iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79719

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

PeekShield - Advanced Real Time Detection & Prevention System to Safeguard Against Unauthorized Screen Snooping & Visual Espionage

Erukonda Mohan Manoj[1], Punna Roshni[2], Pippalapalli Purushotham[3], N.Mounika[4]
Department of AI&DS, Methodist College of Engineering & Technology, Hyderabad, Telangana, India

Abstract: ***The common computer settings like personal computers and laptops are some of the sources where the control of access to age-inappropriate and restricted internet content has continued to challenge control especially among children and adolescents. The current parental control systems are based on predetermined rules, manual settings, or user verification, which narrows down their application in shared device cases and allows bypass, highlighting the importance of automated age-aware access control systems [1], [3]. The article presents a new version, PeekShield, an intelligent web filtering and screen protection framework, that combines artificial intelligence, computer vision, and proxy-based viewpoint system to provide adaptive control of content. The system uses real time detection and age estimations of faces to identify minor and adult users without specifics of logging in, using previously studied age-sensitive access control and biometric authentication [1], [3].A local age-checking service is dynamically applied to implement browsing policies through a man-in-the-middle proxy design, and is aligned with traditional secure web filtering designs [4], [6].Also, PeekShield has visual privacy by identifying and blocking unknown faces around the screen and automatically blurring screen content or locking down to stop shoulder surfing, as confirmed by screen privacy research [2], [5].In general, PeekShield offers a privacy-sensitive and scalable solution to the securement of shared computing environments.***

Keywords: ***Age-aware access control, Web content filtering, Computer vision, Screen privacy protection, Shared computing environments***

I. INTRODUCTION

The swift development of digital technologies has caused the intensive introduction of shared computing facilities at home, educational, and communal settings. There is a possibility of having many users who are of different ages and have different digital awareness levels on personal computers and laptops.

Although this mutual use enhances the availability of online data, education, and digital services, it also comes with a great challenge of security and safety. The problem with unintentional exposure of minors to inappropriate, harmful, or age-sensitive online media is one of the most severe issues and may negatively affect psychological, social, and developmental outcomes[7].

The traditional parental control and web filtering systems focus on alleviating these threats with the help of static rule-based filtering, user accounts, or access control mechanisms based on authentication. Nevertheless, these methods presuppose a steady user identification and discipline in the use habits which is most of the time not practical in shared-devices situations. People tend to switch without leaving their passwords, use others credentials, or bypass limitations in general, making these protection features unreliable and useless. This means that the current solutions do not offer continuous and context-sensitive protection especially in situations where devices are shared regularly and without supervision. Other than the control of digital content, another issue that has not been addressed is the physical privacy protection that is not offered in common areas. Any sensitive data shown on the screens, such as personal messages, financial data or restricted web material can be easily viewed by unauthorized parties, either by shoulder surfing or by chance viewing. Such breaches of privacy are possible even with software-level security countermeasures in place, which underscores a essential vulnerability in existing security models[8].

