Research Proposal: Privacy and Security of Data Concerns of IoT Technologies for Visually Impaired People

Aitkazy B., Bekbulat A., Baktash A.P., Kurmanbekov A., Turtulov R.

Instructor: Altynbek Seitenov

MiII 3222: Research Methods and Tools

SE-2312, Astana IT University

September 2025

Introduction

Background and Context

IoT-oriented assistive technology such as smart canes and wearable navigation systems use sensors (e.g., GPS, ultrasonic, RFID) and artificial intelligence (AI) for real-time obstacle detection and orientation of vision-impaired individuals (Casanova et al., 2025; Farooq et al., 2022). These devices employ networks of connected devices thorough data acquisition that enable tools for path planning and audio and touch feedback for navigation (Lavric et al., 2024). For example, smart canes use ultrasonic sensors to detect obstacles to make the assumption that wearable devices using light visible communication (VLC) improve indoor location (Kovacs et al., 2025). This technology development falls in line with paradigms of ambient assisted living that are aimed at the social and economic inclusion of impaired people (Rochford, 2019). More recently, the introduction of AI-enabled systems such as those dating from effective visual question answering (VQA) and deep learning are improving the accuracy and personalising tools for navigation aids (Srinivasaiah et al., 2024). However, the necessity for cloud-inhabiting computation and devices which enable wireless protocols (e.g. Bluetooth, Wi-Fi) complicate the already existing problems of data security and privacy especially for the vulnerable users of technologies dictated by such devices to have autonomy on an everyday level.

Problem Statement

While beneficial schemes exist to compliment poor eyesight, IoT-assisted devices that lead such populations face gravissima privacy problems and security issues. It has been shown that such devices capture essential data such as location and movements or otherwise, but do this more often than not without the entities of robust defends, and are therefore liable to grey-scale effects such as data-breach and Hack and implent access unduly (Dian et al., 2020; Semary et al., 2024). For instance, instances of unencrypted protocols such as Bluetooth or Zigbee fall prey to eavesdropping and spoofing, which may lead to a scenario in which false alerts are generated resulting in confusion and accidents (Farooq et al., 2022). Accordingly, there are technical limitations associated with GPS (e.g., loss of availability in urban settings) or the blocking of ultrasonic signals by walls, leading to reduced navigation efficacy and increased risk of collision (Han et al., 2024; Rosiak et al., 2024). It has been noted that some systems have slow response times (for example, 260 ms on a range of 50 cm for obstacle avoidance), leading to further concerns about safety (Gonzales-Saavedra et al., 2025).

Though encryption schemes and blockchain solutions exist, their incorporation in devices constrained by resources, such as IoT devices generally, is limited, with few exceptions in terms of security versus accessibility for non-visual interfaces (Okolo et al., 2024). Moreover, there is a lack of standardization with respect to validation in real situations, resulting in a lack of device reliability and therefore lack of confidence among users supporting overall use (Casanova et al., 2025). Such situations result in a risk for user safety and autonomy, necessitating research into the development of safe and user-centric solutions.

Research Questions

This research is driven by the following questions:

1. How do security threats, such as eavesdropping and spoofing, impact the usability and safety of these technologies?
2. What is the awareness level among visually impaired users regarding privacy and security risks in IoT devices, and how does this affect adoption?
3. What existing security measures (e.g., encryption, authentication) are applied in IoT assistive technologies, and what gaps persist in their effectiveness?
4. How can best practices and standards be developed to balance security, privacy, usability, and accessibility in IoT-driven assistive designs?

