

Smart IoT Robot Toy with AI-Based Safety Judgment and Parental Monitoring Features

Check-Yee Law¹, Wee-Yang Goh², Yong-Wee Sek³

COE for Advanced Cloud-Centre for Intelligent Cloud Computing (CICC), Multimedia University, Melaka, Malaysia^{1,2}

Faculty of Artificial Intelligence and Cyber Security, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia³

Abstract—Smart Internet of Toys (IoToys) can provide interactive learning and companionship for children, but many systems still provide limited support for guardian awareness and safety notification. This study presents the design and development of a smart IoT robot toy with AI-based safety judgment and parental monitoring features. The prototype integrates a robot head unit, web-based monitoring dashboard, camera viewing, remote movement control, two-way communication, AI-assisted safety judgment, Telegram guardian notification, memory-based allergy reminder, chat history, and behavior report. The system uses an ESP32-S3 CAM head unit, an ESP32-C3 mobile base, a Node.js server, cloud-assisted AI services, and a Telegram Bot notification channel. Scenario-based testing was conducted, and the results showed that the prototype can support remote observation and notify guardians about child safety-related scenarios such as fear, injury, danger, and food allergies.

Keywords—Child safety; internet of toys; IoToy; IoT robot; parental monitoring; privacy concerns; smart toy; Telegram notification

I. INTRODUCTION

Smart toys have progressed from being simple electronic devices to complex connected systems that are able to sense, communicate, and act upon users. These developments play a key role in the domain of the Internet of Toys (IoToys), which aims to have toys interact with children and their environments, typically autonomously. These toys are equipped with sensors, actuators, and AI algorithms that allow them to offer tailored and interactive play experiences [1, 2].

Smart toys can be used as a kind of entertainment and learning instrument in home scenarios, which can create creative play and cognitive development activities [3, 4]. They can gather and analyze data using cameras, microphones, and other sensors. However, there is a problem of privacy and safety concerns with children interacting with these toys without the supervision of their parents [1, 2, 5]. Some toys, for example, stream data to servers on an ongoing basis, which could allow audio surveillance, whereas others have been the victim of privacy breaches or the ability of the attacker to control the toy [2, 5].

Therefore, it is necessary to improve smart toys to overcome the above challenges, which should include functions to entertain and help the guardians keep track of safety-related events. This includes receiving live alerts for any strange activity or possible dangers identified by the toy's sensors or AI-based analysis.

However, existing research reveals a gap in a unified security model or security guidelines for secure use of smart toys [2, 6]. The work on ontologies that explicitly support privacy and security requirements for smart toys is still in progress, and implementation is still limited [1, 7]. This implies that smart toys have great potential to be interactive and educational, but they need to be designed with careful consideration of strong safety and privacy protections to support guardians' ability to keep children safe in their interactions with the toys when they are not being supervised [1, 2, 5].

There are some smart toys that focus on entertainment, learning, or interaction, with limited monitoring by guardians and safety notifications. For example, some devices feature mobile apps, but they tend to focus more on content control instead of situation awareness and parental control [1]. Previous studies have also pointed out that child-centered IoT toys need to be more attentive to privacy, security, and parental control, as well as communication safety. Smart toys are often equipped with sensors, cameras, and microphones that gather personal and situational information, a fact that is worrying many about their ability to be accessed by other people without consent, and their potential to violate privacy rights [1, 2]. In addition, the absence of uniform guidelines for parental control and privacy protection adds to these risks, making children susceptible to digital and physical dangers [8, 9].

This study reports on the parental monitoring part of an AI-enabled IoT robot toy developed as a prototype. The aim is not to replace adult supervision, but to provide an additional awareness and communication channel between the child, the robot, and the guardian. Compared with the complete robot platform, this study focuses on modules related to monitoring, safety notification, remote intervention, and behavior awareness.

The remainder of this study is organized as follows. Section II reviews related work on Internet of Toys, smart toy safety, and parental monitoring. Section III describes the proposed system design and the parental monitoring workflow. Section IV describes the implementation of the web-based monitoring dashboard, camera monitoring, Telegram notification, AI-based judgment, behavior report, and remote intervention modules. Section V presents the scenario-based testing results with screenshots and photos as supporting evidence. Section VI discusses the findings, limitations, and privacy concerns of the prototype. Finally, Section VII concludes the research work with the main contributions and future work.