©IJRASET: All Rights are Reserved

II. ARCHITECTURE

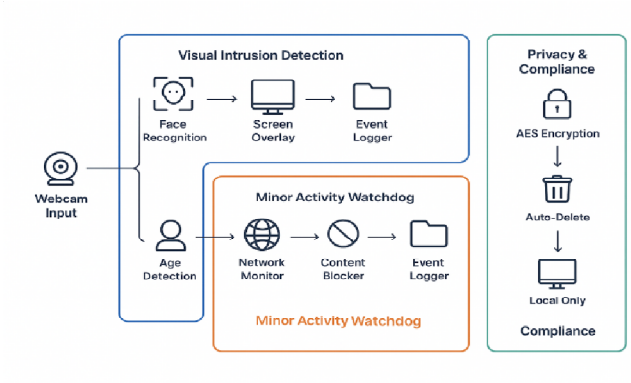


Fig: Architecture of PeekShield

Within the PeekShield architecture, system information and sensor feeds are run by an automated and structured security pipeline, which is used to secure common computing infrastructure. All the work initiates with the ongoing video stream (obtained by the device web camera) and system browser history and access logs. These are sent to a preprocessing layer where the visual information is purged, standardized and then arranged to be intelligently analyzed. The face detecting process is used to isolate active users and also irrelevant frames or the background noise is filtered to enhance better detection. After the preprocessing, the visual information is processed with an artificial intelligence-based age estimation model. The model is used to extract the features of a face and approximate age of the face is estimated which can be classified into minor or adults. The resultant classification of the user is treated by a local age service module that holds the existing access state without explicit authentication and manual selection of profile. Such dynamic identification of users enables PeekShield to be dynamically adjusted to user change. On the basis of classified user category, the system imposes access control policies on the network layer using a proxy-based interception mechanism. Intrusion is detected on web traffic and requests to blocked or age-related web sites are blocked before the browser can access the content. Any system decisions and events or any enforcement can be sent over to some interactive dashboard which serves as a visualization and monitoring interface. The live user classification status, block attentions, and screen privacy events are cleared in the dashboard, and this enables the administrators or guardians to have a clear view of how the system is acting. Logs and summary reports can be checked and sent out to be audited and analyzed. With such an integrated architecture, PeekShield is able to provide automated, adaptive and privacy conscious protection to shared devices with smooth user experience.

III. RELATED WORK

TheStudies to guard users in common digital spaces have also increased in fields like content moderation, protection of children online and protection of visual privacy. Regardless of such advancement, the majority of current solutions consider these issues individually instead of fixing them using a single protection approach. Isolated mechanisms can be ineffective when using the same system by different users in different times and locations, i. e. shared-device situation. This disaggregation amplifies the security and privacy risk, especially when there is dynamism in the roles of users, or when there is co-existence of digital and physical threats. This leads to the increasing necessity of context-sensitive and automatic frameworks of integration, such that they can respond to user specifics alongside the environmental conditions.

Context-based access control has been extensively researched specifically regarding the limitation of this method within shared computer systems. Wisniewski et al. [9] critically analyze popular parental control technologies and see a primary fault in their design assumptions and behavior patterns of use in the real world. The vast majority of parental control systems presuppose that there are one-to-one user accounts, age profiles, or age-on-board, adult control. But in real comics interactive environments, children and adults will often interchange the computer without the need to log in, change profiles or express themselves explicitly. Due to this fact, account based access control mechanisms become useless or can be easily circumvented. In addition to these structural constraints, the problem of usability also makes manual parental control systems less effective. Wisniewski et al. [9] note that the process of setting up and proper control policy maintenance is a long-term effort with complex technical skills and consciousness of the caregivers. With time, such requirements cause improperly configured settings, old restrictions or intentional evasions of the users.

These disadvantages are especially pronounced in places where users turnover rates are very high, such as schools, libraries, and agents that provide access to the public, where access control cannot be, or are not, done based on identities.

The authors hence attach relevance to adaptive mechanisms which will respond to real time context as opposed to using predetermined rules. The further improvement of computer vision turned age estimation into a potential alternative to the conventional access control based on authentication. As Levi and Hassner [10] show, deep learning models are capable of effective age and gender prediction of face images obtained in an uncontrolled environment and subject to changes in lighting, facial expression, and pose. They demonstrate that current convolutional neural networks can identify features of age with high precision and speed to provide support in real-time. Notably, they emphasize that not all security and access control are the situations where an exact age forecast is necessary. Rather than that, crudely classified age like that between a minor and an adult is usually enough to give the context of the decision-making.The latter may especially apply to a shared-device setting, where the need to authenticate users or self-claim their age causes friction and heightens the chances of policy abuse. Based on this observation, PeekShield takes age estimation as part of its enforcement logic. Instead of age prediction as a derivative of analysis, the system applies the predicted age category as a control signal that is continuously adjusted in real-time and either enablest/disables network-level access policy. Through its close association of perception and enforcement, PeekShield builds on earlier studies by making age estimation an operational and automated security solution. Along with exposure to digital content, threats of physical observation are a serious but a frequently unaddressed issue of privacy risk. Shoulder surfing, in which sensitive information on the screen is noticed and vicinity people look at it without permission has continued to increase in public and shared settings. Eiband et al. [11] explore this question and prove that, in most cases, breaches of privacy occur due to passive visual inspection more than technical violation. According to their results, users do not tend to take into account potential observers in their vicinity, even in such places as a classroom, an office, a library, and a transportation hub. In the authors, they complain that attentiveness of the user is not enough to alleviate the risks to visual privacy since the users are often concerned with what they are doing. They should be used to solve this shortcoming by introducing automated systems that can identify risky visual states and react without any user instructions. PeekShield is no exception as it keeps scanning the physical environment with live face recognition of the device it attaches to. The system automatically takes relevant measures to protect the visual privacy by blurring the screen or locking up when unfamiliar or unauthorized faces are identified in the area of display thus forming a continuous shield to the visual privacy of the user. One of the common themes of the previous studies is the insufficiency of one-layered defense. The solutions where the content filtering is applied only or the screen-level privacy controls are present frequently introduce vulnerabilities to the security software systems when one role is altered or when the digital and physical threats co-exist. Peak Shield tackles these constraints by enforcing on the network with continuous visual and immediate monitoring. Through proxy-based access control prior to being rendered and combining it with automatic screen protection, the solution provides a fully integrated, customisable and user orientated solution that moves the protection of shared computing environments to a new level.

