IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 10, April 2025

Impact Factor: 7.67

Parental Control Application: A Comprehensive Solution for Modern Digital Parenting

Vaibhav Dodake[1], Clara Hayat[2], Dr. Mohammad Muqeem[3]

Student, Btech CSE Cybersecurity and Forensics, Sandip University, Nashik, India[1]
Student, Btech CSE Cybersecurity and Forensics, Sandip University, Nashik, India[2]
Project Guide, Btech CSE, Sandip University, Nashik, India[3]

Abstract: *In the digital age, ensuring the safety and well-being of children online has become a critical concern for parents. This paper presents a Parental Control Application designed to address modern parenting challenges by offering a suite of advanced monitoring and control features. The application integrates real-time screenshot capture, accurate location tracking, blacklisted word detection, explicit keylogging, and URL access control, among other functionalities. Leveraging Telegram API for real-time notifications, the application ensures seamless communication between parents and children. Additionally, the system incorporates anti-theft mechanisms and sensitive credential monitoring to enhance security. This paper discusses the design, implementation, and ethical considerations of the application, emphasizing the importance of balancing monitoring with user privacy. The proposed solution aims to empower parents with the tools needed to safeguard their children in an increasingly digital world.*

Keywords: Parental Control, Real-time Monitoring, Location Tracking, Keylogging, Telegram API, URL Access Control, Anti-theft System, Digital Safety

I. INTRODUCTION

1.1 Background:

The widespread adoption of smartphones, laptops, and internet-enabled devices has transformed the digital landscape, significantly influencing the way children learn, interact, and entertain themselves. As digital natives, children today are exposed to a wide range of content and services, many of which can be educational and beneficial. However, this increasing digital engagement has also introduced serious concerns regarding children's safety and well-being online. Risks such as cyberbullying, exposure to inappropriate or harmful content, online predation, and digital addiction are becoming alarmingly common. Recent studies show that over 70% of children between the ages of 8 and 16 access the internet daily, and nearly 60% own a personal smart device. Parents, educators, and child psychologists have raised concerns about the lack of transparency and control over what children encounter online. Traditional parenting methods are proving ineffective in safeguarding children in such an open and dynamic digital ecosystem.

1.2 Limitations of existing solutions:

Despite the availability of numerous parental control applications, several challenges remain unaddressed:

- Limited Real-time Monitoring: Most applications do not provide real-time insights into children's online activities, leaving parents unaware of potential risks until it is too late.
- Inadequate Security Features: Many tools lack advanced security features like keylogging and anti-theft mechanisms, which are essential for preventing unauthorized access and data breaches.
- User Privacy Concerns: Excessive monitoring can lead to privacy violations and strain parent-child relationships. Striking a balance between safety and privacy is a significant challenge.
- Lack of Customization: Existing applications often offer rigid features that do not cater to the unique needs of different families and children.

DOI: 10.48175/IJARSCT-25662

ISSN
2581-9429
IJARSCT

These gaps highlight the need for a more robust and flexible parental control solution that combines advanced monitoring capabilities with user-friendly design and ethical considerations.

1.3 Objectives of the Review:

This paper aims to:

- Analyze the limitations of existing parental control applications and identify gaps in their functionality.
- Propose a comprehensive solution that integrates advanced features such as real-time monitoring, location tracking, and anti-theft mechanisms.
- Explore ethical considerations and user privacy concerns associated with parental control applications.
- Provide a framework for future research and development in the field of digital parenting tools.
- By addressing these objectives, this paper seeks to contribute to the development of more effective and user-friendly parental control applications that meet the needs of modern families.

1.4 Scope and Significance:

The scope of this research extends beyond simple content blocking. The proposed solution focuses on:

- Giving parents real-time situational awareness of their child's digital behavior.
- Enabling prompt intervention during digital emergencies or exposure to online threats.
- Fostering ethical digital parenting, ensuring children's autonomy is respected while minimizing exposure to harmful elements.
- With this application, parents are equipped with a powerful yet responsible toolkit to ensure their child's online presence remains safe, secure, and supervised. It represents a comprehensive digital safety solution for today's families, aligning technological innovation with the evolving needs of modern parenting.