II. RELATED WORK

Internet-connected toys (IoToys) combine embedded hardware, sensors, wireless communications, and software services to provide interactive and connected play experiences. The toys are typically designed with integrated capabilities like voice control, wireless connectivity, and adaptive feedback, which add to their attractiveness and usability at home [10, 11, 12]. Even at home, many factors come into play, including safety, transparency, and having guardians' control. The main issues related to safety involve privacy and security related to the collection and processing of personal data, such as sensitive data about children, by IoToys. This information may be subject to hacking, unauthorized use, or misuse, raising serious privacy concerns [10, 13, 14, 15]. Another major concern is transparency; information regarding the collection, storage, and use of personal data by these toys is often unclear to children and their guardians. To enhance transparency, privacy rules and privacy education resources are being developed to better inform children and parents about data collection mechanisms [11, 16].

Guardian control is vital to making sure that IoToys are used safely and responsibly. There are currently challenges related to the lack of uniform safety labelling on IoToys and the difficulty for parents to be able to determine the level of security that these devices have before buying them. This is the reason why there are privacy labels and security labels such as "ChildShield" being proposed to help consumers understand the safety features of IoToys [14]. Furthermore, IoToys will need to be both educational and entertaining, yet safety measures must be very robust to ensure that they are interesting and safe for children [10, 12]. This means that IoToys creates innovative and personalized playing experiences, but its use at home will require attention to privacy, security, and parental control issues to ensure safe and transparent use [10, 11, 13, 14, 15].

Smart toys pose serious security and privacy concerns related to children's speaking data and cloud processing, network communication, application vulnerabilities, and lack of parental control. Smart toys can also record voice information and send it to the cloud to analyze. This adds a layer of privacy concerns, since live streams of data can be exploited for unauthorized audio monitoring. For example, some AI-powered toys are known to send constant audio data to servers, which might pose privacy and surveillance concerns [5, 17]. There are many smart toys that have security issues with their network communications with servers, so they can be hacked and their data exposed. These weaknesses tend to be related to bad practices in the implementation of security policies, as has been reported in the analyses of toy communication environments [18, 1, 19]. Smart toy companion apps often have excessive permissions and do not employ robust security measures. Static and dynamic analyses have identified problems in these apps, including unnecessary data collection and lack of adherence to privacy laws [19, 2]. Parents' control mechanisms are still inadequate. This adds to privacy concerns because parents may not have the means to monitor or limit their children's data collection and utilization by toys. This is reported to be a major concern of parents, especially in developed economies [20]. Besides that, with their capacity to collect and handle delicate data like location and activity patterns, smart toys can encounter

information leaks, unauthorized access, and even physical safety hazards. In addition to this, privacy frameworks are not standardized, and compliance is inconsistent with privacy laws [21, 22, 23]. This indicates that the security and privacy issues with smart toys are complex and encompass technical, regulatory, and usability concerns. Solving these problems needs better security measures, stricter enforcement of regulations, and better parental control options.

McReynolds et al. [24] reported that Internet-connected toys may record or transmit children's speech, while parents and children may not always understand what data are collected or how the data are used. Chu et al. [18] found that commercially available children's IoT toys can contain network and application vulnerabilities that conflict with privacy and security best practices. Shasha et al. [2] further proposed a threat taxonomy for smart toys and showed that unsafe access or weak protection may expose children to privacy leakage and safety risks.

Parental control for smart toys should be accompanied by visibility of children's interactions, control over data sharing, notification of important events, and means for making children's interactions known to their guardians. Parents should have resources to watch and comprehend their children's interactions with their smart toys. This means access to the information gathered and its usage [25, 8, 9]. For instance, dashboards or interfaces to show parents what their child is doing and sharing with the toy interaction information are crucial [26].

Parental control tools need to enable parents to control and limit information that their child shares with their smart toy or third parties. This is important because of potential privacy violations and misuse of data [25, 8, 27, 21]. Tools available today are inadequate to meet these needs, and having customizable data-sharing preferences [8, 28] is therefore important. If the parents are involved in the sharing of sensitive information, or if there is a possibility that their information is being shared in an insecure way, they should be informed of this. This will enable prompt action to help protect the child's privacy and safety [1, 28].

Tools should help increase parental awareness of privacy risks and offer easy-to-use interfaces for effective privacy management by non-technical users [29, 30]. Parents must have control of what happens to their children, which means making the design of the products more usable and having clear privacy labels. This suggests that there is strong support for the proposed parental control measures, which include visibility, control, notification, and awareness mechanisms to address concerns about the privacy and safety of smart toys. Therefore, monitoring and notification should be considered as practical design requirements for child-oriented IoT systems.

Based on these concerns, the proposed system integrates parental monitoring directly into the robot platform. Instead of only providing a separate mobile application, the system connects the robot, server, web dashboard, AI judgment, and Telegram Bot notification into one workflow. This allows the guardian to easily receive important information without continuously checking the dashboard.

