Hidden in Plain Speech: A Covert Safety System for Foreign Residents via Ambient Speech Recognition

Lee Guhn
leeguhn@kaist.ac.kr

Tulanova Dilnurakhon
dilnura17102004@kaist.ac.kr

Baek Schein
schein.baek@kaist.ac.kr

Yang Dongyeon
cori1219@kaist.ac.kr

KAIST
Daejeon, South Korea

Abstract

Foreign residents and multicultural families often face compounded risks in domestic and professional environments where language barriers and physical surveillance limit their ability to report abuse. In situations of immediate threat, accessing a mobile phone is frequently dangerous or impossible, leaving victims without a viable means to signal distress. To address this gap, we present a voice-activated, private IoT system designed to operate covertly using ambient speech recognition. By allowing users to embed predefined rescue keywords into natural conversation in their native language, the system leverages the linguistic gap between the victim and the aggressor to trigger a silent alert and capture audio evidence. Our evaluation with international residents (N=8) revealed participants perceive these hands-free and linguistic camouflage features as advantages over traditional mobile safety applications for navigating high-stakes conflicts. Participants also provided insights for future improvements, including the need for multimodal triggers and size miniaturization. This study demonstrates the potential of ambient computing to provide discreet, user-centered safety nets for vulnerable populations.

Keywords: IoT based emergency support, Ambient Intelligence, Domestic Safety, Offline Speech Recognition, Covert Alert Systems.

1 INTRODUCTION

The increasing population of foreign residents and multicultural families in Korea faces specific safety vulnerabilities compounded by language barriers and social isolation [1]. In high-stakes scenarios like domestic violence or workplace abuse, victims need to signal for help but cannot safely access mobile devices due to direct physical surveillance [6]. Perpetrators frequently monitor movements, rendering the manual manipulation of a smartphone impossible or dangerous. Consequently, this inability to discreetly request assistance significantly elevates the risk of injury and prolonged victimization.

Current technological interventions struggle to address these specific constraints. While smart home devices provide connectivity, research indicates they often introduce privacy risks and can be weaponized for coercive control within domestic environments [4]. Similarly, a review of existing mobile safety applications reveals a reliance on visual attention and manual interaction to trigger SOS alerts and actions that are liable to escalate conflict when under observation [8]. While web-based "quick exit" mechanisms offer some digital discretion [5], there remains a critical lack of physical safety systems that operate offline and require no tactile interaction to function.

To bridge this gap, we propose a voice-activated emergency support system that operates covertly via ambient speech recognition. Unlike standard voice assistants, our approach leverages the linguistic difference between the user and aggressors as a security feature. By embedding predefined "rescue keywords" into natural conversation in their native language, users can create a layer of hidden communication. This allows for the injection of help requests directly within a shared physical space without raising suspicion. While initially designed to mitigate domestic conflict, our findings suggest broader applicability, positioning the system as a critical tool for navigating workplace harassment and public safety threats.

2 MOTIVATION

2.1 Social Context

South Korea is undergoing a significant demographic shift and evolving into a multicultural society driven by an influx of foreign workers and international marriages [9]. While government policies have improved to

support economic integration through equal pay regulations and visa support, social integration remains a challenge. Foreign residents, particularly those in manual labor or service industries, often report a disconnect between legal protections and their daily lived experiences. As economic pressures mount, societal attitudes toward immigrants have reportedly shifted from curiosity and kindness to indifference or hostility [7]. This creates an environment where foreign residents feel increasingly isolated and vulnerable to friction in both public and private spheres.

2.2 Formative Study

We conducted formative interviews with three long-term Chinese female migrant residents. One participant specifically identified as Korean-Chinese (Chaoxianzu) holding an F-4 visa, while the others were Chinese nationals with long-term residency in Korea. Their experiences spanned from 15 to 20 years and revealed critical dimensions of vulnerability that standard safety tools fail to address.

A key finding from these interviews was that vulnerability is not limited to the home environment. One participant who works in food processing described her job as intensive manual labor where mobile phone usage is strictly prohibited during shifts. Despite facing verbal harassment and hostility from older co-workers, she lacks the means to document these incidents or contact help immediately. This highlighted a crucial design constraint because emergency tools must function without physical access to a smartphone. Many vulnerable workers are physically or policy-bound from using mobile devices during critical moments.

