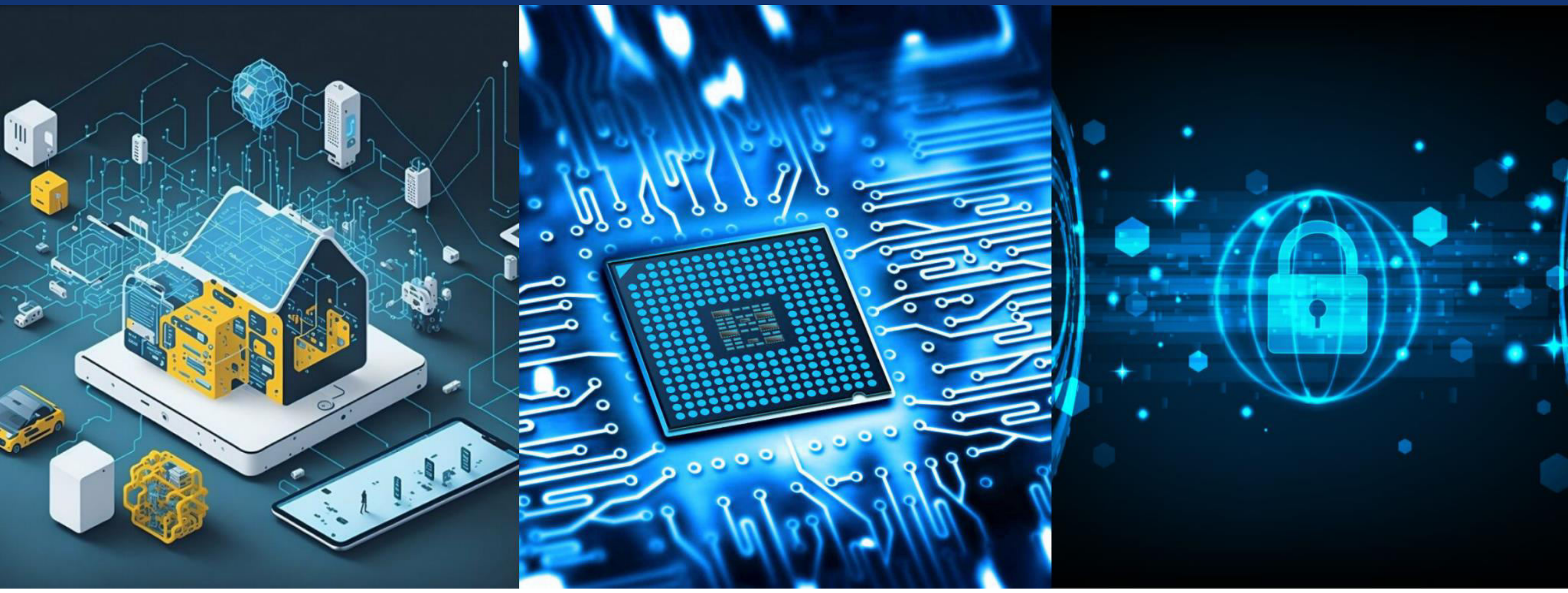
IJIRCCE

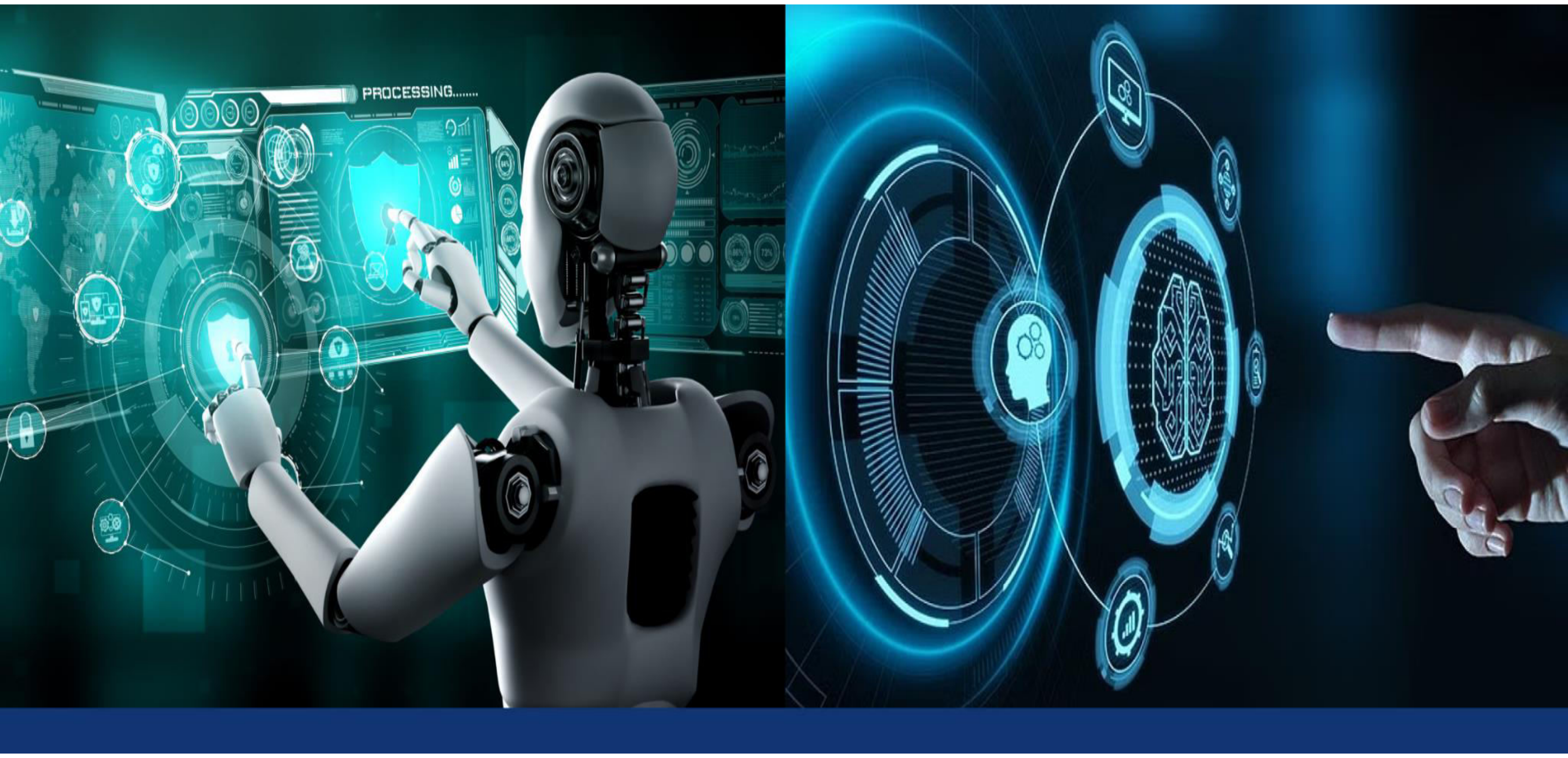
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 5, May 2025

www.ijircce.com ijircce@gmail.com +91-9940572462 +91 63819 07438

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305087

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Smart Parental Surveillance: Advanced Keylogging Techniques for Child Cybersecurity

Niroop P, Tejaswini K S, Sandeep U, Amshu B Patel, Prof. Gangamma H

UG Student, Dept. Of CSE., Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India

Associate Professor, Dept. of CSE., Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India

ABSTRACT: This work introduces the design and development of Smart Parental Surveillance, a cybersecurity-oriented solution that utilizes state-of-the-art keylogging methodologies to track and safeguard children online. The system offers real-time keystroke logging, application usage, and web browsing activity to help parents detect potential threats such as cyberbullying, grooming, and access to offensive content. Designed with privacy-sensitive mechanisms and safe storage protocols, the tool promotes minimal invasiveness while assuring high oversight. In contrast to conventional monitoring tools, the system proposed combines smart filtering and alerting mechanisms to differentiate normal from suspicious activities. Performance reviews confirm the efficacy of the tool in identifying initial indicators of dangerous online interactions, rendering it an important resource for child online protection programs.

KEYWORDS: Keylogging, Child Cybersecurity, Parental Monitoring, Real-time Surveillance, Secure Logging, Behaviour Tracking, Online Safety.

I. INTRODUCTION

Children today face increasing threats online, including cyberbullying, surveillance, and exposure to harmful content. Traditional parental control systems often lack the real-time, intelligent capabilities necessary to address these modern dangers effectively. As technology advances, so too must the sophistication of parental monitoring tools systems that are not only integrated with security platforms but also designed with a strong appreciation for user privacy.

This paper proposes an intelligent parental monitoring system that goes beyond conventional keylogging methods. It aims to track a child's online activities including application usage, internet browsing, and behavioural patterns—in real time. The system incorporates a secure, Quasar-based archiving and filtering infrastructure. Its goal is to strike a balanced approach to child cybersecurity: delivering early warnings about potentially dangerous online behaviour without infringing upon the child’s right to privacy in an excessive or unethical manner.