III. SYSTEM DESIGN

A. Overall Architecture

Fig. 1 shows the context diagram of the parental monitoring workflow of the proposed IoT toy. The parental monitoring architecture consists of a robot head unit, a server layer, an AI judgment component, a web dashboard, a behavior logging module, and a Telegram notification module. The robot collects interaction input through microphone and camera modules, while the server coordinates AI processing, dashboard communication, logging, and notification. The guardian accesses the system through the web dashboard or receives Telegram alerts when serious situations, such as injury reports, fear expressions, danger-related messages, allergy-related requests, or direct requests to contact the guardian, are detected.

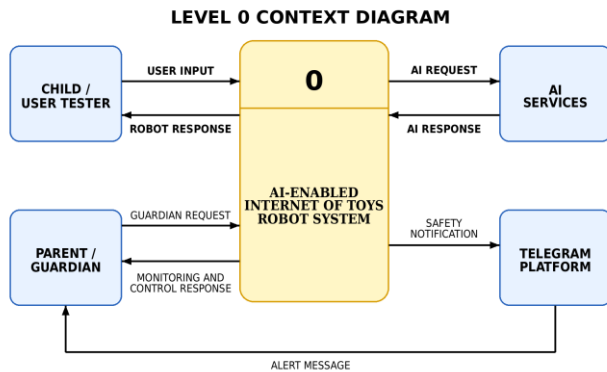


Fig. 1. Context diagram of the parental monitoring workflow.

B. Hardware and Server Components

The robot head unit is based on an ESP32-S3 CAM module and includes a camera, microphone, speaker output, touch input, and display feedback. The mobile base uses an ESP32-C3 controller for wheeled movement. The two parts form a modular robot platform. The Node.js server acts as the central coordination layer between the robot, browser interface, AI services, memory storage, report module, and Telegram Bot.

C. Parental Monitoring Workflow

During normal interaction, the child can communicate with the robot using natural language speech instead of a fixed command list. The interaction can be started through the robot's wake-up mechanism, such as voice activation or touch activation. After activation, the microphone captures the child's speech and sends the audio to the server for speech-to-text processing. The recognized text is then forwarded to the GPT API to generate a context-aware response. Since the GPT API supports multilingual text processing, the robot can support multilingual interaction in principle. However, the actual language performance depends on the speech-to-text module, the selected GPT model, the text-to-speech output, and the availability of support for low-resource languages.

Visual assistance refers to the use of the ESP32-S3 camera to support image-based interaction. For example, when the child asks a visual question such as "What is this?" or asks the robot to look at an object, the camera captures the current image and sends it together with the child's question to the AI service. The AI analyses the visual context and generates a response, which

is then converted into speech and played through the robot speaker.

The AI judgment module is executed after each child-robot interaction. The server provides the module with the child's original input, the AI-generated response, and the optional camera image or visual description. The module then classifies the interaction into two outcomes: "guardian notification required" or "no guardian notification required". A notification is triggered when the interaction contains a direct request to contact a guardian, emotional distress, injury, sickness, danger, stranger-related concern, fire or electrical risk, unsafe food, allergy-related request, or other safety-related condition. If the interaction is a normal conversation, such as asking for a story or asking a general question, the system stores the interaction in the behavior log without sending a Telegram alert.

When a notification is required, the server generates a short summary of the situation and sends it to the guardian through Telegram. The Telegram message includes the child's original input, the AI response, the situation summary, whether an image is attached, and the timestamp. This decision mechanism reduces unnecessary alerts while still notifying the guardian during meaningful safety-related situations.

IV. IMPLEMENTATION

A. Web-Based Monitoring Dashboard

The web-based monitoring dashboard, as shown in Fig. 2, allows the guardian to access the robot through a browser and interact with different monitoring functions. For camera viewing, the guardian clicks the camera or stream button to view the child's surrounding environment through the ESP32-S3 camera. The output is a live or updated camera view, which helps the guardian understand the child's current environment when the guardian is not physically beside the child.

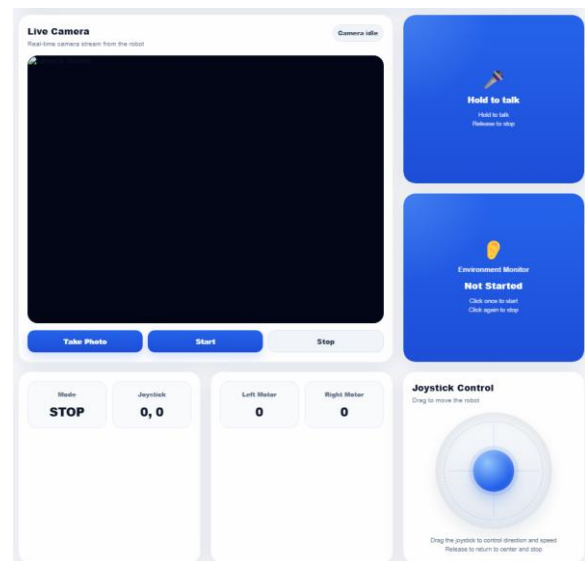


Fig. 2. Web dashboard for camera viewing and remote robot control.

