process follows an Agile approach to support iterative design and refinement, while the research methodology focuses on evaluating system functionality and usability.

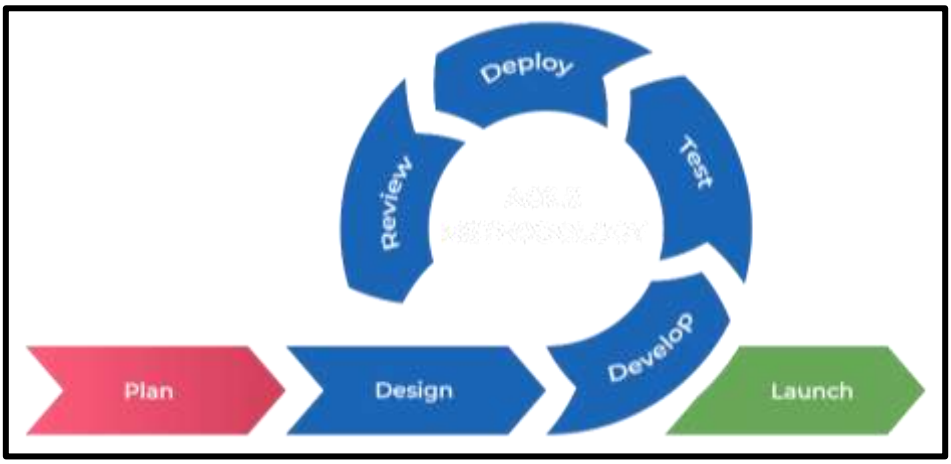

Fig. 1 Research Methodology with Agile Development

The system was developed using an Agile development model implemented in four iterative sprints, each lasting approximately two weeks. Each sprint focused on incremental feature development and evaluation to ensure that the system evolved based on testing results and feedback. In the first sprint, the main deliverable was the initial system prototype, including user authentication, basic user interface design, and integration with Firebase services. Feedback from this stage focused on usability of the login process and system accessibility, leading to improvements in interface clarity and authentication flow.

The second sprint focused on the implementation of the core monitoring functionality using a local VPN mechanism. The system was configured to capture DNS queries and extract domain names accessed by the user. At this stage, domain logging and local data storage were implemented. Feedback from testing identified issues related to monitoring stability and background execution, which were addressed by optimizing VPN service handling and improving data recording consistency.

The third sprint introduced domain classification and statistical visualization features. Domain classification was implemented using a blocklist-based approach, where detected domains were compared against predefined categorized domain lists representing pornography-related websites. The system was able to classify domains in real time and store categorized access data. The deliverable of this sprint included a statistics dashboard displaying domain access frequency and categorized usage. Feedback from this stage led to improvements in data visualization and refinement of classification rules.

The fourth sprint focused on system refinement and usability improvement. This included optimization of data synchronization between local storage and cloud services, enhancement of user interface elements, and preparation for usability evaluation. The final version of the system was stabilized for testing, ensuring that all core features—domain detection, classification, logging, and statistics presentation—functioned as expected.

From a research perspective, this study applies a functional evaluation and usability evaluation framework. Functional evaluation is conducted using a black-box testing approach to verify that system features operate according to expected input and output behavior. In addition to basic feature validation such as login, VPN activation, and data storage, testing also includes domain detection and classification scenarios, including detection of valid domains, handling of unmatched domains, and verification of classification results based on blocklist matching. These tests ensure that the system can consistently capture and process domain access activity under normal operating conditions.

Domain classification is implemented using a blocklist-based approach. The system compares domain names obtained from DNS queries with predefined categorized domain lists that represent pornography-related websites. The blocklists are managed within the system and can be updated by administrators to improve classification coverage. This approach enables real-time classification while maintaining user privacy, as only domain-level information is processed without accessing webpage content. However, the effectiveness of classification depends on the completeness and accuracy of the blocklist.

* Litafira Syahadiyanti

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.159920
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Usability evaluation is conducted using the System Usability Scale (SUS) method to measure user perception of the application. The evaluation involved 20 respondents consisting of adolescents aged approximately 13–18 years old, representing the intended target users of the system. Each respondent used the application before completing the SUS questionnaire, which consists of ten standardized statements measured using a five-point Likert scale. The SUS score is calculated using the standard formula, where responses to odd-numbered items are adjusted by subtracting one from the response value (score = response − 1), and responses to even-numbered items are adjusted by subtracting the response value from five (score = 5 − response). The adjusted scores are then summed and multiplied by 2.5 to obtain a final SUS score ranging from 0 to 100 (Manurung et al., 2024).