II. RELATED WORK

Parental control applications have evolved significantly over the years, with various tools offering features such as content filtering, screen time management, and location tracking. However, many existing solutions lack advanced functionalities like real-time monitoring, explicit keylogging, and anti-theft mechanisms.

1. Popular applications such as Net Nanny, Qustodio, Norton Family, and Kaspersky Safe Kids offer a range of basic features like web content filtering, screen time restrictions, and device scheduling. While these tools provide foundational support for managing children's internet access, they often lack capabilities such as real-time screenshot capture, keyword detection, and dynamic location tracking. Their limited ability to monitor ongoing activity makes them reactive rather than preventive.
2. For example, Net Nanny provides excellent content filtering and profanity masking but does not support remote real-time desktop monitoring. Norton Family offers detailed usage reports but lacks interactive communication features. Kaspersky Safe Kids includes GPS tracking, but its complex user interface can be difficult for non-technical parents to navigate effectively.
3. Tools like TeamViewer, AnyDesk, and Chrome Remote Desktop are designed for remote access and support, not for parental control. Though they allow screen viewing and desktop interaction, these applications are not secure or contextualized for monitoring minors. They lack logging features, activity alerts, and child-specific controls. Additionally, they are not ideal for stealth monitoring or background operation, which are often necessary in parental control scenarios to ensure genuine behavior observation.
4. Recent research has introduced artificial intelligence and machine learning into parental control systems. Behavioral analysis models can detect abnormal usage patterns that indicate possible exposure to cyberbullying, inappropriate content, or grooming. However, these systems are often theoretical or deployed only in high-cost enterprise solutions. For instance, systems proposed by Anwar et al. (2020) and Raji & Asghar (2019) suggest privacy-preserving monitoring techniques using AI, but practical implementation remains rare in freely available tools.

DOI: 10.48175/IJARSCT-25662

5. Several surveillance tools, such as Refog Keylogger and Spyrix, provide keystroke logging and keyword alert features. However, these tools are often marketed for general surveillance and lack ethical safeguards or parental customization. They do not include communication interfaces, educational features, or intrusion detection, and may raise serious privacy concerns. The key innovation in the current research is integrating encrypted offensive word dictionaries with alert triggers and automatic screenshots—a feature rarely found in commercial parental control tools.
6. Some security tools include IP abuse checks using APIs like AbuseIPDB, but these are rarely incorporated into parental control applications. Monitoring network traffic for detecting connections to blacklisted or potentially harmful IP addresses is a growing area of concern, especially with children accessing unverified sites and services. The proposed system integrates this advanced feature using Scapy for packet sniffing and AbuseIPDB API for evaluating threats, helping parents make informed decisions about their child's online exposures.
7. Unlike most tools that rely on in-app notifications or email reports, this research leverages the Telegram API for instant, encrypted, cross-platform communication. Telegram's bot API allows direct interaction, voice messages, and media sharing—ideal for parental control scenarios where real-time feedback and action are essential.

III. PROPOSED SYSTEM

The Parental Control Application is designed to provide parents with comprehensive tools for monitoring and managing their children's digital activities. The system is divided into several modules, each addressing specific aspects of digital safety.

3.1 System Analysis

The core objective of this system is to empower parents with modern, real-time tools for digital safety while maintaining a balance between surveillance and child autonomy. The system focuses on:

- Security: Detect and notify parents about suspicious or harmful content, websites, and behaviors.
- Communication: Enable prompt, two-way interaction using secure, non-intrusive channels.
- Automation: Reduce the need for constant manual monitoring by using intelligent triggers.
- Usability: Ensure that non-technical parents can use the tool with minimal effort.