For movement control, the guardian presses the forward, backward, left, or right buttons on the interface. The command is sent from the browser to the server and then forwarded to the ESP32-C3 mobile base. The output is the physical movement of

the robot, allowing the guardian to reposition the robot or observe a different direction remotely.

For AI wake-word control and camera toggle, the guardian can enable or disable selected robot functions from the dashboard. The output is the updated function status shown on the interface. This helps the guardian control when the robot should listen for interaction or activate the camera, depending on the usage situation.

The dashboard also provides links to memory, chat history, and behavior report pages. Through these pages, the guardian can review previous child-robot conversations, safety-related events, and reminders stored, such as allergy information. These outputs help the guardian understand what the child asked, how the robot responded, and whether any important behavior or safety condition occurred.

B. Telegram Guardian Notification

Telegram Bot is used as the guardian notification channel because it supports fast message delivery and can include both text and images. When the system identifies a safety-related event or a guardian contact request, the server sends a structured message to the guardian. The message can include the child's original words, the AI response, a brief situation summary, image availability, and time information. Fig. 3 illustrates an example of the Telegram message generated for a child-to-guardian communication request.

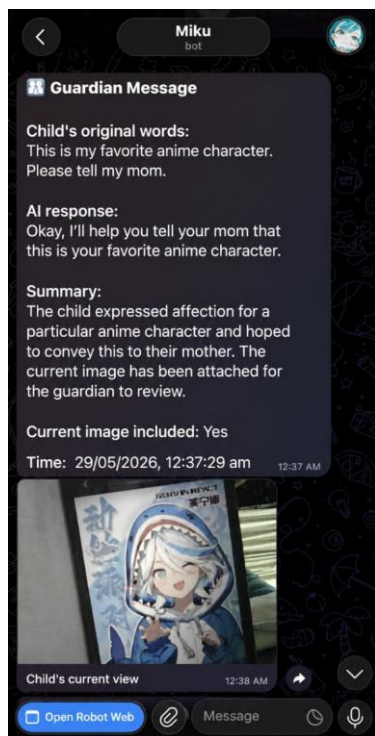


Fig. 3. Telegram notification generated for a child-to-guardian communication request.

C. AI Safety Judgment and Behavior Logging

The AI judgment component operates after each child-robot interaction. The server sends the child's original input, the AI-generated response, and optional visual context from the camera to a judgment prompt. The judgment prompt asks the AI to

classify the interaction into two outcomes: guardian notification required or no guardian notification required. The decision is based on whether the interaction contains safety-related or guardian-related content, such as direct requests to contact a parent, expressions of fear such as "I am scared," injury reports such as "I fell down," dangerous environment descriptions such as "There is fire," and allergy-related questions such as "Can I eat peanuts?"

If guardian notification is required, the system generates a short summary and sends a structured Telegram message to the guardian. The message includes the child's original input, the AI response, the event summary, image availability, and timestamp. If the interaction is a normal conversation, such as asking for a story or asking a general question, the system stores the record in the behavior log without sending a Telegram alert. This mechanism helps reduce unnecessary notifications while still allowing the guardian to receive important safety-related or behavior-related information.

The system also records selected chat history and behavior information so that the guardian can review important events later. Fig. 4 shows the behavior report page used to review previous child-robot interactions and safety-related records. Through this report, the guardian can understand what the child said, how the robot responded, and whether any event required attention.

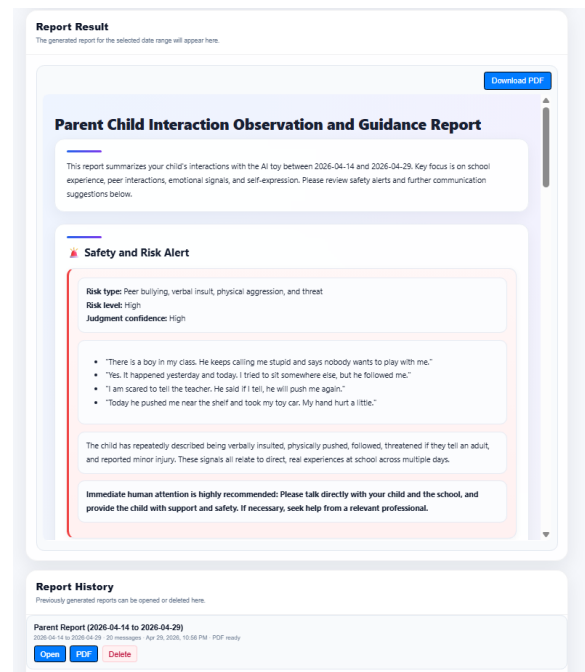


Fig. 4. Behavior report page for reviewing interaction and safety-related events.