The evaluation framework in this study is limited to assessing functional correctness and usability. This study does not aim to diagnose user behavior, but rather to evaluate the effectiveness of the system in monitoring and presenting domain access activity in a structured and privacy-aware manner.

RESULT

This section presents the results of system implementation, domain monitoring performance, and system evaluation. The results are organized to demonstrate both the operational capability of the system and its evaluation outcomes.

System Implementation

The developed system was successfully implemented as an Android-based mobile application integrating user authentication, local VPN-based monitoring, domain classification, and statistical visualization. The application enables users to monitor domain access activity in real time, while maintaining a structured record of detected domains and their corresponding categories.

The login interface allows users to authenticate securely using a Google account, ensuring that access to the monitoring system is restricted to authorized users. After successful authentication, users are directed to the main dashboard, which provides a summary of monitoring results including total detected domains and categorized access activity.

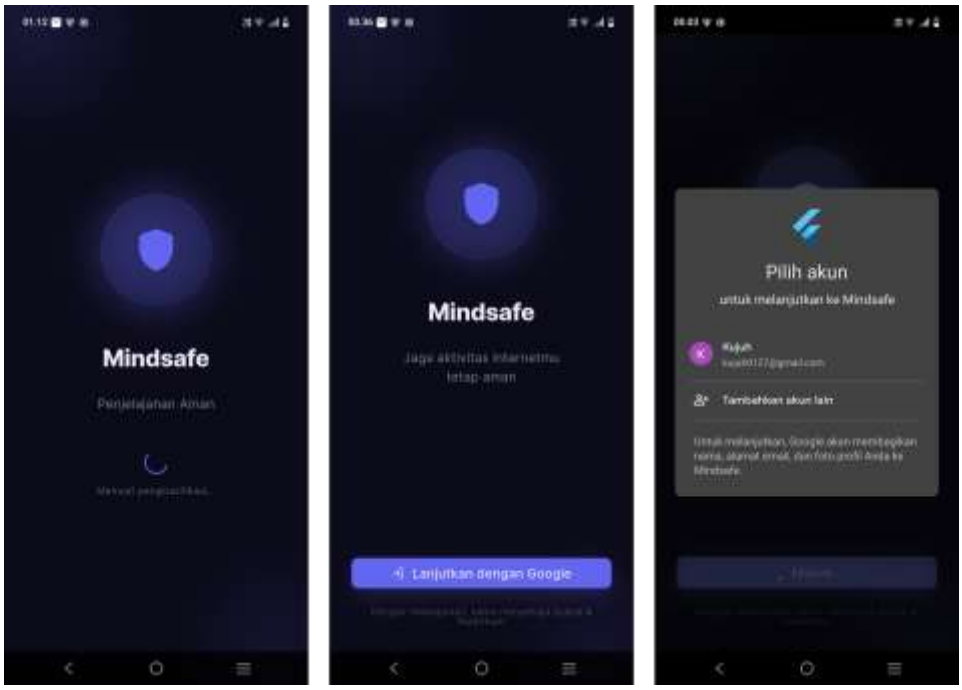

Fig. 2 Application Login Page View

* Litafira Syahadiyanti

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.159920
e-ISSN : 2541-2019
p-ISSN : 2541-044X