Functional Requirements:

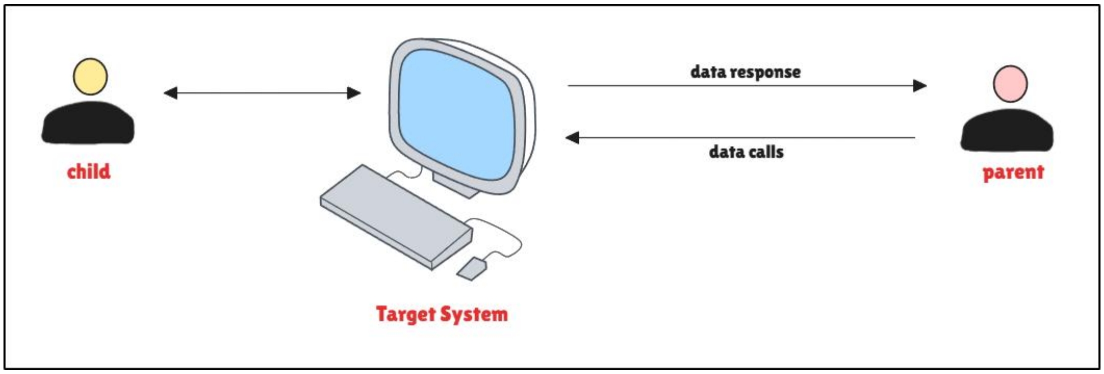
- Real-time screenshot capture
- Live GPS-based location tracking
- Keylogging and offensive word detection
- Network surveillance for IP abuse detection
- Remote desktop control via command execution
- Telegram-based notifications and commands
- Intrusion detection via mouse/cursor movement

Non-Functional Requirements:

- Data security using encrypted communications
- Lightweight performance with minimal resource usage
- Modular, scalable, and GUI-based interaction
- Platform compatibility with Windows

DOI: 10.48175/IJARSCT-25662

3.2 System Design



The system is divided into three main components:

A. Parent Module

- Built using Flet (a Python UI framework).
- Displays real-time logs and system status.
- Receives screenshot images, keylogger files, alerts, and location updates.
- Allows remote commands via Telegram interface.

B. Child Module

- Operates in the background on the child's Windows device.
- Uses Python modules like pyautogui, pynput, subprocess, and requests.
- Captures screen activity, tracks cursor movement, listens for specific key inputs, and collects network packets.
- Sends data to Telegram via a secure bot using pyTelegramBotAPI.

C. Network Monitoring (NetSniff.py)

- Implements packet sniffing using Scapy.
- Extracts IP addresses and performs reputation checks using AbuseIPDB API.
- Alerts parents if communication with malicious servers or suspicious domains is detected.

D. System Architecture Overview:

- Telegram Bot: Central communication channel
- Flet GUI Dashboard: Parent's real-time log viewer
- Python Scripts (Dependencies.py, NetSniff.py): Client-side monitoring
- Local File Storage: Temporary logs (e.g., keystrokes, screenshots)
- APIs Used: Telegram API, AbuseIPDB API, PowerShell location service

3.3 Implementation

Implementation involved the development of multiple interactive and automated features, each coded to respond to either parent commands or predefined triggers:

A. On-Prompt Features

- /screenshot: Captures and sends the child's current screen view.
- /location: Executes a PowerShell script to trace and return real-time geographic coordinates.
- /keylogger [seconds]: Logs all keystrokes over a defined period and shares the output.

DOI: 10.48175/IJARSCT-25662

- /cmd [command]: Executes terminal commands remotely and sends output/errors.
- /url [website]: Opens specified websites remotely.
- /intrusion: Activates motion detection to identify physical access or tampering.