D. Allergy Reminder and Remote Intervention

The memory module can store simple child-related information, such as allergy reminders. When the child asks about food that may be unsafe, the system retrieves the stored allergy information and includes it in the AI response. The robot then responds with a warning through speech output, reminding the child to avoid the restricted food. An example of the allergy reminder output is shown in Fig. 5.

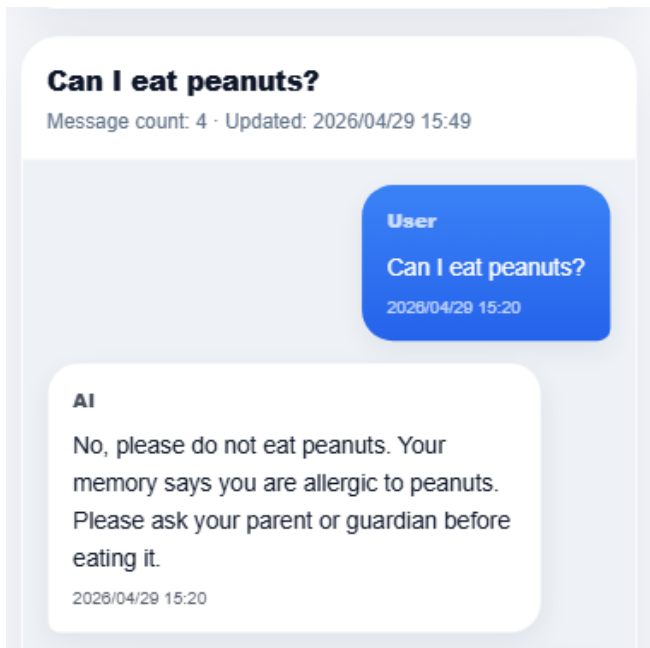


Fig. 5. Allergy reminder output generated based on stored child-related information.

Remote intervention is supported through camera viewing, movement control, and two-way guardian communication. The guardian can first check the camera view to understand the child's surrounding environment. If the guardian needs a different viewing angle, the guardian can use the movement buttons on the dashboard to reposition the robot. If the child needs guidance, the guardian can use the hold-to-talk function to speak through the web interface, and the robot plays the voice message through its speaker to guide the child remotely. Fig. 6 shows the hold-to-talk function used for remote intervention.

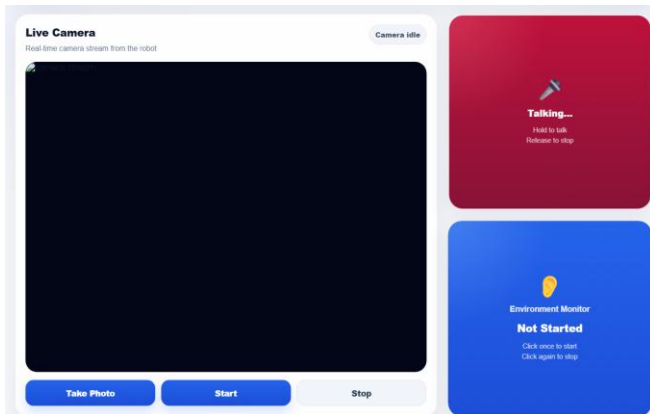


Fig. 6. Two-way guardian communication interface for remote intervention.

V. SCENARIO-BASED TESTING AND RESULTS

Scenario-based testing was conducted to verify whether the parental monitoring functions produced the expected outputs. The testing focused only on monitoring-related features. Each test used a realistic scenario, input, and output, as shown in Table I. The scenarios include guardian contact request, fear expression, injury report, danger warning, allergy reminder, remote monitoring, remote intervention, and behavior review.

TABLE I. SCENARIO-BASED TESTING OF PARENTAL MONITORING FEATURES

Scenario	Input	Output
Guardian contact	Child asks robot to tell mother	Telegram message is sent to guardian
Fear expression	Child says "I am scared"	AI comforts child and alerts guardian
Injury report	Child says "I fell down"	Safety notification is generated
Danger warning	Child says "There is fire"	Warning response and Telegram alert generated
Allergy reminder	Child asks about restricted food	Robot gives allergy warning
Remote monitoring	Guardian opens dashboard	Camera view and control buttons are displayed
Remote intervention	Guardian uses hold-to-talk function	Robot delivers guardian voice guidance to the child
Behavior review	Guardian opens report page	Interaction summary is shown

The supporting screenshot evidence is shown in Fig. 2 for the web-based monitoring dashboard, Fig. 3 for Telegram guardian notification, and Fig. 4 for behavior report review. Additional output evidence is provided in Fig. 5 for the allergy reminder and Fig. 6 for two-way guardian communication. These figures provide supporting evidence for the main outputs as listed in Table I.