IV. METHODOLOGY

ThePeekShield system is intended to be a complete, robotic security model that should safeguard shared computing systems against inappropriate content encountering and also a threat of visual confidentiality. The methodology assumes a modular and layers architecture, which combines artificial intelligence, computer vision, and network level cybersecurity controls. With this organized method, proper classifications of the users are achievable, access policies are enforced with great accuracy, and constant monitoring is realized by ensuring fewer users need to engage in the process. The design has also been focused on adaptability, scalability, and preservation of privacy and, therefore, is applicable in varied shared-device settings, e.g., homes, educational institutions, and a public access system.

PeekShield adheres to a processing pipeline that consists of multiple components that can have a specific functionality and contribute to the final security goal. The following are some of the main modules that form the system architecture:

- Detection of users and estimation of age.
- Local Age Checking and Local Policy Management.
- Web Filtering and Enforcement Proxy-Based.
- Monitoring and Protection of thescreen privacy.
- Financial Overview Interface and System Monitoring Interface.

These modules are coordinated with little to no context exchange in order to keep the system efficient and minimize system overhead.

The modular architecture enables the specific components to be revised or replaced and the overall system functionality is not impacted, akin to current adaptive security architecture [7].

A. *Detection of users and estimation of age*

The initial step of PeekShield pipeline is on detection of presence of users before the device. A web camera constantly captures video images and these images are processed through the face detecting algorithm to recognize active users. After face detection, an age estimation model that makes use of deep learning is implemented to determine the range of the age of the user. Depending on preset limits, the user is dynamically labeled as a minor or an adult.

Let an input video frame be represented as: $I_t \in R^{H \times W \times 3}$

A face detection function F_d maps the image to bounding boxes: $B_t = F_d(I_t)$ where,

$B_t = \{(x_i, y_i, w_i, h_i)\}_{i=1}^{N}$

- N = number of detected faces
- (x_i, y_i, w_i, h_i)= bounding box of face i

This age-based classification is not based on any of the login credentials or selecting the profiles manually which in most cases is not a reliable method in any shared-device setting. The system does not save raw images or biometric data to ensure privacy and only the calculated age category is saved temporarily in order to enforce the policy.

Local Age Verification and Policy Management The approximated age group that the computer vision component produces is handled by a special local age verification and policy management service which is the decision making unit of the PeekShield system. This service has the role of interpreting the result of age classification, and converting this result to meaningful access control actions of the result of the age classification according to predefined security policies. Instead of using multiple user accounts or manually setting up their policies, the system assigns each identified user to a suitable policy, mirroring the adults can unlimited access to applications, a more restricted access to applications by minors, or outright blocking of content unacceptable to elderly children.

The policy management service keeps the prevailing user context constantly up to date by listening to real-time updates of the face detector and age estimator modules. When the user presence has changed by detecting the entry of another person into the vicinity or the presence of several users is detected, the service automatically re-evaluates the active policy and adjusts the enforcement rules accordingly.

Using a predefined age threshold T (e.g., 18 years):

$C_i = \{\text{Minor}, a^i < T \ \text{Adult}, a^i \geq T\}$

Only the **class label C_i** is retained, ensuring privacy preservation.

is stored, so access control guarantees content secrecy.Access control is done so that the content secrecy remains intact even in areas where users often change, like family devices, classrooms, and access terminals.

The age verification and policy management service reduces the time taken to respond when utilizing solely the local system, implying that it can ensure real-time policy enforcement. On-premises execution also helps avoid the dependency on external cloud-based services, which means that the network delay, service outages, or the collection of data by third parties are minimized. The design decision is robust in protecting privacy since the sensitive biometric data, including facial scan or age approximations, are processed and stored outright in the device. Altogether, the responsive, privacy-appropriate, and context-reliant protection of PeekShield is made possible, due to the dynamic and locally controlled policy framework, which responds to the realities of the shared-device usage.

B. *Web Filtering and Enforcement Proxy-Based*

PeekShield uses a man-in-the-middle (MITM) proxy framework which puts web access control directly into the network layer and this allows implementing centralized and application-free policy enforcement. All outgoing Internet requests that are generated by the system are transparently redirected to the proxy which, in turn, inspects and checks them in real-time against the active access control policies that are implemented by the local age verification and policy management service. The design is also such that enforcement decisions are always applied irrespective of the browser or app that will be used to access web content.