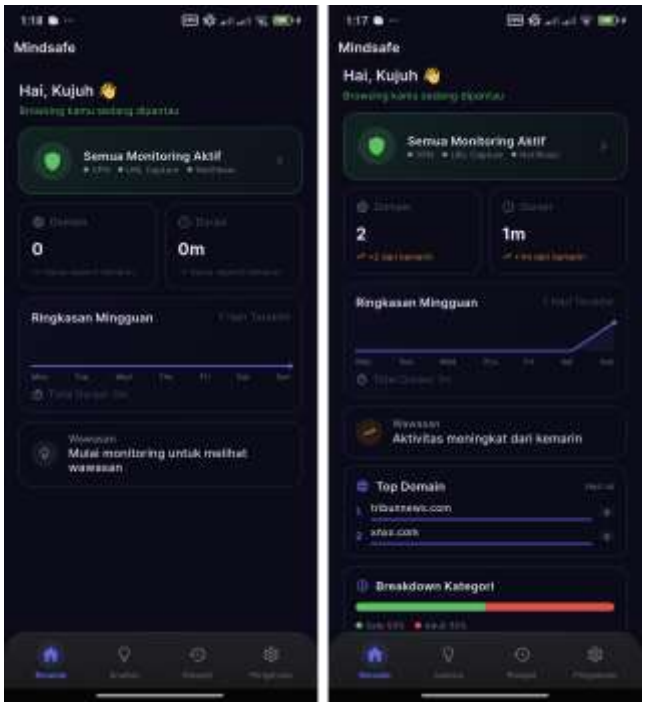

Fig. 3 Monitoring Dashboard Display

In addition to the dashboard, the system provides a statistics page that presents domain access data in graphical form. This page allows users to observe general usage patterns based on domain frequency and categorized distribution. The visualization supports users in understanding their internet activity without requiring detailed technical knowledge.

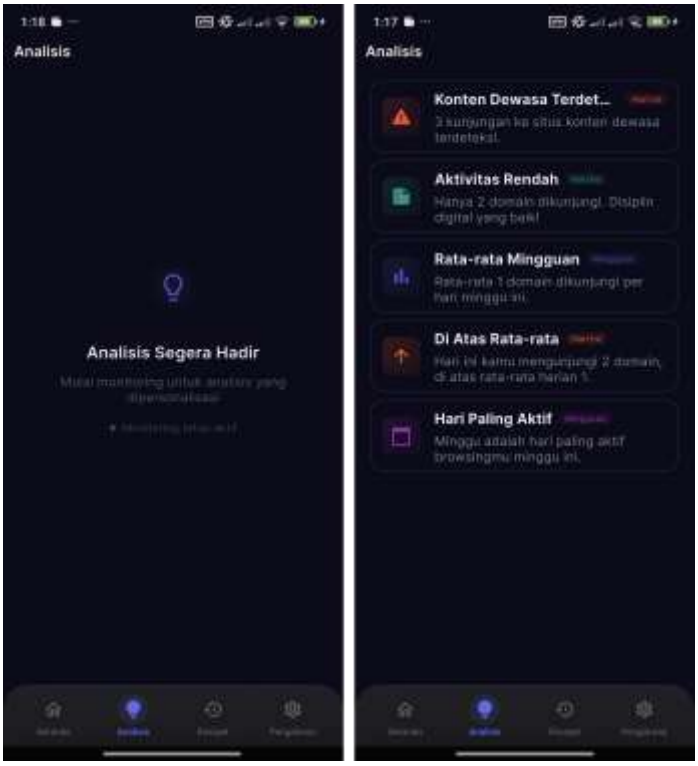

Fig. 4 Statistics Page Views

Domain Monitoring and Classification Results

* Litafira Syahadiyanti

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.159920
e-ISSN : 2541-2019
p-ISSN : 2541-044X

The system demonstrates the ability to capture domain access activity through a local VPN mechanism integrated into the mobile application. During operation, DNS queries generated from user browsing activity are intercepted and processed to extract domain names. These domain names are then recorded in the system database as monitoring data for further classification and analysis.