The test results show that Telegram notifications were triggered for guardian-contact and safety-related scenarios, while the web dashboard supported remote camera viewing, movement control, and remote intervention. The allergy reminder and behavior report pages also helped the guardian review child-related information and previous interaction records. These results indicate that the proposed system can support guardian awareness and remote intervention in basic child-care scenarios.

VI. DISCUSSION

The main advantage of the system is that the guardian does not need to constantly monitor the web dashboard. Safety-related information can be pushed through Telegram when the AI judgment module detects a meaningful event. Camera viewing, behavior reporting, and remote control provide additional context for the guardian to understand the child's situation and respond when necessary. These features allow the IoT toy to act not only as an interactive robot, but also as an additional awareness and communication channel between the child and the guardian.

The reliance on Connectivity and AI Judgment is a recurring theme, with abstracts underscoring the vulnerabilities introduced by connections with other systems, including cloud-based ones, and on real-time decision-making capabilities [31, 32]. This is in line with the issue of relying on cloud AI and Wi-Fi. There are multiple studies that highlight some of the problems with the accuracy of AI, such as false negatives and false positives. In medical and child well-being, the use of AI systems can be complicated by problems with predictive

accuracy, especially if qualitative or contextual data is lacking [32, 33]. This can result in false alarms or in failure to detect the alarm, as mentioned in the question. AI systems need to be thoroughly tested and have more precise instructions on how to operate to become more reliable. For instance, the need for robust evaluation metrics, post-deployment monitoring, and dynamic testing scenarios is frequently mentioned [34, 35]. These measures can be helpful to improve the safety classification rules and minimize errors.

The privacy issues surrounding the IoToy, including the capturing of sensitive information such as children's voices, images captured by the camera, notes of interactions, and any alerts given, were raised. Currently, it is only a prototype where access to this data is limited to a configured guardian through a web dashboard and a Telegram account, but other security elements such as more robust authentication, encrypted communication, access control, and data retention settings are needed before deployment with children.

IoT devices, including smart toys, often collect sensitive data such as video, audio, and interaction logs, which can expose children to significant privacy risks if not adequately secured [36, 37, 38]. For example, there have been reports of weaknesses in IoT-enabled toys that have led to the unauthorized use of cameras and sensors to capture live images and videos without the user's consent [38, 39, 40]. The current IoToy prototype using the web dashboard and Telegram account to access data emphasizes the need for a more secure approach. Research highlights the need for the use of encryption, multi-factor authentication, and access control to reduce risks of unauthorized access and data breaches [36, 39, 41]. For instance, blockchain authentication and encryption have been suggested to improve the security of IoT toys. One concern is Data Retention and Regulatory Gaps, where IoT devices may not have explicit data retention policies, and there is a lack of transparency regarding who accesses or stores sensitive data. To conclude, although the IoToy prototype restricts data access to guardians, there is a strong need for further improvement in authentication, encryption, and access control to ensure effective protection of children's privacy. Moreover, it is essential to address the regulatory gaps and put in place strong data retention policies to guarantee long-term privacy and security [36, 37, 39, 41].

VII. CONCLUSION

This study presented the design and development of a smart IoT toy with parental monitoring features. The main contribution of this work is the development of a server-assisted IoT toy prototype that connects child-robot interaction with parental monitoring functions. The proposed IoT toy not only provides a joyful play experience and entertainment, but it also helps guardians receive important safety-related information about the child's behavior and surrounding environment. The prototype integrates web-based camera monitoring, remote movement control, AI-based safety judgment, Telegram guardian notification, allergy reminder, behavior logging, and behavior review to support parental monitoring and childcare. Scenario-based testing showed that the system can generate appropriate monitoring outputs, notify guardians, and support remote observation in safety-related situations. Future work will

focus on improving notification accuracy, privacy protection, network robustness, and larger-scale user evaluation with parents and child users.