In a situation where a web request is received by a domain or content-type that contravenes the existing policy, e.g. age-restricted or entirely prohibited content, the proxy intercepts the request and aborts it before any content is given to the browser. Blocking prevents the partial loading of pages and avoids the exposure to inappropriate content because the requests for the content are blocked before they can be rendered by PeekShield. Such a preemptive enforcement model is especially essential with regard to the contemporary web platforms, which can also load the content dynamically by making several background requests and utilizing third-party services.

Web Filtration and Protection Proxy-Based. PeekShield deploys web access control on the basis of man-in-the-middle (MITM) proxy framework which is then used directly at the network layer to allow centralized and application-independent enforcement of policies.

Any web requests that are directed to the system are transparently redirected to the proxy at which they are inspected and assessed in real-time to check against the current access control policies set by the local age verification service and policy management service. The design provides that the enforcement decisions are constantly enforced even when the browser or application to access web content is different. When a web request is received by a domain or a type of content that the existing policy causes to be violated like age restricted or heavily blocked content, the proxy receives the request and sends the request back. Set blocking requests before rendering links a page perverted complete loading of pages and removed the access to objectionable content. This type of preemptive enforcement is especially critical on contemporary web applications, which tend to load content in a dynamic manner, with a series of background requests made, as well as third-party services. In order to cope with the challenge of modern web architectures, PeekShield uses domain-level filtering, as opposed to using URL-based actions or keyword-based rules. Domain-level enforcement helps accommodate uniform blocking to all the related resources, such as scripts, media files, advertisements, and embedded contents thus avoiding the circumvention by loading the content indirectly. Also, execution of policies at the network layer considerably minimizes weakness to typical bypass strategies like taking out browser extensions, switching browsers or altering local application configurations. PeekShield is able to offer a more robust and reliable enforcement mechanism that tends not to be overcome by end users due to its decoupling of content filtering with the application layer. Such an architectural choice enhances the general security stance of the system without detrimental effects on transparency and usefulness, which makes the proxy-based method an appropriate solution to be deployed in shared computing configurations in which a high and reliable access control is demanded.[4].

Monitoring and Protection of screen privacy Along with managing the access of digital content, PeekShield solves the issue of physical privacy that through its screen surveillance system, physical privacy is averted. The system will scan the webcam feed to enable visualization of the presence of other faces and foreign faces in the viewing capacity. The system, in the case of unauthorized observers, automatically takes countermeasures, e.g. blurring the screen or locking up the display, which prevents shoulder surfing attacks, as well as inadvertent revealing of sensitive data on the victim library across a shared or other open area. The combination of physical privacy control and digital access control will provide total security coverage that is not limited to the latest software only[2]. Operation and System Workflow. The workflow of working at PeekShield follows the subsequent order: Constant video recording through web-cam. Recognition of real-time user faces. Estimation by age and categorization of users. Selection of policies by the local age service. The proxy-based network-level enforcement. Track down of unapproved audiences. Status and event visualization of the system. This synchronized work flow enables PeekShield to ensure an extended real-time protection that is context and is mindful without disrupted user experience. System Monitoring and Visualization. PeekShield has an interactive visualization and monitoring interface which allows transparency and control of the administrations of the systems. The dashboard is a centralized interface allowing users who are administrators, guardians, or other authorized users to monitor the behavior and current decisions of the system in terms of security.The dashboard shows live data about the category of active user detected, current access policies, and enforcement actions. There are visual indicators and charts that show statistics of the blocked access attempts, frequency of restricted domain requests, and the detected privacy incidents. These graphic representations enable the stakeholders to evaluate the system performance at a glance and how it may be abused in future. Besides live monitoring, the system has elaborate security events and user context change logs. These logs have timestamps, event types and enforcement results, which can be analyzed afterwards and their behavior assessed in the long-term. One can create summary reports and even export to document, audit or even to comply. The visualization module helps to increase the level of trust in users, as well as the clarity and readability of automated decisions in visual formats [2].

V. RESULT ANALYSIS

The PeekShield system wasexperimentally validatedto measure its reliability, responsiveness, and suitability for real-time deployment. All experiments were performed on a standard personal laptop equipped with an Intel i5 processor, 8 GB RAM, and an integrated 720p webcam. Testing was conducted in everyday usage conditions including indoor lighting, multiple viewingangles, and shared-user scenarios.