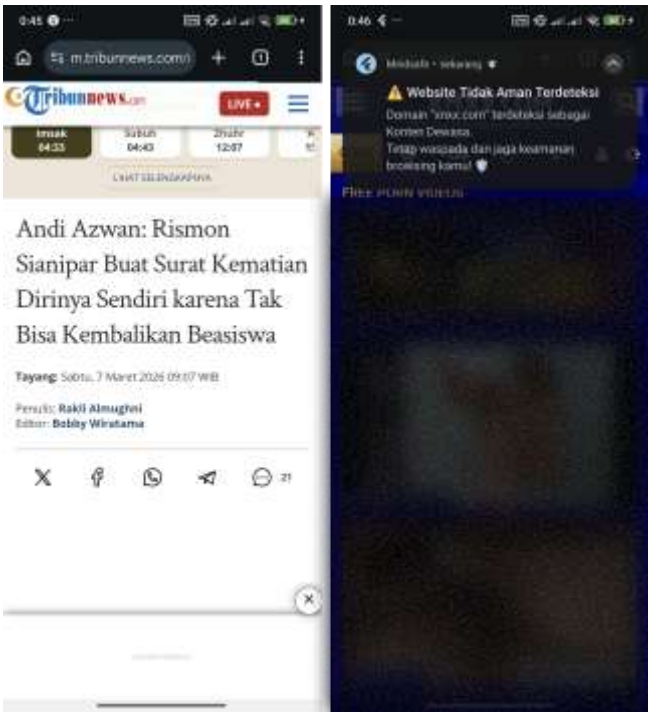

Fig. 5 Monitoring Process and Notification

The monitoring process operates continuously in the background, enabling real-time detection of accessed domains. When a user accesses a domain classified as safe, such as m.tribunnews.com, the system allows normal browsing activity without interruption. In contrast, when a domain identified as pornography-related, such as xnxx.com, is accessed, the system automatically triggers a real-time notification indicating that an unsafe website has been detected. This notification is displayed directly on the device without requiring the user to open the application, providing immediate feedback regarding potentially harmful content.

The classification process is performed by comparing detected domains with predefined blocklists representing pornography-related websites. Domains that match entries in the blocklist are categorized as adult content, while unmatched domains are classified as safe or general access. This approach enables real-time categorization without inspecting webpage content, ensuring that monitoring is performed in a privacy-aware manner.

* Litafira Syahadiyanti

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.159920
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Fig. 6 Monitoring Results Visualization

The monitoring results are further presented through a history page that provides both summary and detailed views of domain access activity. The summary view displays aggregated statistics, including daily activity graphs that differentiate between adult and safe domains, total usage duration, percentage of categorized content, and the most frequently accessed domains. For example, during testing, the system recorded a total usage duration of 58 seconds with an equal distribution between adult and safe domains, and identified the most frequently accessed domains based on visit count. During testing, multiple domain access events were successfully recorded, indicating that the system can operate continuously under real usage conditions.

The calendar view provides a temporal representation of monitoring data, allowing users to review domain access activity on specific dates. Detailed activity information includes the number of domains accessed and their classification into adult and safe categories. This structured presentation enables users to observe domain access patterns and frequency over time.

Overall, the results indicate that the system is capable of consistently detecting domain access activity, classifying domains in real time, and presenting monitoring results in a structured and interpretable format. The integration of real-time notification and historical data visualization supports users in understanding their browsing behavior while maintaining system operation without direct content inspection.

Functional Testing Results

Functional testing was conducted using the black-box testing approach to evaluate whether each system component operates according to its intended functionality. The testing covered core features including authentication, VPN activation, domain detection, classification, data storage, and statistical visualization.

The results show that all major system features operate successfully under normal conditions. Domain detection and classification processes function as expected, with the system able to capture DNS queries, match domains against blocklists, and store the results without errors. Additionally, the system maintains stable operation during monitoring, and no critical functional failures were observed during testing.

Table 1 Black Box Testing Results

No	Features	Test Scenario	Result
1	Authentication	Valid login	Success
2	VPN Monitoring	Activation	Success
3	Domain Detection	DNS query capture	Success
4	Domain Classification	Blocklist matching	Success
5	Data Storage	Activity logging	Success
6	Statistics	Data visualization	Success

Usability Evaluation Results

Usability evaluation was conducted using the SUS method involving 20 respondents. The target respondents of this study were students at the junior and senior high school levels (approximately 13–18 years old), in accordance

* Litafira Syahadiyanti

e-ISSN : 2541-2019
p-ISSN : 2541-044X

with the intended user group of the application. Each respondent interacted with the system and completed a standardized questionnaire consisting of ten statements measured using a five-point Likert scale.

The SUS score was calculated using the standard scoring method, resulting in an average score of 76.0. This score falls within the acceptable range and corresponds to a "Good" usability rating. The results indicate that the system is generally easy to use and understandable by users, with no significant usability barriers encountered during testing.

Table 3 SUS Respondent Report

No	Metric	Value
1	Target of respondents	13–18 years old
2	Number of respondents	20
3	Average SUS score	76.0
4	SUS grade	B
5	Adjective rating	Good

DISCUSSIONS

The implementation results indicate that the proposed system is capable of monitoring domain access activity in real time using a local VPN mechanism. Unlike approaches that rely on self-reported data or questionnaire-based assessment, the system provides objective monitoring by capturing actual domain access activity from the device. This allows the system to generate measurable data such as domain frequency and categorized access patterns, which can support a more data-driven understanding of internet usage behavior.

The domain classification mechanism based on blocklist matching demonstrates that real-time categorization can be achieved without inspecting webpage content. This approach provides a balance between monitoring capability and user privacy, as only domain-level information is processed. However, the effectiveness of this approach is influenced by the completeness and accuracy of the blocklist. Domains that are not included in the predefined list cannot be classified correctly, which may lead to incomplete categorization results. This limitation highlights the need for continuous blocklist updates or more advanced classification approaches in future work.