One participant highlighted that family conflict and discrimination from Korean in-laws remain persistent and under-addressed issues. She noted a distinct lack of resources and support systems for foreign spouses facing domestic strife. This reinforced the need for a system that is discreet enough to exist within the home without triggering aggression from family members. Additionally, participants noted that discrimination has evolved from overt institutional barriers to subtle and ubiquitous social friction in public spaces, necessitating a safety tool that is adaptable to different contexts.

2.3 Beyond the Home

Initially, this research focused exclusively on domestic violence intervention for multicultural families. However, the formative interviews revealed that the core constraint is the inability to freely manipulate a communication device due to surveillance or restriction. This is a shared reality in both domestic abuse scenarios and exploitative workplace environments. Consequently, our research focus expanded to explore how we can address the problem of silenced distress by developing a ubiquitous and hands-free safety net. The system is designed not just as a panic button for the home but as a discreet and ambient witness.

3 RELATED WORK

3.1 Coercive Control in Smart Homes

Smart home technologies offer convenience but frequently exacerbate domestic power imbalances by design. Research highlights that these systems are often built for a primary user who retains unilateral control over monitoring and regulation [4]. This setup inadvertently provides abusers with sophisticated tools for "Technology-Enabled Coercive Control" (TECC) [3]. For foreign residents, this power imbalance is often compounded by linguistic and cultural barriers that prevent them from accessing or understanding the controls of their own home environments.

While recent innovations like PrivacyCube explore data physicalization to increase transparency around data collection [2], such transparency-focused approaches are insufficient for victims who lack the agency to act on that information. In abusive environments, particularly for socially isolated immigrants, the primary need is not just awareness of surveillance but opacity and concealment. These tools allow them to operate safely underneath the radar of the aggressor.

3.2 Limitations of Mobile Safety

The current landscape of digital safety interventions relies heavily on mobile applications which presents a significant barrier for vulnerable populations. A systematic review of 178 safety apps found that the majority prioritize GPS tracking and SOS alerts [8]. These functionalities demand visual attention and manual interaction. This requirement becomes a liability in high-stakes situations where victims are physically restrained or under direct surveillance [6]. In these scenarios, handling a device is dangerous or impossible.

The "digital safety dilemma" describes how remote support models presume victims have access to safe and private devices. This is a condition frequently unmet for immigrants living in shared or monitored spaces. Consequently, existing care infrastructures struggle to reach individuals who cannot safely navigate a smartphone interface during a crisis [8]. This highlights a critical gap for hands-free and accessible interventions.

3.3 From Digital to Physical Defense

To mitigate the risks of digital surveillance, Human-Computer Interaction (HCI) researchers have developed "quick exit" buttons for websites [5]. These allow users to instantly hide sensitive content and minimize digital traces. These mechanisms acknowledge that for victims of abuse speed and stealth are survival requirements.

However, current research predominantly focuses on these principles within the digital realm of web browsers. This leaves a void in physical safety tools. There is a lack of research translating these quick exit principles into physical and ambient defenses for the offline world. This gap is particularly acute for foreign residents who must navigate professional and public friction in an unfamiliar environment. For them, the ability to exit a dangerous situation or signal for help without escalating conflict is essential.

While extensive research documents how perpetrators weaponize technology to worsen abuse, there is a distinct scarcity of research focused on developing defensive tools that empower victims to resist. This gap is most critical for foreign residents whose safety is compromised not just by interpersonal conflict but by structural isolation and language barriers. Understanding the aggressor's perspective is also critical for designing safer systems. Research into abusive partners' narratives reveals that they often view their controlling behaviors as provoked or impulsive [11].

This suggests that safety interventions must be non-provocative and discreet to avoid escalating conflict. Our work addresses this by moving beyond the analysis of abuse patterns to the design of active defense. We adapt the principles of stealth and immediate access into a voice-activated system that leverages the user's native language as a shield. This provides a safety net that operates independently of the abuser's control and without the need for physical device interaction.

4 SYSTEM DESIGN

4.1 System Overview

The proposed solution is a stationary, IoT-based emergency support system designed for domestic environments where mobile phone usage may be restricted or monitored. Unlike wearable or mobile app-based solutions, this system is intended for permanent installation in high-risk zones within the home, such as the living room or kitchen. It operates as an "always-on" background process that utilizes offline speech recognition to detect specific user-defined "rescue keywords." Upon detecting a keyword, the system triggers a covert alert sequence. It automatically records the audio context following the trigger and transmits this evidence via email to a trusted contact. By processing speech data locally and offline, the system prioritizes user privacy and data security, ensuring that no audio is transmitted to the cloud until a confirmed emergency event occurs.