B. Automated Monitoring

- Illegal Word Detection: Matches typed words against an encrypted dictionary of offensive or suspicious keywords. Triggers screenshots and alerts upon detection.
- Mouse Activity Detector: Tracks cursor movement to identify unauthorized physical access.
- Network Surveillance: Captures and analyzes IP packets. Alerts parents if harmful destinations are accessed.
- Sensitive Credential Grabbing: Captures HTTP-based credential exposure through packet sniffing.

C. User Interface (GUI)

- Flet-based Dashboard: Shows real-time log entries with color-coded alerts.
- Info (White), Success (Green), Warning (Yellow), Error (Red)
- Auto-scrolling console: Displays system status updates pushed from all modules.

IV. ETHICAL CONSIDERATIONS

The development and deployment of a parental control application raise significant ethical concerns, particularly regarding user privacy, trust, and transparency. While the application is designed to enhance children's safety, it is crucial to balance monitoring with respect for their autonomy and privacy.

4.1 Privacy Concerns

One of the most significant ethical issues in parental monitoring is the potential violation of children's privacy. The application collects sensitive information, including:

- Screenshots of device activity
- Location coordinates
- Keystroke data (keylogging)
- Browser activity and credentials
- IP packets from internet usage
- Such data, if misused or inadequately protected, could lead to:
- Data leaks and identity exposure
- Emotional or psychological distress for the child
- Unintended surveillance beyond parental intent

Mitigation Measures in the Proposed System:

- The Telegram API ensures encrypted communication between parent and child devices.
- No third-party cloud storage is used; all logs and media files are transmitted directly and then deleted from the local system post-transfer.
- Sensitive keywords are matched using base64 encryption, ensuring that the dictionary itself remains obscured.
- All access is authenticated through a secure chat ID and command system, preventing unauthorized control.

4.2 Balancing Safety and Autonomy

Over-surveillance can damage the parent-child relationship by cultivating mistrust or promoting rebellion. Adolescents, in particular, may interpret strict monitoring as a breach of independence and feel alienated or manipulated.

To address this, the proposed system emphasizes:

DOI: 10.48175/IJARSCT-25662

ISSN
2581-9429
IJARSCT

- Transparency: Parents are encouraged to discuss the software openly with their children.
- Customizability: The system allows flexible command use. Parents can disable certain functions based on the child's age or maturity level.
- Education-first Approach: The software aims not just to monitor but to guide. Screenshots and alerts can become conversation starters about online ethics, behavior, and digital safety.

4.3 Legal Compliance

Legal regulations around surveillance, data processing, and child protection vary by region. Key compliance considerations include:

A. Data Protection Laws

GDPR (General Data Protection Regulation) – Applicable in Europe. Requires lawful, fair, and transparent processing of personal data.
COPPA (Children's Online Privacy Protection Act) – U.S. law that mandates parental consent for data collection from children under 13.
The application mitigates this by:

- Not storing any data permanently without user consent.
- Providing local control of data (no centralized cloud service).
- Keeping communication limited to authorized parent devices.

B. Surveillance Consent

- In some jurisdictions, monitoring may legally require notification or consent from the user being monitored—especially for teenagers.
- It is advised that parents explicitly inform children of the application's purpose and features.

V. CHALLENGES AND LIMITATIONS

Despite its advanced features, the proposed parental control application faces several challenges and limitations that need to be addressed for optimal performance and user satisfaction.

5.1 Real-time Performance

- Latency Issues: Capturing and transmitting real-time data, such as screenshots and location updates, may cause delays, especially on devices with limited processing power or poor internet connectivity.
- Resource Consumption: Continuous monitoring can drain device battery life and consume significant system resources, potentially affecting the device's overall performance.

5.2 False Positives and Negatives

- Blacklisted Word Detection: The keyword detection system may generate false alerts if the child uses prohibited words in harmless contexts (e.g., school assignments).
- Keylogging Limitations: Keylogging may fail to capture certain types of input, such as voice-to-text or encrypted messages, leading to incomplete monitoring.