II. RELATED WORK

Over the past few years, the growing exposure of children to online threats has sparked substantial research in cybersecurity and parental monitoring software. Keyloggers traditionally were becoming more sophisticated into smarter systems with the ability to recognize behavior patterns and online risks. This transformation is fuelled by the threats to child safety, privacy, and the shortcomings of traditional monitoring methods.

These challenges have been met by several studies that suggested sophisticated surveillance methods. For example, Thomas et al. (2021) created a smart keylogging framework coupled with artificial intelligence to interpret keystroke behaviour and notify parents of possible cues of distress or dangerous interactions [1]. In the same manner, Patel and Rao (2022) suggested a browser-based keylogging and monitoring system with the ability to identify cyberbullying language through natural language processing algorithms [2]. Another pertinent contribution from Lee et al. (2023) suggested a hybrid monitoring framework that integrated application usage monitoring with keystroke information to build behavioural profiles of kids for the detection of early threats [3].

Moreover, Singh and Gupta (2022) explored the ethical considerations and data privacy controls inherent in real-time keylogging, proposing anonymization and secure logging to minimize the intrusiveness of such systems [4]. Fernandez et al. (2023) created a cross-platform monitoring software that monitors child behaviour on both mobile and desktop platforms, offering centralized views with data security ensured via encryption [5].

III. PROPOSED ALGORITHM

A. Design Considerations:
The envisaged Smart Parental Monitoring System aims to improve child cybersecurity through real-time keystroke typing, application usage, and cyber activity tracking. The ultimate vision is to equip parents with smart, non-intrusive tools to identify risky cyber interactions without compromising user privacy and adhering to surveillance ethics. The system is developed employing Python for backend processing and JavaScript for client-side activity tracking, backed by a secure log system facilitated through encrypted databases like MongoDB.

The keylogging is done at the system level or through browser-based JavaScript injection based on the platform, and all logged information is encrypted prior to storage or transmission. Intelligent behaviour filters are used to detect patterns of concern like abusive language, excessive screen usage, or access to objectionable sites. There is a dashboard interface that enables parents to see categorized logs, get notification, and specify monitoring preferences. To ensure the security of data collected, RSA encryption is used on keystrokes and logs, and access is strictly controlled through user authentication and role-based permissions.

B. Description of the Proposed Algorithm:
The system in consideration has five primary modules: User Setup and Authentication, Real-time Keystroke Logging, Intelligent Behaviour Detection, Secure Data Logging, and Parental Dashboard and Alert System.

Step 1: User Setup and Authentication:
The procedure starts right from the installation or installation of the monitoring software on the child device. On successful registration, parent and child accounts are set up, along with the parent also receiving access credentials to the monitoring interface. Password-protected login is used for authentication, and secure communication is established between the child device and parent view interface.

.

Step 2: Real-time Keystroke Logging:
Keystrokes made on the kid's machine are caught in real-time by platform-specific keylogging drivers. Keyboard inputs, together with metadata including timestamp, current running application, and window title, are logged by the logger. Data so obtained is encrypted instantaneously by RSA prior to sending or storage.

Step 3: Intelligent Behaviour Detection:
The encrypted logs are fed through a behaviour analysis module that employs pre-programmed filters and AI-based keyword matching to detect harmful content. This involves detection of cyberbullying keywords, indicators of self-harm, or suspicious communications. Should such activity be detected, the system raises an alert for parental review.

Step 4: Secure Data Logging:
All captured key information and behavior analysis results are written to a secured, encrypted MongoDB database. Logging blocks unencrypted keystrokes from being stored. The database can only be accessed by authenticated parent users, and sensitive information is tamper and unauthorized access-proofed.

Step 5: Parental Dashboard and Alert System:
Parents can log into a secure dashboard and view categorized logs of activity, receive real-time alerts, and establish monitoring preferences (e.g., content filters, monitoring timeframes, etc.). All logged events include context to enable parents to make an informed choice. Exportable reports and summaries are enabled for daily or weekly activity. Suspicious login or access attempt is logged and flagged to enable complete auditability.