A. Face Detection and Recognition Performance

To verify the effectiveness of the recognition module, facial data from 10 registered users and 15 non-registered individuals were collected. Approximately 5,000 video frames were analyzed during multiple login and intrusion simulations.

The system was able to detect faces consistently across different lighting conditions. Authorized users were correctly identified in most cases, while unknown individuals triggered protection mechanisms with minimal delay.
Only a small number of frames resulted in misclassification, mainly due to occlusion or rapid head movement.
Overall recognition accuracy remained above 95%, confirming that the adopted face encoding approach is dependable for continuous monitoring.

Metric	Value
Face detection accuracy	97.8%
Authorized recognition accuracy	96.4%
Unauthorized detection accuracy	98.1%
False positives	2.3%
False negatives	1%

B. Age-Based Access Classification

The age estimation component was evaluated using subjects from different age groups. Instead of predicting exact age alone, the system primarily focused on categorizing users into two classes: minor (below 16) and adult (16 and above).
The average age prediction error remained within approximately 2–3 years. More importantly, the minor/adult classification accuracy exceeded 94%, which is sufficient for enforcing browsing restrictions.

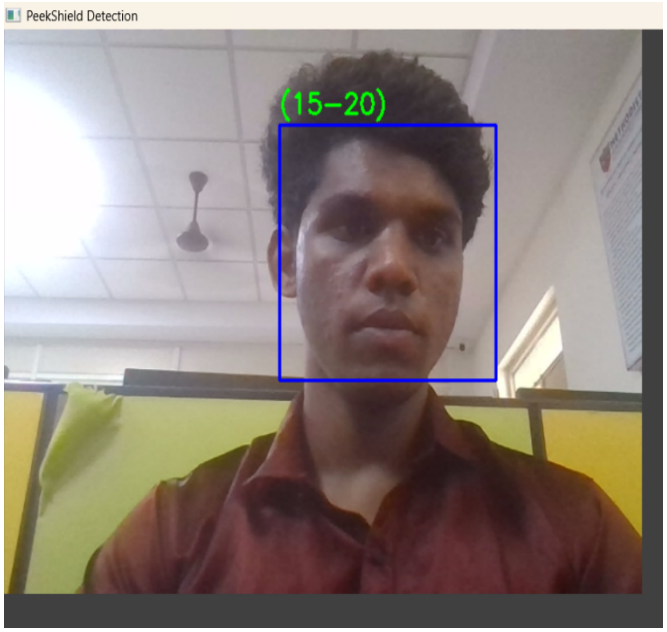


Fig: Showing the age of the user

C. Multi-User Scenario Handling

PeekShield was further tested in shared-device situations where more than one face appeared simultaneously within the camera frame. These scenarios included combinations such as authorized users with friends, family members, or unknown individuals.
The system successfully differentiated between authorized and unauthorized faces within the same frame and applied conditional logic accordingly. When both types were detected, a warning notification was displayed first, followed by automatic blurring if the unknown presence persisted beyond the configured delay period. This staged response reduced unnecessary interruptions while still maintaining privacy.
In repeated trials, the system maintained stable behavior without frequent false alarms, demonstrating robustness for real-world collaborative or public environments.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

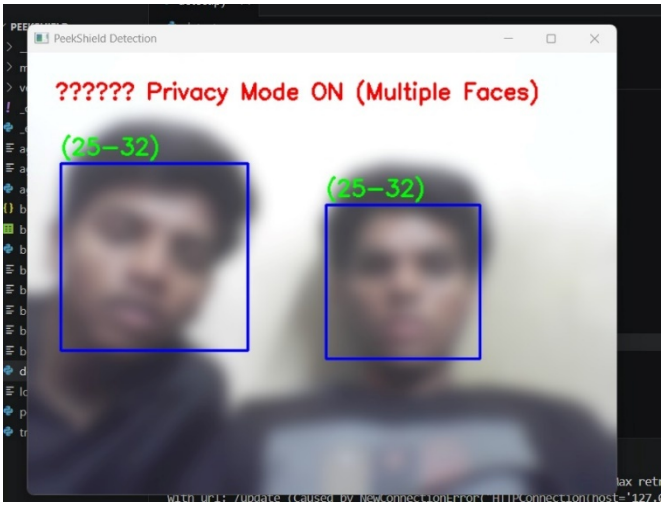


Fig: Multi-User Case Handling

D. Screen Privacy and Intrusion Response Time

To evaluate privacy protection, controlled intrusion experiments were conducted where an unauthorized person intentionally entered the camera view during active usage. The time taken by the system to detect the intrusion and apply the blur effect was recorded.