4.2 Interaction Flow

The interaction design prioritizes safety and discretion through a hands-free workflow:

1. *Configuration.* During a safe period, the user accesses a local frontend interface to register a specific rescue keyword. This keyword is ideally selected from the user's native language or a contextually distinct phrase that is unlikely to be triggered accidentally in daily conversation.

2. *Passive Monitoring.* Once configured, the system enters a listening state. It continuously processes ambient audio but discards data immediately if the keyword is not detected, ensuring privacy.

3. *Activation.* In a conflict situation, the user utters the rescue keyword embedded within a natural sentence (e.g., speaking to a family member in their native tongue).

4. *Response.* The system detects the keyword, initiates an audio recording of the subsequent conversation, and sends an SMTP-based email alert to the pre-designated contact. The email includes the audio file attachment, providing the recipient with immediate context and evidence of the situation.

4.3 Implementation

Figure 1: Raspberry Pi used for offline speech processing.

The prototype is built on a Raspberry Pi single-board computer (Fig. 1), chosen for its compact form factor and ability to run continuously as a stationary domestic appliance. The software architecture consists of a lightweight frontend for configuration and a

Python-based backend handling the core logic.

The core listening capability is powered by VOSK, an offline, open-source speech recognition toolkit. We selected VOSK for its ability to run locally on edge devices without internet dependency, eliminating latency and privacy risks associated with cloud-based APIs. The system is configured with a lightweight language model (approx. 50MB) suitable for real-time inference on the Raspberry Pi. This model supports over 20 languages, allowing the system to be tailored to the specific linguistic background of the target user (e.g., a specific dialect or foreign language model).

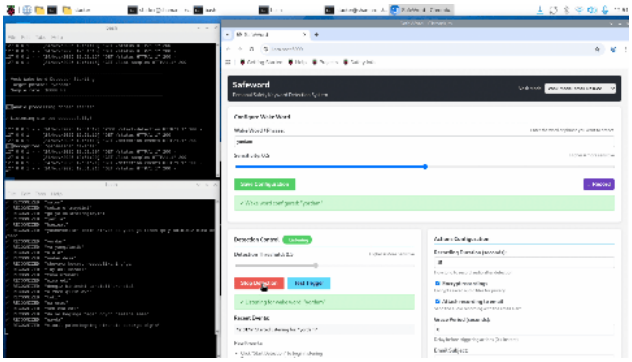

Figure 2: Keyword configuration and ambient logging.

The backend script monitors the VOSK data stream for the designated keyword. Upon a match, it triggers a system-level recording using ALSA (Advanced Linux Sound Architecture) tools and packages the resulting `.aac` file into a MIME-multipart email, which is dispatched via a standard SMTP server to the trusted contact (Fig. 2).

5 EVALUATION

To validate the design principles of the system, specifically its "hands-free" interaction model and covert nature, we designed a controlled and scenario-based study. The goal was not to simulate the trauma of abuse but to evaluate the usability of the configuration process, the reliability of the keyword detection, and the psychological sense of security provided by the system compared to traditional safety tools.

5.1 Participant Demographic

To evaluate the usability and safety of the proposed system, we recruited a total of eight participants (N=8) from the international community located within the Korea Advanced Institute of Science and Technology (KAIST). The study cohort was comprised of both international students and researchers hailing from a diverse array of cultural backgrounds, with specific representation from countries including India, Vietnam, and Indonesia. Regarding demographic composition, the group was gender-mixed and included individuals spanning an age range from their early 20s to their mid-30s.

This specific demographic was selected to represent foreign residents who are most likely to face linguistic isolation in Korea. By recruiting participants who are non-native Korean speakers, we tested the effectiveness of the system in leveraging a "linguistic gap" by using a native language keyword to trigger a rescue signal without alerting a potential aggressor who does not understand that language.

5.2 Study Procedure

The evaluation was conducted as a single-session study of three distinct phases. The structure was designed to guide the participant from system setup to a simulated emergency interaction.

Researchers introduced the "always-on" listening prototype and instructed participants to configure the system themselves. This phase was crucial for testing the personalization features. Participants were asked to select a unique keyword. They were encouraged to choose a word that felt natural to them, such as a term in their native language or a context-specific word (e.g., "Oven," "Bachao") that could be easily camouflaged in a sentence. Additionally, they configured the recording duration (30 to 60 seconds) to determine how long the system should capture audio after activation.