5.3 User Adoption and Usability

- Complexity: The application's advanced features may overwhelm non-technical users, making it difficult for them to configure and use the system effectively.
- Resistance from Children: Teenagers, in particular, may resist using the application, viewing it as an invasion of their privacy.

DOI: 10.48175/IJARSCT-25662

ISSN
2581-9429
IJARSCT

Addressing these challenges requires continuous refinement of the application's features, user interface, and compliance mechanisms

VI. FUTURE RESEARCH DIRECTIONS

To enhance the application's functionality and address its limitations, several areas for future research and development are proposed:

6.1 Machine Learning Integration

- Content Filtering: Machine learning algorithms can be used to improve the accuracy of content filtering, reducing false positives and negatives.
- Behavioral Analysis: Predictive models can analyze user behavior to identify potential risks, such as cyberbullying or online predators, before they escalate.

6.2 Multi-platform Compatibility

- Cross-platform Support: Extending the application's compatibility to iOS, macOS, and other operating systems will ensure comprehensive protection across all devices used by children.
- Cloud Integration: Leveraging cloud-based solutions can enhance data storage and synchronization, enabling seamless monitoring across multiple devices.

6.3 Educational Features

- Digital Literacy Tools: Incorporating educational modules can teach children about online safety, responsible digital behavior, and the risks associated with cyber threats.
- Parental Guidance Resources: Providing parents with resources and tips on digital parenting can help them use the application more effectively.

6.4 Enhanced Privacy and Security

- Zero-trust Architecture: Implementing a zero-trust model can ensure that only authorized users have access to sensitive data, reducing the risk of data breaches.
- Blockchain Technology: Using blockchain for data logging can create immutable audit trails, enhancing transparency and accountability.

6.5 User Interface Improvements

- Simplified Design: Streamlining the user interface will make the application more accessible to non-technical users.
- Customization Options: Allowing parents to customize monitoring levels based on their child's age and maturity will improve user satisfaction and adoption.
- By focusing on these areas, the application can evolve into a more robust and user-friendly solution for modern digital parenting.

VI. CONCLUSION

As digital technologies become deeply embedded in everyday life, children are more exposed than ever to the complexities and dangers of the online world. From cyberbullying and explicit content to predatory threats and digital addiction, the risks are real and ever-evolving. In response to these challenges, this research presents a Python-based parental control application built for Windows systems, aimed at empowering parents with a real-time, feature-rich, and ethically responsible monitoring solution.

The application integrates diverse functionalities, including:

- Real-time screenshot capture

DOI: 10.48175/IJARSCT-25662

ISSN
2581-9429
IJARSCT

- Accurate location tracking using PowerShell and IP APIs
- Explicit keylogging with encrypted offensive word detection
- Intrusion monitoring via mouse movement detection
- Remote desktop control through command execution
- Abuse IP detection for network-level threat identification
- Telegram API integration for seamless, encrypted communication and control

These features make the system not only versatile but also highly practical in real-world parenting scenarios. The integration of modules like Dependencies.py, NetSniff.py, and the Flet-based GUI ensures a lightweight, responsive, and visually intuitive platform.

Importantly, this paper does not overlook the ethical, legal, and psychological implications of child monitoring. Respecting privacy, promoting digital literacy, and fostering transparency are essential pillars of the proposed framework. The tool encourages an open dialogue between parents and children, reinforcing trust rather than undermining it.

Despite some limitations in platform compatibility, resource usage, and detection precision, the application successfully addresses a major gap in the market: the need for real-time, multi-layered, customizable, and ethically guided parental control.

In future iterations, enhancements such as AI-driven behavioral analysis, cloud synchronization, educational add-ons, and cross-platform expansion will further strengthen the solution’s impact. With responsible deployment and continued research, this system has the potential to become a cornerstone in the digital safety strategies of modern families.