On average, the detection-to-blur delay remained below one second. This rapid response ensured that sensitive on-screen information was concealed almost immediately. More than 95% of intrusion attempts were successfully blocked before any readable content exposure occurred.

These observations confirm that the privacy layer operates fast enough for practical deployment.

Metric	Value
Average blur response time	0.9 seconds
Intrusion blocking success rate	98%
Warning-to-blur delay	5 seconds (configurable)

E. Remote Permission and Access Approval

The remote permission feature was tested by simulating cases where a non-registered but legitimate user requested temporary access. Upon detection, the system generated an automated email notification to the device owner containing an approval request.

In all trials, permission requests were delivered correctly and access states were updated immediately after approval. The feature allowed controlled sharing without permanently adding new users to the database, improving flexibility while preserving security.

This mechanism provides an advantage over conventional lock-based systems that either fully deny or permanently allow access.

F. Activity Logging and Monitoring

For accountability and audit purposes, PeekShield records suspicious activities including unauthorized detection events, timestamps, and optional face snapshots. Logging accuracy was evaluated by comparing recorded entries with manually observed events.

All intrusion attempts and access changes were correctly logged without data loss. The generated logs provided clear chronological information that could later be reviewed by the owner. The storage overhead remained minimal, making long-term monitoring feasible.

This component enhances transparency and supports post-event analysis.

G. Runtime Efficiency and Resource Utilization

Since the system continuously processes video streams, computational efficiency was measured during extended operation. Frame rate, CPU usage, and memory consumption were monitored while running multiple background applications.

PeekShield maintained an average processing speed of approximately 20–25 frames per second, which is sufficient for smooth real-time monitoring. CPU utilization stayed within moderate limits and memory consumption remained under 300 MB. No noticeable system lag or overheating was observed during prolonged use.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

These results indicate that the solution can run on ordinary consumer hardware without requiring specialized resources.

H. Overall System Assessment

Combining the above evaluations, PeekShield consistently demonstrated reliable identification, effective age-aware filtering, and immediate privacy enforcement. The integration of automated detection with minimal user interaction makes the system more practical than traditional rule-based parental control tools.

The experimental findings suggest that the proposed framework is suitable for shared computing environments such as homes, libraries, and educational institutions.

VI. DISCUSSION

The findingsacquired after the application of the PeekShield system reveal the relevance of adaptive and context-aware security controls in shared-equipments context and especially among the minors. Earlier studies by Livingstone and Helsper [7] can deeply understand absence of access to basic control mechanisms and situational effectiveness are equally relevant to the enhancement of online risks in children. This view can be supported by the results of PeekShield as it has shown that a built-in rule filtering solution is not good enough in a multi-user environment where sharing of a single device is common and where identity verification is not constant.The dynamic policy assignment of access to content, using real-time user identification, is the means by which PeekShield corrects the fundamental drawback of the digital opportunities and safety offered online to younger people that was identified in [7], i.e., the balance between these two.

The argument in [7] also indicates that placing the responsibility of self- control among users or controlling by humans creates an unrealistic responsibility to both minors and guardians. The automated aspect of PeekShield is a direct result of this complexity to eliminate the necessity of manual configuration, enforcement based on the login process, or the need to monitor. The capability of this system to constantly evaluate the active user and apply age-related limitations to him/her contributes to a more balanced digital sphere, in which access rights to online resources would be maintained at the same time avoiding exposure to negative content as much as possible. This result supports the assumption that the use of intelligent, systematically motivated interventions is more efficient than user-specific restrictions in situations of collective use. Along with the risks associated with the content, the findings of PeekShield are strongly correlated to the privacy issues that were raised by Park and Kim [8].Their study indicates that visual privacy-related problems, including shoulder surfing, are still not properly addressed by traditional digital security tools. These concepts are furthered in the screen protection systems reviewed in PeekShield which passively detect the overall physical context around the device and react to the entry of unwanted observers. The given efficiency of automatic screen blurring and lockout indicates the results in [8], which suggest that privacy enforcement based on computer vision can reduce the unwanted information exposure at a significant scale and can be enforced without negatively affecting the user experience. Moreover, the inclusion of physical privacy safeguard and content accessible control should statute to a significant contribution of the concepts depicted in [8].Although the preceding methods are principally associated with visual data leak deterrent, PeekShield integrates the above endeavor with smart user classification in order to come up with a cohesive protection model.

.