Relevance and Importance of the Research

Some 2.2 billion people worldwide suffer visual impairment resulting in practical navigational problems that IoT based assistive technologies can rectify (Casanova et al., 2025). However, failure to identify the associated risks and problems, indeed in studies indicating that 79% of those device evaluation studies suffer from a lack of a practical validation, threatens user confidence and safety (Casanova et al., 2025). Thus, culture systems with 60% object identification or inability to identify font types that may be complex (error rate of 22.2 %) do not meet the essential requirements and involve risk of collision or wrong navigation (Abidi et al., 2024; Kral et al., 2024). There are also risks of privacy invasion resulting from the continuous transmission of data which are to be secured, imply user exposure to mismanagement of confidential data such as localization and invasion of privacy (Dian et al., 2020). These difficulties are aggravated by the emotional stress involved in negotiating non-inclusive environments and the resistance to dependent family or costly professional help (Abidi et al., 2024; Lavric et al., 2024).

The research will result in the generation of privacy-by-design solutions for frameworks and user-centric solutions such as automatic denunciation of security threats and accessible means of authentication (e.g., voice biometrics) which will allow for greater levels of personal and autonomous safety (Kovacs et al., 2025). Manufacturers will gain from this work in terms of guidelines for the design of security into their systems. Healthcare providers will have direction in terms of technology implementation allowing safe technology integration and government policy makers will be aided by information with which to support relevant data security measures (Rochford, 2019). Therefore, this study offers guidance and solutions in terms of equity and digital inclusion and can be expected to improve opportunities for the visually impaired to negotiate an interconnected world.

Literature review

Figure 1

sources

Authors (Year)	Title / Venue	Method / Design	Data / Context	Key Findings	Limitations	Relevance to Idea
Abidi et al., 2024	Navigation Systems for VI (review) / Heliyon	Narrative/structured review	Multi-modality survey	Synthesises trends; highlights energy, acceptance, integration gaps	Limited quantitative synthesis; calls for standardised metrics	This review identifies a gap in the systematic evaluation of data privacy and security for IoT assistive devices, focusing more on functional aspects like efficacy and cost.

Casanova, E., Guffanti, D., & Hidalgo, L. (2025)	Technological Advancements in Human Navigation for the Visually Impaired: A Systematic Review. / Sensors 2025	Systematic Literature Review (SLR) using the PRISMA 2020 methodology, filtering 898 records down to 58 articles published between 2019 and 2024.	Analysis of 58 articles categorized into smartphone technologies, haptic systems, navigation algorithms, and AI systems (deep learning/neural networks)	Found sustained interest in the field. Integration of AI (deep learning, neural networks) optimizes navigation accuracy and energy efficiency. 79% of reviewed articles included experimental validation.	Limitations persist in sensor accuracy and complexity in map production, highlighting a need for greater integration of smart devices with robust connectivity and efficient processing systems.	This systematic review highlights the dominant focus on functional performance (accuracy, efficiency) with 79% of studies including experimentation, while implicitly revealing a gap where explicit security, data handling, and ethical considerations remain critically underexplored
Cheraghi et al., 2016/17	GuideBeacon BLE Wayfinding / IEEE PerCom	BLE beacons + smartphone compass; user study	Single building; BVI & sighted (disoriented) users	Faster routing and shorter paths vs baseline; commodity hardware works	Small, single-site deployment; beacon placement/ config burdens	This comparative work highlights that BLE localization offers low power advantages but operates via constant signal

						exchange, implying continuous transmission of location data which necessitates robust security to prevent unauthorized tracking.
Chumkamon, S., & Keeratiwintakorn, P. (2008)	A Blind Navigation System Using RFID for Indoor Environments. / Conference Paper (ECTICON 2008)	Prototype system development using low-cost passive RFID tags for location reference and path-finding via a Java-based navigation server employing the shortest path algorithm.	Simulated map built with a grid of 16 RFID tags (4x4 paths) for voice-guided indoor navigation. The device used GPRS for server communication.	The portable prototype successfully provided navigation using only voice guidance derived from tag locations and distance costs based on the shortest path algorithm.	The paper implies challenges with initial communication delays due to the GPRS module connecting to the remote server, and the simulation relied on a limited, grid-based simulated map.	This foundational work explicitly details communication issues related to network dependency (GPRS cold start cycle delay) and file transfer delays, exposing early vulnerabilities in open connectivity for navigation systems that prioritize remote processing.