Compared to previous studies that focus on pornography-related behavior, most existing systems are based on psychological screening or intervention models. These systems typically rely on user input and are designed to assess addiction risk or provide behavioral support. In contrast, the system proposed in this study does not attempt to diagnose or intervene, but instead focuses on monitoring domain access activity objectively. This distinction is important because it shifts the approach from subjective evaluation to data-driven observation.

In comparison with parental control and web filtering systems, the proposed system differs in its primary objective and functionality. Conventional parental control systems are generally designed to restrict or block access to certain websites, emphasizing prevention and supervision. While effective for limiting exposure, these systems often provide limited visibility into user behavior beyond blocked or allowed access. In contrast, the system developed in this study emphasizes monitoring and logging rather than blocking. It records domain access activity and presents structured statistical information, allowing users to observe their own usage patterns. This provides an alternative perspective where users can gain insights into their behavior instead of relying solely on restriction mechanisms.

From a technical perspective, many filtering systems operate at the network or router level, whereas the proposed system operates directly on the smartphone using a local VPN mechanism. This enables domain detection to be performed at the device level without requiring external infrastructure. As a result, the system can function independently and provide personalized monitoring data for each user. However, this approach also introduces limitations related to device resource usage and dependency on VPN activation, which may affect long-term monitoring performance.

The functional testing results indicate that the system operates reliably under normal conditions, with all core features functioning as expected. The system is able to detect domain access, perform classification, and store monitoring data without critical errors. The usability evaluation results, with an average SUS score of 76.0, suggest that the application is generally acceptable and easy to use. This indicates that the system can be adopted by users without significant usability barriers.

Despite these findings, several limitations should be acknowledged. First, the evaluation is limited to functional correctness and usability, without quantitative measurement of classification accuracy such as false positive or false negative rates. Second, the monitoring capability depends on the quality of the blocklist used for classification. Third, the study does not evaluate long-term usage behavior or system performance under extended usage conditions. These limitations provide opportunities for future research to improve classification accuracy, incorporate adaptive or machine learning-based approaches, and conduct more comprehensive system evaluations.

* Litafira Syahadiyanti

Overall, the results demonstrate that a smartphone-based domain access monitoring system using a local VPN mechanism can provide a practical and privacy-aware approach to observing internet usage patterns. The system offers an alternative to traditional screening or blocking approaches by focusing on objective monitoring and structured data presentation.

CONCLUSION

This study developed a smartphone-based application for monitoring pornography-related domain access using a local VPN mechanism. The system is capable of detecting domain access activity in real time, classifying domains using a blocklist-based approach, and presenting monitoring results in the form of structured statistical information. Functional testing results indicate that the system operates according to its intended design, while usability evaluation using the SUS yielded an average score of 76.0, indicating that the application is generally acceptable and easy to use. These results demonstrate that the proposed system can effectively support objective monitoring of domain access activity without inspecting webpage content.

However, this study has several limitations. The domain classification process relies on predefined blocklists, which may affect classification completeness and accuracy. In addition, the evaluation is limited to functional testing and usability assessment, without quantitative analysis of classification performance such as false positive or false negative rates. Future research can address these limitations by improving classification methods, incorporating adaptive or machine learning-based approaches, and conducting more comprehensive evaluations, including long-term usage and performance analysis. Expanding platform support beyond Android devices may also enhance the applicability of the system.

REFERENCES

Akter, M., Godfrey, A. J., Kropczynski, J., Lipford, H. R., & Wisniewski, P. J. (2022). From parental control to joint family oversight: Can parents and teens manage mobile online safety and privacy as equals?. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW1), 1-28. https://doi.org/10.1145/3512904

Allison, K., Dawson, R. M., Messias, D. K. H., Culley, J. M., & Brown, N. (2024). Early adolescent online sexual risks on smartphones and social media: Parental awareness and protective practices. *The Journal of Early Adolescence*, *44*(7), 882-908. https://doi.org/10.1177/02724316231212560

Barata, J., Da Cunha, P. R., & De Figueiredo, A. D. (2023). Self-reporting Limitations in Information Systems Design Science Research: J. Barata et al. *Business & Information Systems Engineering*, *65*(2), 143-160. https://doi.org/10.1007/s12599-022-00782-8