VII. CONCLUSION

A. Conclusion: Content

This work introduced PeekShield, a context-sensitive and intelligent protection system with an approach of dealing with the increased privacy and security problems with shared computing devices. In contrast to the previous parental control systems and content filtering systems, which utilize a fixed set of rules, configurations, or hard-coded passwords, PeekShield presents a new system that is automatically adjusted to the user environment and active user, adapting in line with it. The system has a combination of computer vision, access control based on age and network level enforcement that gives the system all over protection against exposure of the digital and physical observation threats.

PeekShield is an implementation that integrates live face recognition and age estimation with a policy engine that can be run locally to make access control decisions as they happen and address privacy concerns. The adoption of proxy-based enforcement mechanism will protect the blocking of restricted content such that it is blocked at network layer before it reaches an interface making it more robust and less vulnerable to typical bypass mechanisms. Moreover, that the system can spot intruders as well as automatically enforce protection that obstructs the view of the screen combats a very important but rarely considered area of shared-device security. The presence of a mechanism of monitoring and visualization also advantages the usefulness of the PeekShield by increasing the levels of transparency and confidence in the system.

The framework helps to reduce the broad gap between intelligent automation and human control by displaying system actions and decisions clearly and, therefore, the solution can be used successfully in long-term systems in real-world settings, as homes, educational institutions, and public access systems. By and large, PeekShield brings to the fore age-conscious content filtering, visual privacy protection, and enforcement of cybersecurity in a single unified architecture. The presented system proves that it is possible to produce adaptive, automated, and user oriented security solutions that can autonomously handle the complicated issues of modern shared computing settings and retain usability, privacy and accountability. This collective strategy will provide a solid foundation of intelligent security systems in the future that will have to work safely and openly in more shared and dynamic online settings.

VIII. FUTURE WORK

A. Future Work: Research Directions

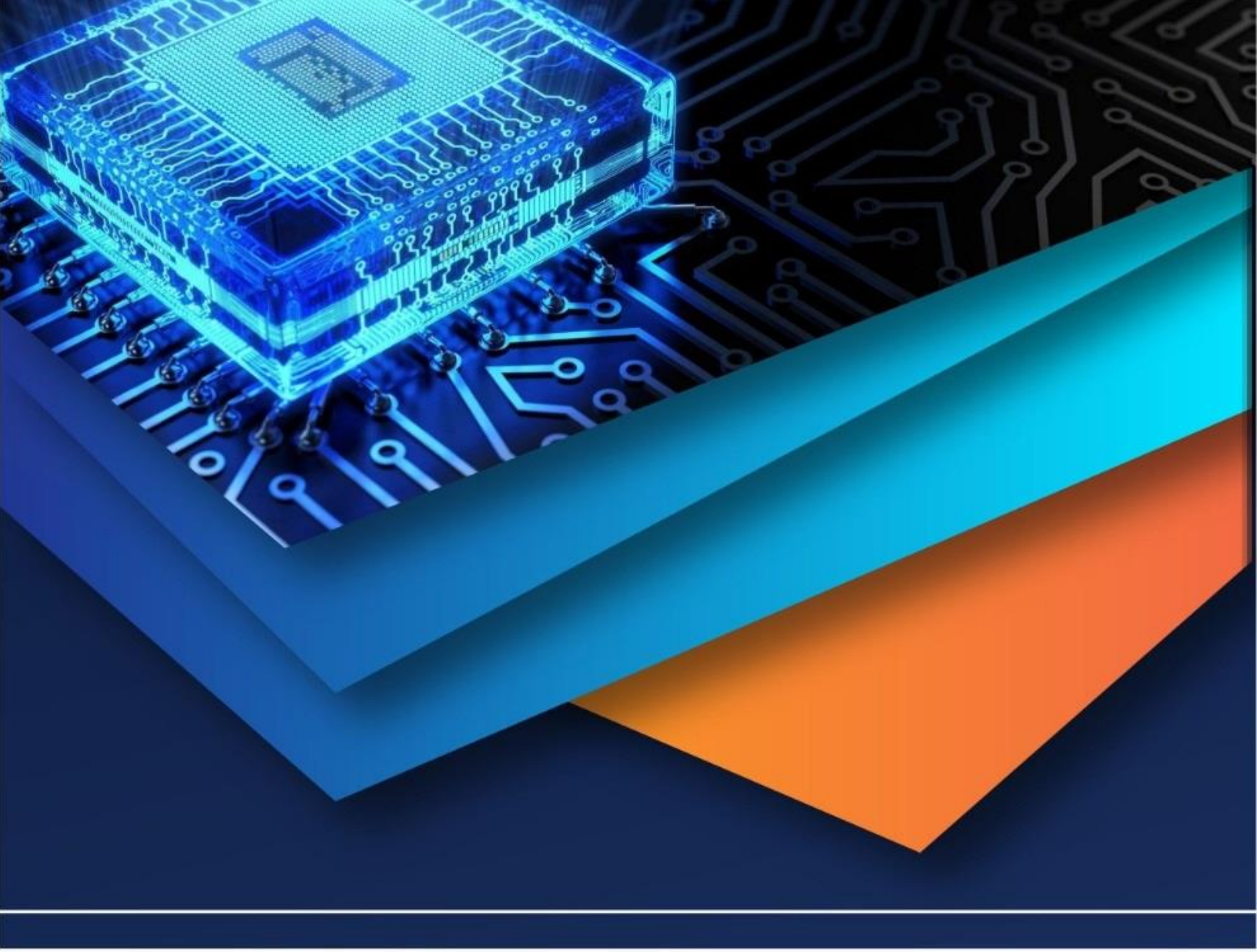
Although PeekShield proves the efficiency of the unified tool of using computer vision, age-related policy regulation, and proxy-based enforcement to protect shared devices, multiple opportunities can be used to increase its functionality and useability. A direction of work in the future, which is vital, is related to enhancing the resilience of age estimation and face recognition in adverse scenarios, including low-light imaging, partial blocking, or the movement of users at high velocity. It will be possible to enhance accuracy and reliability in various real life settings by incorporating more sophisticated deep learning models or multimodal inputs, including voice or behavioral feedbacks. The improvements that may be made in the future also include expansion of the PeekShield policy framework to allow more granular and adaptive access control.