Dian, F. J., Vahidnia, R., & Rahmati, A. (2020)	Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey. / IEEE Access	Comprehensive literature survey and classification of IoT-enabled wearable research into four clusters: health, sports/activity, tracking/localization, and safety.	Review analyzed fundamental algorithms for various applications, including localization methods (e.g., fingerprinting, stochastic-oriented models) across health and tracking categories.	Cellular IoT (CIoT) offers enormous potential but is rarely studied by researchers in the context of wearable IoT, suggesting a missed opportunity for advanced applications.	Wearable IoT implementation faces challenges related to power consumption and the inherent complexity of integrating sophisticated functionalities into lightweight devices.	Directly addresses security and privacy trade-offs in wearable IoT, noting that lightweight devices often lack robust encryption, leading to vulnerabilities in sensitive data transmission (e.g., health and location data) and emphasizing the need for robust privacy models.
Farooq et al., 2022	IoT-Enabled Intelligent Stick / MDPI Sensors	Smart cane (ultrasonic, water detection, camera)	Lab + short field tests	Detects obstacles and puddles; haptic and voice feedback	MCU limits; durability/ power not tested long-term	Explicitly engages with data handling by integrating sensitive features (live location sharing, panic button) via a cloud platform

						(ThingSpeak), which requires careful management of unique credentials to balance user safety (tracking) with necessary data privacy.
Gonzales-Saavedra, H. et al. (2025)	Inclusive innovation: Implementation of low-cost proximity sensors for canes. / Revista Científica de Sistemas e Informática	Development of a low-cost, IoT-based cane prototype using an Arduino Nano and an ultrasonic sensor (HC-SR04) to provide progressive acoustic alerts (buzzer).	Tested detection effectiveness against objects (cardboard, cup, laptop, wall) in an environment with preset proximity alert levels (100 cm, 75 cm, 50 cm).	The prototype achieved high effectiveness (100% accuracy for large objects/walls) and provided reliable immediate acoustic alerts, prioritizing affordability and simplicity in its functional design.	The system demonstrated limitations with small objects, liquids, and in humid environments, suggesting a need for future integration of wireless charging and LiDAR sensors.	Highly focused on low-cost and fast technical function, the work neglects explicit mention of data privacy or security frameworks, implicitly indicating that robustness against cyber threats is not a primary design criterion in this prototype.
Han et al.,	Wearables	Perspective	Synthesis	Body/torso	Narrative	This

2023	for persons with blindness and low vision: form factor matters / Assistive Technology	/mini-review on form factor and ergonomics	across BLV wearables	-mounted designs can reduce shake, improve comfort and battery	evidence; no head-to-head trials or large samples	comparison of wearables links device design choices to potential data protection vulnerabilities, noting that advanced functionality often requires offloading data to external servers.
Kovacs et al., 2025	RFID-Based Indoor Guiding / MDPI Information	UHF RFID route-tagging + guidance app	Public-building style routes; experiments	Corridor-level guidance possible with tag routes; voice feedback	Infrastructure overhead; tag maintenance; needs BVI field trials	While aiming for accessibility and low cost, this RFID system potentially creates a persistent record (TID/location data) in a database, implying security risks if the database or Wi-Fi manager were compromised, although

						the authors note it does not need Internet connectivity for core function.
Kral, Jacko & Vince, 2025	Low-Cost Multifunctional Assistive Device / IEEE Access	Engineering prototype (multifunction cane/wearable), component integration	Lab bench + small functional demos	Low-cost BOM can integrate multiple assistive functions into one device	Early-stage evaluation; limited field use; generalisability untested	This system uses remote volunteer assistance and cloud-based AI that introduce major privacy risks by disclosing highly sensitive, real-time visual and contextual data.