Once configured, participants tested the system by integrating their chosen keyword into natural sentences. They were asked to vary their tonal contexts, such as switching between casual, slow speech and faster, more urgent speech, to verify the responsiveness of the system and its ability to detect the trigger without false negatives. Participants waited for the preset recording duration to elapse and then accessed their personal email accounts to confirm the successful receipt of the recorded audio file.

To assess the system's efficacy, we employed a mixed-methods approach combining quantitative usability metrics with qualitative inquiry. Participants completed a survey using a 5-point Likert scale designed to measure two core dimensions: system intuitiveness and psychological security. The usability questions focused on the ease of configuring and remembering the keyword, as well as the naturalness of integrating it into a conversation without disrupting the flow. Simultaneously, the safety-oriented questions assessed the participants' perceived level of protection, specifically asking whether voice activation felt safer than physical smartphone interaction and if they were confident their rescue attempt remained undetected by the simulated "abuser."

6 RESULTS

6.1 Quantitative Results

Participants rated the system across eight criteria using a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). The results indicate a high degree of acceptance for the voice-based interaction model, with high consistency across the expanded participant group.

- *Intuitiveness and Ease of Use.* The system received high marks for intuitiveness (Mean $\approx$ 4.8/5). Participants consistently reported that the setup process was "easy to remember" and that the system could be used "naturally without interrupting the conversation flow" (rated 4/5 or 5/5 by most).
- *Safety vs. Smartphones.* When asked if "using voice was safer than touching a smartphone in this scenario," participants overwhelmingly agreed (Mean $\approx$ 4.8/5). This validates the core design premise that physical device manipulation is a liability in conflict situations.
- *Discreetness.* Participants reported high confidence (Mean $\approx$ 4.6/5) that a potential abuser would not notice the rescue attempt.
- *Helpfulness.* While generally rated high, there was some variance. One participant (P6) rated the system's helpfulness in domestic conflicts at 3/5, noting that while the voice attempt is safe, "actual wearable buttons can be more effective in concealing" in certain physical confrontations, highlighting a desire for multimodal functionalities.

6.2 Qualitative Insights

The semi-structured interviews revealed three primary themes regarding the system's value proposition and areas for future development.

When compared to existing emergency applications that require shaking a phone or pressing a specific button, participants identified the "hands-free" nature of our system as its most significant advantage. Participant P1 noted how in a conflict, "you may not find your phone around, or making an action [to reach for it] could be more suspicious." P6 succinctly described the advantage as "verbal, easy," reinforcing that removing the physical friction of locating a device is critical. P4 emphasized the psychological comfort of the system, noting that voice activation felt "safer and more comforting" because it removes the need for physical engagement, which might be restricted by an aggressor.

The study validated the hypothesis that linguistic variance creates a layer of security. Participants utilized words like "Bachao" (Help in Hindi) or context-specific terms like "Oven" (P4) to mask the alert. P8 noted that while the situation of domestic conflict itself causes anxiety, using the system did not add to that stress: "The chance of him [the abuser] knowing my language would be really low... so the word itself wouldn't cause any more stress." P6 also reported feeling "no anxiety" or hesitation during the mock scenario, suggesting that the system successfully lowers the barrier to seeking help by leveraging the user's cultural identity as a defensive tool.

Participants provided critical feedback for refining the system for long-term deployment, focusing on reliability and control:

- *Granularity and Cancellation.* P6 introduced the concept of "critical levels," suggesting the system should support multiple keywords for different severity scenarios. She also emphasized the need for a "cancel option" or a way to "double confirm" to avoid sending false alarms, a sentiment echoed by P2.
- *Redundancy.* The desire for multiple triggers was common. P7 and P6 both suggested allowing "multiple words for the same purpose" to prevent forgetting a single keyword under stress.
- *Multi-Modal Feedback.* P4 and P3 suggested that the system could trigger secondary actions, such as a "fake call" to the user's phone to provide an excuse to leave the room, or real-time location sharing alongside the audio recording.
- *Wearability.* P5 and P7 emphasized the need for the device to be inconspicuous and durable. Suggestions included integrating the technology into wearable items like "sticky patches" to ensure protection extends beyond the home.