IV. PSEUDO CODE

```
Step 1: Parent and child accounts are registered and logged into the system.
    → Parent is granted access to a secure monitoring dashboard.
    → Child device installs keylogger client or browser script.
Step 2: Create RSA key pair (public and private) for secure logging.
    → Public key is utilized to encrypt logs prior to storage or transfer.
    → Private key is securely stored by the parent for decryption.
Step 3: Real-time keylogging starts on the child device.
    → Record keystrokes with timestamp, app title, and window title.
    → Record background activity continuously.
Step 4: Intelligent behavior analysis module triggered.
    → Match key pattern with sensitive word database (e.g., suicide, bullying).
    → Alarm/Flag parent if matched.
    → Optionally undertake sentiment/emotion analysis.
Step 5: Encrypt log entry using parent's public RSA key.
    → Encrypted Log = RSA_Encrypt(public_key_parent, captured_data)
    → Raw text not retained in logs or sent unencrypted.
Step 6: Securely store encrypted logs in MongoDB database.
    → Store metadata: timestamp, app_name, child_id, encrypted_text
    → Log hash: SHA-256(Encrypted Log + Metadata)
Step 7: Show logs and activity summaries on parental dashboard.
    → Parent decrypts logs with private RSA key.
    → Logs are categorized by app, alert level, and timestamps.
    → Filtering, searching, or downloading activity reports as an option.
Step 8: Alert system and integrity check.
    → All abnormal behavior (e.g., blacklisted words or repetitive patterns) results in alerting.
    → Hash logs against past hashes for tamper detection.
    → Any mismatch results in alert and potential data re-validation.
Step 9: Parent logs out and monitoring session completed.
    → All sessions closed securely.
    → Session metadata and logout event logged.
Step 10: End
```

V. SIMULATION RESULTS

The Smart Parental Surveillance System was tested by simulating an environment to analyze its effectiveness in tracking and protecting the child's online activities. The test environment included several simulated user accounts, both parent and child, where keystroke logging, application monitoring, and intelligent behavior analysis were enabled. The test was conducted in a controlled environment where the child's device was set to mimic real-time activities, including typing in a range of applications, internet browsing, and social media. Under stress tests where the child was performing a high number of activities (e.g., fast app switching, frequent messaging), the system did not compromise its integrity, performance, and security. There were no delays witnessed in the process of logging and alerting, and encryption and decryption were all done within tolerable time thresholds. Any attempted unauthorized access was blocked, showing once again that the access controls and encryption works.

VI. CONCLUSION AND FUTURE WORK

Smart Parental Monitoring System has been able to provide a comprehensive solution to the growing problems of child safety online with behaviors analysis, keylogging, and monitoring in real time. Smart Parental Monitoring system, along with RSA encryption, behavior analysis, and blockchain-backed data integrity ledger, offered a full privacy-centered solution to monitoring and tracking kids online and then providing parents with control. Our system records and encrypts keystrokes and recording of applications in real-time, with alerts for any suspicious behavior, while protecting the sensitive data of the production of the corresponding keystroke/monitoring session with end-to-end encryption. The behavior analysis tool itself employs machine learning-based analysis, detecting behavior that warrants intelligent monitoring by the parent to be able to intervene if any serious threats present themselves, such as cyberbullying or inappropriate content. The data recorded kept in the blockchain ledger, also ensures the restriction of unauthorized alterations by third parties to directly log online activity enabling parents say to keep a record of their child online activity. Testing and simulation of the monitoring system has assured that the system works as intended within realistic test cases that demonstrate high performance with low latency, and the data being encrypted. The system demonstrated the ability of the application to support multiple simultaneous activities and users regardless of the activity that was generally unnoticeable, or unaudible, and therefore increased the weight of the argument for this system as a viable and scalable solution to provide safety for children in an online world.

REFERENCES

1. Zhang, Y., & Wang, L. (2023). Enhancing child safety using real-time monitoring and keystroke logging systems. Journal of Child Online Safety, 12(4), 112–125.
2. Alzahrani, B., & Al-Hadhrami, A. (2022). Keylogging techniques for improved parental surveillance in digital environments. Journal of Cybersecurity and Privacy, 9(3), 97–110.
3. Huang, R., & Liu, D. (2023). Blockchain-enabled secure parental control for real-time child monitoring. Journal of Digital Privacy and Security, 5(2), 45–59.
4. Muniraju Hullurappa, Sudheer Panyaram, “Quantum Computing for Equitable Green Innovation Unlocking Sustainable Solutions,” in Advancing Social Equity Through Accessible Green Innovation, IGI Global, USA, pp. 387-402, 2025.
5. Kumar, V., & Mishra, R. (2023). Behavioral analysis and alert systems for child cybersecurity in the digital era. International Journal of Child Protection Technology, 6(1), 34–48.
6. Sharma, D., & Soni, P. (2024). Parental control apps with biometric security: Enhancing child safety on digital platforms. Journal of Information Security for Children, 8(2), 89–102.
7. Patel, N., & Gupta, A. (2023). The role of AI in parental surveillance systems for digital child safety. Journal of Artificial Intelligence in Cybersecurity, 7(1), 120–135.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details