Kunhoth et al., 2019	CV vs QR vs BLE Indoor Wayfinding / Int. J. Health Geographics	Built CamNav (CNN), QRNav, BLE baseline; comparative study	10 blindfolded participants; one building	CV more accurate; BLE more scalable/cost-effective	Small N; blindfolded not BVI; single site; limited generalisation	This comparative study implicitly raises privacy concerns regarding data architecture: vision systems often centralize image processing on a server (cloud/remote), increasing exposure, whereas BLE processing is noted as occurring locally on the smartphone.

Lavric, A., Beguni, C., Zadobrischi, E., Căilean, A.-M., & Avătămănit,ei, S.-A. (2024)	A Comprehensive Survey on Emerging Assistive Technologies for Visually Impaired Persons: Lighting the Path with Visible Light Communications and Artificial Intelligence Innovations. / Sensors 2024	Comprehensive survey analyzing commercially available solutions, the benefits of VLC, the use of AI for diagnostics, and proposing a framework for AI-driven VLC solution development.	Review focuses on the synergistic integration of AI/ML (for processing/ diagnostics) and Visible Light Communications (VLC) for secure, high-precision indoor localization and data communication.	VLC provides enhanced data privacy due to its confined communication range and achieves centimeter-precision indoor localization. AI integration enhances data interpretation and positioning accuracy.	Despite remarkable potential, the application of VLC in blind assistance is currently insufficiently explored. There is an imperative need for clear guidelines regarding data privacy and security from all involved parties.	Strongly champions VLC for its inherent privacy benefits due to limited communication range, while simultaneously raising major ethical concerns regarding the transparency and privacy risks associated with required AI biometric datasets.

Messaoudi, M. D., Menelas, B.-A. J., & Mcheick, H. (2022)	Review of Navigation Assistive Tools and Technologies for the Visually Impaired. / Sensors 2022	Literature review focusing on navigation technologies, obstacle recognition methods, and feedback mechanisms for the visually impaired.	Evaluation analysis based on criteria including cost, compactness, reliability, and coverage region, comparing various systems from RFID to RGB-D sensor tools.	Many proposed methods are academically sound but are often "lab-based" prototypes that prioritize accurate results over addressing non-functional, real-world issues like power consumption and deployment feasibility.	The lack of user acceptance and low utilization rates are key drawbacks. Previous work generally ignored critical non-functional factors like adequate power consumption solutions and wearability.	Notes methodological shortcomings, observing that many solutions are "lab-based" prototypes that prioritize accuracy over long-term, non-functional challenges, such as implementing adequate power consumption solutions necessary for sustained, robust security features.

Okolo, G. I., Althobaiti, T., & Ramzan, N. (2024)	Assistive Systems for Visually Impaired Persons: Challenges and Opportunities for Navigation Assistance. / Sensors 2024	Review comparing technologies and analyzing AI-based object detection and IoT navigation systems for visually impaired persons.	Analysis of AI systems (e.g., YOLO, SSD) and IoT architectures (smart sticks using ultrasonic, GPS, GSM), evaluating their effectiveness and usability.	AI systems achieve high accuracy (e.g., 90.00% with YOLO) but often demand high computational resources. IoT systems enhance mobility and safety through components like GPS/GSM modules for emergency location sharing. M	Many strategies, while effective in principle, may be excessively difficult or time-consuming for users in practice, and many AI systems lack early warning capabilities for far-off obstructions.	Directly identifies the gap in security robustness, noting that many AI systems require high computational resources (implying cloud reliance) but lack defined security standards or standardized metrics for assistive IoT devices.
Panazan & Dulf, 2024	Intelligent Cane (dual ultrasonic) / MDPI Technologies	Dual-sensor cane + mobile app	Indoor/outdoor demos	Dual placement improves obstacle coverage with simple alerts	Minimal user testing; no comparative metrics	This low-cost, prototype-focused work achieves high accuracy in obstacle detection but largely neglects sophisticated security protocols,