7 DISCUSSION

Our study strongly validates the hypothesis that removing physical device interaction reduces the burden on victims during a crisis. Participants identified the "hands-free" nature of the system as a critical advantage because locating and unlocking a smartphone creates a dangerous liability in conflict scenarios. Qualitative feedback highlighted a distinct sense of relief among users who noted that voice activation felt "safer and more comforting" by bypassing the need to conceal actions from an aggressor. This suggests that non-tactile safety tools can alleviate the anxiety of being monitored and empower users to act rather than remain passive.

The interviews further confirmed the efficacy of leveraging the "linguistic gap" as a security feature.

Participants reported that using a native language keyword like "Bachao" or context-specific terms allowed them to embed rescue requests into natural conversation without raising suspicion. This validates our design choice to utilize the user's cultural identity as a defensive shield. By transforming linguistic isolation from a vulnerability into a mechanism for covert signaling, the system provides a layer of security that standard panic buttons cannot match. The high confidence among participants that an abuser would not detect the rescue attempt underscores the potential of this approach to function safely within the domestic sphere.

This research aimed to solve the problem of "silenced distress" where victims of domestic or workplace abuse are unable to access communication channels due to surveillance or physical restriction. Our system addresses this gap by functioning as an ambient witness that requires no physical contact. Current safety infrastructures largely suffer from the "digital safety dilemma" because they presume victims have private, unfettered access to their devices [8]. This condition is rarely met in abusive relationships or exploitative labor conditions. By shifting the interaction modality from manual input to ambient speech, our solution provides a necessary intervention for high-stakes environments where holding a phone is impossible.

Moreover, the system specifically targets the underaddressed intersection of safety and migration. While general safety tools exist, they fail to account for compounded risks faced by foreign residents such as language barriers and lack of social support. Our solution fills this void by creating a safety net that operates independently of the abuser's control and creates a bridge to the outside world using the victim's own language. It moves beyond the concept of a simple panic button to establish a persistent and low-friction lifeline. This ensures that the most vulnerable populations have a method to document abuse and request help without escalating the immediate physical threat.

Our system diverges significantly from existing mobile safety applications that rely predominantly on GPS tracking and manual SOS activation [8]. While those tools are effective in public spaces where the user has freedom of movement, they are fundamentally flawed in domestic coercion scenarios where visual attention and manual dexterity are restricted. Unlike apps that demand the user's focus, our system adopts an "eyes-free" and "hands-free" approach similar to smart speakers but re-engineered for privacy. We demonstrate how safety tools can be designed to operate peripherally and allow the user to maintain social and physical situational awareness while triggering a rescue protocol.

Our work extends the concept of "quick exit" mechanisms from web browsers into the physical domain [5]. While existing research has focused on digital stealth to hide browsing history, there has been a lack of research on physical tools that offer similar capabilities for real-world confrontations. Using an offline first and edge-computing architecture, we mitigate the surveillance risks inherent in cloud-connected devices, addressing transparency concerns often found in IoT systems [2]. Our findings align with the need to support workers in hostile environments, offering a physical countermeasure to workplace harassment that complements existing educational and training interventions [10]. Finally, while previous work has explored designing training to address workplace harassment [11], our findings suggest that our system could serve as a complementary physical safety tool for service workers described in our supplementary interviews.

8 LIMITATIONS & FUTURE WORK

A primary limitation of the current prototype involves the physical constraints imposed by the hardware. The system currently relies on a standard Raspberry Pi, resulting in a relatively bulky and stationary form factor. This restricts the deployment of the device to fixed domestic environments where it must be deliberately concealed, such as under a table or behind a bed frame, to remain undetected by an aggressor. Consequently, the current design creates a protection gap once the user leaves the home. This prevents the system from acting as a safety net in dynamic public spaces where foreign residents frequently encounter harassment and discrimination.

The demographic composition of our formal study also presents a limitation regarding generalizability, as we primarily recruited international students within a university setting. To broaden our perspective, we conducted supplementary interviews with two Vietnamese service workers to gauge the applicability of the system in customer-facing roles. These individuals affirmed the utility of the system and expressed a clear willingness to adopt it for managing workplace harassment. They noted that the technology would be most effective for their needs if adapted into a discreet wearable form factor, such as a pendant or necklace. This modification would allow them to maintain access to the safety mechanism while moving freely between tables without drawing attention from customers or supervisors.