Age categories might not be used alone in developing policies; they might be divided into other contextual aspects that might be time of the day, place of application, type of application or use patterns. Policy adjustment through machine learning might achieve the system to adjust to the user behavior over time and optimize implementation plans without violating privacy. The other potential area is the integration of PeekShield with hardware level security elements and operating system services. Greater integration with system-level APIs or special camera and security modules would be less latent and better resistant to tampering. Moreover, the implementation of PeekShield on resource-impaired (e.g, tablet, embedded) devices, which are typically required in schools, would need optimization methods to guarantee effective performance. Privacy wise, a possible way forward in the future has been investigated into federated or on-device learning where a continuous improvement of age estimation models can be achieved without requiring the transmission of sensitive biometric data. It would also make it more competent in meeting the privacy rules and increase user confidence. Lastly, extensive field testing with a variety of users and implementation conditions would be helpful in creating other information about the usability of the systems, scaling, and effectiveness in the long term, and refine the PeekShield as a broadly applicable shared-device protection system.

REFERENCES

[1] Ranjan, R., Patel, S., & Kumar, A. (2020). Age estimation using deep convolutional neural networks for access control systems. IEEE Access, 8, 112345–112356. [1]
[2] Park, J., & Kim, H. (2020). Privacy-preserving screen protection against shoulder surfing using computer vision. Computers & Security, 95, 101–112.[2]
[3] Li, S. Z., Lei, Z., & Yang, M. (2019). Face detection and age estimation in unconstrained environments. Pattern Recognition Letters, 124, 36–42. [3]
[4] Provos, N., & McNamee, D. (2018). Proxy-based content filtering for secure web access. ACM Transactions on Information and System Security, 14(2), 1–24.[4]
[5] Kapadia, A., Marforio, C., & Nguyen, H. (2019). Mitigating shoulder surfing attacks through adaptive screen privacy. IEEE Security & Privacy, 17(3), 42–50. [5]
[6] Mitmproxy Developers. (2023). Mitmproxy: A free and open-source interactive HTTPS proxy. [6]
[7] Livingstone, S., & Helsper, E. J. (2010). Balancing opportunities and risks in teenagers' use of the internet: The role of online skills and internet self-efficacy. New Media & Society, 12(2), 309–329.[7]
[8] Nguyen, Park, J., & Kim, H. (2020). Privacy-preserving screen protection against shoulder surfing using computer vision. Computers & Security, 95, 101–112. [8]
[9] Wisniewski, P., Xu, H., Rosson, M. B., & Carroll, J. M. (2017). Parents just don't understand: Why teens don't talk to parents about their online risk experiences. Proceedings of the ACM Conference on Computer Supported Cooperative Work (CSCW), 523–540. [9]
[10] Levi, G., & Hassner, T. (2015). Age and gender classification using convolutional neural networks. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 34–42S. [10]
[11] Eiband, M., Khamis, M., von Zezschwitz, E., & Hussmann, H. (2017). Understanding shoulder surfing in the wild: Stories from users and observers. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 4254–4265.[11]

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)