Kohli, R., Gupta, S., & Gaur, M. S. (2025). Guarding Digital Privacy: Exploring User Profiling and Security Enhancements. *arXiv preprint arXiv:2504.07107*. https://doi.org/10.48550/arXiv.2504.07107

Li, W., Manickam, S., Chong, Y. W., Leng, W., & Nanda, P. (2024). A state-of-the-art review on phishing website detection techniques. *IEEE Access*, *12*, 187976-188012. https://doi.org/10.1109/ACCESS.2024.3514972

Liberato, M., Affinito, A., Meijerink, B., Jonker, M., Botta, A., & Sperotto, A. (2025). To Block Or Not To Block? Evaluating Parental Controls Across Routers, DNS Services, and Software. In *2025 9th Network Traffic Measurement and Analysis Conference (TMA)* (pp. 1-10). IEEE. https://doi.org/10.23919/TMA66427.2025.11096991

Lubis, M., & Handayani, D. O. D. (2022). The relationship of personal data protection towards internet addiction: Cyber crimes, pornography and reduced physical activity. *Procedia Computer Science*, *197*, 151-161. https://doi.org/10.1016/j.procs.2021.12.129

Manurung, R. Y., Krisbiantoro, D., & Utami, D. A. B. (2024). Usability Evaluation of Tokopedia Application Version 3.242 Using System Usability Scale (SUS) Method. *Sinkron: jurnal dan penelitian teknik informatika*, *8*(1), 366-374. https://doi.org/10.33395/sinkron.v9i1.13191

Ma'ruf, F., Pattiasina, P. J., Setiawati, R., Camerling, B. C. F., & Tuasela, P. E. (2024). The influence of social media usage, internet access, and mobile device penetration on social interaction quality among adolescents in Indonesia. *The Eastasouth Journal of Social Science and Humanities*, *1*(03), 106-119. https://doi.org/10.58812/esssh.v1i03.275

* Litafira Syahadiyanti

Meilani, N., Hariadi, S. S., & Haryadi, F. T. (2023). Social media and pornography access behavior among adolescents. *International journal of public health science*, *12*(2), 536-544. https://doi.org/10.11591/ijphs.v12i2.22513

Muhammad, R., Ardimansyah, M. I., & Wahyuningsih, Y. (2024). Mobile Applications for Self-Handle of Pornography Addiction. *Jurnal Nasional Pendidikan Teknik Informatika: JANAPATI*, *13*(1), 180-191. https://doi.org/10.23887/janapati.v13i1.71488.

Namrutha, M., Reddy, G. N., Akshaya, N., & Sreeraag, G. (2025, November). Parental Control System using ARP Spoofing. In *2025 Third International Conference on Emerging Applications of Material Science and Technology (ICEAMST)* (pp. 1105-1111). IEEE. https://doi.org/10.1109/ICEAMST67459.2025.11335963

Puvvadi, A. (2025). Using Recursive Resolvers for Parental Controls, Malware Filtering, and Enterprise Security. *Journal Of Engineering And Computer Sciences*, *4*(10), 94-102. https://doi.org/10.5281/zenodo.17368032

Rose, S., Liu, C., & Gibson, R. (2025). Secure Domain Name System (DNS) Deployment Guide. *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-81r3

Silverman, E. (2023). Organising obscenity: a three-part exploration into the architecture of adult sites from the western world, their intimate interactions and lusty language when searching for sex. https://doi.org/10.48730/k210-sc25

Sim, K., Heo, H., & Cho, H. (2024). Combating web tracking: analyzing web tracking technologies for user privacy. *Future Internet*, *16*(10), 363. https://doi.org/10.3390/fi16100363

Turvey, J., McKay, D., Kaur, S. T., Castree, N., Chang, S., & Lim, M. S. (2024). Exploring the feasibility and acceptability of technological interventions to prevent adolescents' exposure to online pornography: qualitative research. *JMIR Pediatrics and Parenting*, *7*, e58684. https://doi.org/10.2196/58684

Tverdokhlib, O., Vysotska, V., Nagachevska, O., Ushenko, Y., Uhryn, D., & Tomka, Y. (2025). Intelligent Processing Censoring Inappropriate Content in Images, News, Messages and Articles on Web Pages Based on Machine Learning. *International Journal of Image, Graphics and Signal Processing*, *17*(1), 107-164. https://doi.org/10.5815/ijigsp.2025.01.08

* Litafira Syahadiyanti