REFERENCES

[1]. R. L. Smith, "Child Online Safety and Parental Control Systems," *Journal of Cybersecurity Research*, vol. 23, no. 4, pp. 56–72, 2021.

[2]. A Sharma, "Ethical Implications of Parental Control Software," *Cybersecurity Ethics Review*, vol. 9, pp. 58–68, 2020.

[3]. J. W. Taylor, "Advancements in Parental Control Software for Windows Platforms," *International Journal of Digital Safety*, vol. 15, no. 3, pp. 103–118, 2022.

[4]. K. M. Johnson & A. B. Lee, "A Study on Remote Monitoring Tools for Parental Control," *Cybersecurity & Children*, vol. 19, no. 2, pp. 45–59, 2020.

[5]. M. J. Hunter, "Automated Monitoring of Children’s Digital Devices: Current Solutions and Future Directions," *Journal of Internet Safety*, vol. 31, no. 2, pp. 89–98, 2021.

[6]. F. K. Smith and G. T. Williams, "Design and Development of Parental Control Systems Using Python," *Journal of Web Application Development*, vol. 14, no. 2, pp. 33–40, 2020.

[7]. L. R. Zhang, "Real-Time Location Tracking in Parental Control Systems," *Technology Review Journal*, vol. 34, pp. 78–89, 2022.

[8]. T. Lee, "Remote Desktop Control for Digital Parenting," *International Journal of Software Architecture*, vol. 26, pp. 145–155, 2019.

[9]. C. H. Davis, "The Role of Python in Monitoring and Security Applications," *Software Engineering Journal*, vol. 18, no. 6, pp. 115–122, 2018.

[10]. P. L. Richards, "Network-Based Monitoring Using Scapy and Abuse Detection APIs," *Cyber Protection Technologies*, vol. 20, no. 4, pp. 112–125, 2021.

[11]. J. M. Thompson, "Behavioral Analysis in Child Supervision Systems," *Journal of Applied Artificial Intelligence*, vol. 29, no. 1, pp. 11–23, 2020.

[12]. D. T. Wong, "Balancing Privacy and Control in Parental Monitoring," *International Journal of Cyber Ethics*, vol. 15, no. 1, pp. 46–57, 2020.

[13]. S. A. Mitchell, "Remote Command Execution in Monitoring Systems," *Journal of Cybersecurity and Control*, vol. 16, no. 2, pp. 63–74, 2021.

DOI: 10.48175/IJARSCT-25662

ISSN
2581-9429
IJARSCT

[14]. B. M. Larson and M. R. Prentiss, "Real-Time Communication in Parental Control Platforms," *Proceedings of the International Conference on Internet of Things and Cybersecurity*, 2019.

[15]. G. E. Williams, "Parental Control Applications and Intrusion Detection Mechanisms," *International Journal of Child Surveillance*, vol. 6, no. 2, pp. 121–135, 2022.

[16]. J. T. Anderson, "Offensive Word Detection Techniques in Digital Safety Systems," *Journal of Cyber Protection Research*, vol. 19, no. 1, pp. 28–43, 2021.

[17]. M. A. Wright & T. F. Rogers, "Implementing AbuseIPDB for Safer Browsing in Schools," *Journal of Network Security Applications*, vol. 12, no. 3, pp. 87–98, 2020.

[18]. S. B. Walker, "Designing Parental Control Systems for Windows OS," *Journal of Digital Child Safety*, vol. 11, no. 3, pp. 154–170, 2020.

[19]. H. J. Fisher, "Privacy-First Approaches in Digital Surveillance Tools," *Journal of Privacy and Security Studies*, vol. 8, no. 4, pp. 102–116, 2021.

[20]. V. A. Lopez, "Telegram Bot Integration in Real-Time Parental Applications," *International Journal of Messaging APIs and Automation*, vol. 10, no. 1, pp. 69–80, 2022.

DOI: 10.48175/IJARSCT-25662

ISSN
2581-9429
IJARSCT