REFERENCES

- [1] L. G. de Carvalho and M. M. Eler, "Security requirements and tests for smart toys," *Lecture Notes in Business Information Processing*, pp. 291 - 312, 2018.
- [2] S. Shasha, M. Mahmoud, M. Mannan and A. Youssef, "Playing with danger: A taxonomy and evaluation of threats to smart toys," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2986 - 3002, 2019.
- [3] P. Ihmäki and K. Heljakka, "The internet of toys, connectedness and character-based play in early education," *Advances in Intelligent Systems and Computing*, pp. 1079 - 1096, 2019.
- [4] T. Jayaraman, P. Rajkumar, M. Shakunthala, M. Vijayakumar, M. Vimal Kumar and N. Hemavijayaraj, "Eco-friendly IoT-based smart toy automation for interactive learning and engagement," *Proceedings of the 6th International Conference on Electronics and Sustainable Communication Systems*, pp. 1511 - 1515, 2025.
- [5] V. Pavliv, N. Akbari and I. Wagner, "AI-powered smart toys: interactive friends or surveillance devices?," 2025.
- [6] L. Pontes, G. Coutinho, P. C. K. Hung and B. Yankson, "Security in smart toys: A systematic review of literature," 2019.
- [7] O. de Paula Albuquerque, P. C. K. Hung, S. M. Peres, F. Iqbal and M. Fantinato, "A preliminary design of privacy ontology for smart toys," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2024.
- [8] P. C. K. Hung, M. Fantinato and L. Rafferty, "A study of privacy requirements for smart toys," in *Pacific Asia Conference on Information Systems, PACIS 2016 - Proceedings*, 2016.
- [9] P. C. K. Hung, F. Iqbal, S.-C. Huang, M. Melaisi and K. Pang, "A glance of child's play privacy in smart toys," in *Lecture Notes in Computer Science*, 2016, pp. 217-231.
- [10] K. Nikolopoulou, "Internet of toys for young children: Educational value or threat?," in *Research Anthology on Early Childhood Development and School Transition in the Digital Era*, 2022, pp. 85-100.
- [11] L. Rafferty, P. C. K. Hung, M. Fantinato, S. M. Peres, F. Iqbal, S.-Y. Kuo and S.-C. Huang, "Towards a privacy rule conceptual model for smart toys," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2017.
- [12] A. Catala, C. Sylla, A. G. Ozgur, P. Ihmäki and K. Heljakka, "Smart toys, smart tangibles, robots and other smart things for children," in *Extended Abstracts - Proceedings of the 2020 ACM Interaction Design and Children Conference, IDC 2020*, 2020.
- [13] E. Amengual, A. Bibiloni, M. Mascaró and P. Palmer-Rodríguez, "What does the GDPR mean for IoT toys data security and privacy?," in *Advances in Intelligent Systems and Computing*, 2019, pp. 881-889.
- [14] S. Allana and S. Chawla, "ChildShield: A rating system for assessing privacy and security of internet of toys," *Telematics and Informatics*, 2021.
- [15] S. Chaudron, D. Geneiatakis, I. Kounelis and R. Di Gioia, "Testing internet of toys designs to improve privacy and security," in *Studies in Childhood and Youth*, 2019, pp. 223-239.
- [16] A. Manches and L. Plowman, "Smart toys and children's understanding of personal data," *International Journal of Child-Computer Interaction*, 2021.
- [17] V. Pavliv, L. Lazri, J. Büchele and I. Wagner, "'Why is the sky blue?': On the feasibility of privacy-friendly conversational LLM smart toys," in *Lecture Notes in Computer Science*, 2026, pp. 49-65.
- [18] G. Chu, N. Aphorpe and N. Feamster, "Security and privacy analyses of internet of things children's toys," *IEEE Internet of Things Journal*, pp. 978-985, 2019.
- [19] M. Mahmoud, M. Z. Hossen, H. Barakat, M. Mannan and A. Youssef, "Towards a comprehensive analytical framework for smart toy privacy practices," in *ACM International Conference Proceeding Series*, 2018.
- [20] F. M. Pinheiro Amâncio, A. P. Souza, M. Fantinato, S. M. Peres, P. C. K. Hung, L. G. Coutinho do Rêgo and J. Roa, "Parental perception of