Future iterations of this research will prioritize the miniaturization of the hardware to address these mobility and concealment opportunities. We aim to transition the system from a stationary appliance to a wearable device to fulfill the needs identified by the

service workers we interviewed. This evolution would extend the safety perimeter from the domestic sphere to the workplace and public transit. Additionally, we intend to implement the software refinements requested by our study participants. This includes developing a cancellation mechanism to prevent false positives and integrating multi-modal feedback features, such as triggering a fake incoming call to provide the user with a non-confrontational excuse to exit a dangerous situation. These enhancements will be critical in transforming the prototype into a robust and ubiquitous personal safety tool.

9 CONCLUSION

The growing population of foreign residents and multicultural families in Korea faces compounded safety risks due to language barriers and social isolation, particularly within domestic conflict situations. Current mobile safety applications, which predominantly require visual attention and manual interaction, often fail in these high-stakes scenarios where a perpetrator may be monitoring physical movements. To address this critical gap, we introduce a voice-activated, IoT-based emergency support system designed for covert operation through ambient speech recognition. Our approach leverages the linguistic gap between the user and potential aggressors by allowing victims to embed predefined "rescue keywords" into natural conversation in their native language.

We implemented a privacy-centric prototype using a Raspberry Pi and the offline VOSK speech recognition engine which was subsequently evaluated (N=8) through scenario-based testing with international residents. The results indicate that participants perceive hands-free activation as significantly safer and more accessible than touch-based methods during crises. Furthermore, the study yielded critical insights for future iterations, such as the need for multi-level triggers and deceptive features like fake phone calls. Ultimately, this work demonstrates the potential of ambient computing to provide discreet, user-centered safety nets for vulnerable populations.

References

[1] Apthorpe, N., et al. "You, me, and IoT: How internet-connected consumer devices affect interpersonal relationships." *ACM Transactions on Internet of Things*, 3.4 (2022): 1-29.

[2] Bayan, A. M., Nalin, A., Yasar, M., Mohammed. A, Omar, R., and Charith, P. 2025. PrivacyCube: Data Physicalization for Enhancing Privacy Awareness in IoT. In *ACM Transactions on Internet of Things, Vol. 2, Article 12*, 35 pages. https://doi.org/10.1145/3722232

[3] Dana, C., and Natalie, D. 2021. New tools, old abuse: Technology-Enabled Coercive Control (TECC). *Geoforum 126 (2021)*, 224–232. https://doi.org/10.1016/j.geoforum.2021.08.002

[4] Dana, M., and Charlynn, M. 2021. Standing in the Way of Control: A Call to Action to Prevent Abuse through Better Design of Smart Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 332, 1–14. https://doi.org/10.1145/3411764.3445114

[5] Kieron Ivy Turk and Alice Hutchings. 2023. Click Here to Exit: An Evaluation of Quick Exit Buttons. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 547, 1–15. https://doi.org/10.1145/3544548.3581078

[6] Lauren, B., Jessica, H., Tom, Gomersall., Gillian, K., Graham, G., and Andrew, D. J. 2023. The Networking of Abuse: Intimate Partner Violence and the Use of Social Technologies. *Criminal Justice and Behavior 51, 2*, 266–285. https://doi.org/10.1177/00938548231206827

[7] Lee, D., Kim, H. J., and Kang, M. M. 2024. Examining the Role of Social Capital and Socioeconomic Status on Anti-Foreigner Sentiment in South Korea. *Korea Observer 55, 1*, 131–158. https://doi.org/10.29152/KOIKS.2024.55.L131

[8] Md. Hasan, R., Nabila, G. U., Priti, C., Roksana, M. M., Aftab, A., Md. S. Shomik, Syeda, E. A., Ahmed, T. H., and Ahmed, E. R. 2025. Mobile Apps to Prevent Violence Against Women and Girls (VAWG): Systematic App Research and Content Analysis. *JMIR Formative Research 9 (2025)*, e66247. https://doi.org/10.2196/66247

[9] National Geographic Information Institute. n.d. Growth of Multicultural Households. *National Atlas of Korea*.

[10] Rosanna, B., Patrick, O., and Rob, C. 2018. "That Really Pushes My Buttons": Designing Bullying and Harassment Training for the Workplace. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18). Association for Computing Machinery, New York, NY, USA, Paper 235, 1–14. https://doi.org/10.1145/3173574.3173809

[11] Rosanna, F. B. 2024. Abusive Partner Perspectives on Technology Abuse: Implications for Community-based Violence Prevention. In *Proceedings of the ACM on Human-Computer Interaction, Volume 8, CSCW1, Article 15*, 25 pages. https://doi.org/10.1145/3637292