- children's privacy in smart toys in countries of different economic levels," *Technology in Society*, 2023.
- [21] L. G. de Carvalho and M. M. Eler, "Security tests for smart toys," in *ICEIS 2018 - Proceedings of the 20th International Conference on Enterprise Information Systems*, 2018.
- [22] O. D. P. Albuquerque, M. Fantinato, J. Kelner and A. P. de Albuquerque, "Privacy in smart toys: Risks and proposed solutions," *Electronic Commerce Research and Applications*, vol. 39, 2020.
- [23] P.-C. Lin, B. Yankson, Z. Lu and P. C. K. Hung, "Children privacy identification system in LINE chatbot for smart toys," in *IEEE International Conference on Cloud Computing, CLOUD*, 2019.
- [24] E. McReynolds, S. Hubbard, T. Lau, A. Saraf, M. Cakmak and F. Roesner, "Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems," 2017.
- [25] O. D. P. Albuquerque, M. Fantinato, M. M. Eler, S. M. Peres and P. C. K. Hung, "A study of parental control requirements for smart toys," in *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, 2020.
- [26] M. L. Jones and K. Meurer, "Can (and should) Hello Barbie keep a secret?," in *2016 IEEE International Symposium on Ethics in Engineering, Science and Technology, ETHICS 2016*, 2016.
- [27] L. G. de Carvalho, M. Fantinato and M. M. Eler, "Security requirements identification and prioritization for smart toys," *Electronic Commerce Research and Applications*, 2020.
- [28] O. de Paula Albuquerque, M. Fantinato, P. C. K. Hung, S. M. Peres, F. Iqbal, U. Rehman and M. U. Shah, "Recommendations for a smart toy parental control tool," *Journal of Supercomputing*, pp. 11156-11194, 2022.
- [29] A. de Lima Salgado, R. P. de Mattos Fortes, R. R. de Oliveira and A. P. Freire, "Usability heuristics on parental privacy controls for smart toys: From an exploratory map to a confirmatory research," *Electronic Commerce Research and Applications*, 2020.
- [30] A. de Lima Salgado, F. S. Dias, J. P. R. Mattos, R. P. de Mattos Fortes and P. C. K. Hung, "Smart toys and children's privacy: Usable privacy policy insights from a card sorting experiment," in *SIGDOC 2019 - Proceedings of the 37th ACM International Conference on the Design of Communication*, 2019.
- [31] S. Vignesh, D. Sabarevason and A. R. Sachin, "IoT-enabled smart eyewear: A real-time platform for comprehensive child monitoring and proactive intervention," in *3rd International Conference on Emerging Applications of Material Science and Technology, ICEAMST 2025*, 2025.
- [32] P. van Dommelen, Y. C. S. Frans, E. Vlasblom, J. Bouwman and J. A. de Wilde, "AI in childhood development monitoring: Attitudes, needs, and concerns in Dutch youth healthcare," in *Studies in Health Technology and Informatics*, 2025, pp. 158-162.
- [33] S. Kim and Y. Yoon, "Child protection in the digital age in South Korea: Professionals' perceptions on artificial intelligence (AI) and big data efficacy and ethical challenges," *Child and Family Social Work*, 2026.
- [34] G. Ragone, S. Tibidò, P. Buono, R. Lanzilotti, A. Ragone and M. T. Baldassarre, "Evaluating the gaps in existing AI ethics frameworks for children," in *CHIItaly 2025 - Proceedings of the 16th Biannual Conference of the Italian SIGCHI Chapter*, 2025.
- [35] Y. Wang, W. Fu, Y. Zhang, D. Wang, Y. Gu, W. Wang, H. Xu, X. Ge, C. Ye, J. Fang, L. Su, J. Wang, W. He, X. Zhang and R. Feng, "Constructing and implementing a performance evaluation indicator set for artificial intelligence decision support systems in pediatric outpatient clinics: An observational study," *Scientific Reports*, 2024.
- [36] D. Rivera, A. Garcia, M. L. Martin-Ruiz, B. Alarcos, J. R. Velasco and A. Gomez Oliva, "Secure communications and protected data for a internet of things smart toy platform," *IEEE Internet of Things Journal*, pp. 3785-3795, 2019.
- [37] E. Haber, "The internet of children: Protecting children's privacy in a hyper-connected world," *University of Illinois Law Review*, pp. 1209-1248, 2020.
- [38] J. Streiff, O. Kenny, S. Das, A. Leeth and L. J. Camp, "Poster abstract: Who's watching your child? Exploring home security risks with smart toy bears," in *Proceedings - ACM/IEEE International Conference on Internet of Things Design and Implementation, IoTDI 2018*, 2018.
- [39] J. Streiff, S. Das and J. Cannon, "Overpowered and underprotected toys empowering parents with tools to protect their children," in *Proceedings - 2019 IEEE 5th International Conference on Collaboration and Internet Computing, CIC 2019*, 2019.
- [40] J. Streiff, N. Noah and S. Das, "A call for a new privacy & security regime for IoT smart toys," in *5th IEEE Conference on Dependable and Secure Computing, DSC 2022 and SECOC 2022 Workshop, PASS4IoT 2022 Workshop SICSA International Paper/Poster Competition in Cybersecurity*, 2022.
- [41] A. Alkhatib, L. Albdour, S. Fayyad and H. Ali, "Blockchain-enhanced multi-factor authentication for securing IoT children's toys," *International Journal of Computational and Experimental Science and Engineering*, pp. 1041-1049, 2024.