						limiting the scope of its contribution to functional safety rather than robust protection of the minimal connectivity data exchanged via Bluetooth.
Rochford, J. (2019)	Accessibility and IoT / Smart and Connected Communities. / AIS Transactions on Human-Computer Interaction	Practitioner paper/commentary focusing on the ethical and design necessity of incorporating accessibility, privacy, and security into IoT and Smart Cities User Experience (UX).	Discussion centers on data governance and the unique challenges faced by "outliers" (people with disabilities) in IoT datasets, including issues of discrimination and disclosure.	Privacy and Security by Design are crucial. Society benefits when data from outliers are included, but people with disabilities have strong incentives not to identify themselves due to discrimination (the Smart Cities Conundrum).	Machine-learning models trained on average behavior may fail dangerously for use cases that deviate from the norm, such as an autonomous car virtually running over a wheelchair user propelling backward.	Provides the foundational theoretical argument that security, privacy, and fairness must be "baked in" from the outset ("Privacy and Data Protection by Design"), emphasizing the necessity of including vulnerable "outliers" (people

						with disabilities) in the design process to ensure trust.
Rosiak et al., 2024	UWB Indoor Positioning for VI / Applied Sciences	UWB ranging tests vs LiDAR reference; static/dynamic	Controlled indoor scenarios	UWB usable; fusion improves stability esp. under NLoS	Engineering-focused; lacks multi-week BVI evaluation	Directly addresses the ethical and design implications, arguing that security and privacy must be built-in from the outset ("Privacy and Data Protection by Design") to manage the inherent trade-off users with disabilities face between functionality and data exposure.
Sedighi, P. (2023)	A radio-frequency identification based wearable assistive system for	Development of a wearable prototype (glove and shoe) based on passive	System tested in a structured 4.1 x 3.2 m² room (simulating a physician's	The system is self-supporting and does not rely on smartphones or	A primary limitation was the relatively large distance between tags.	Achieves strong privacy implicitly by being self-supporting and relying on

	visually impaired people. / IEEE Transactions on Instrumentation and Measurement	RFID technology for object recognition and navigation, employing Dijkstra's algorithm.	office) covered with 24 passive RFID tags; audio instructions were stored in an onboard SQLite database.	Internet connectivity, offering inherent advantages in privacy and reliability. The platform is reliable, low-cost, and power-efficient for indoor use.	Increasing tag density would lead to higher computational complexities and possible delays in feedback.	independent onboard databases (SQLite) for navigation data and audio instructions, minimizing reliance on external networks for core functionality.
Semary, H. E., Al-Karawi, K. A., Abdelwahab, M. M., & Elshabrawy, A. M. (2024)	A Review on Internet of Things (IoT)-Related Disabilities and Their Implications. / Journal of Disability Research	Comprehensive review focusing on the potential benefits and critical research challenges of IoT for individuals grappling with disabilities, analyzing existing devices (sensors, RFID) and applications.	Discussion covers body sensors and RFID systems in various environments (smart homes, education), emphasizing the need for robust security and user-centered design principles.	IoT systems enhance independence and inclusion. The principle of self-protection is crucial for IoT systems to mitigate security threats and ensure an inclusive experience. Accessible designs, initially for vulnerable groups, benefit everyone ("curb-cut	There is a noted scarcity of research addressing the specific privacy implications of IoT use by people with disabilities. Challenges include ensuring robust security measures, energy efficiency, and affordability.	Explicitly identifies the severe scarcity of research addressing the specific privacy implications of IoT use by people with disabilities, and advocates for self-protection mechanisms (security) to ensure an inclusive and safe user experience.

				effect").		
Srinivasaiah et al., 2024	Turn-by-Turn Indoor Navigation / arXiv	Edge pipeline (phone camera → local CNN + LLM; no cloud)	Preliminary design + pilot	Privacy-preserving local guidance is workable; natural-language directions	Early prototype; energy/latency not fully benchmarked; limited trials	Directly supports the research proposal by adopting an Edge Computing architecture (local processing on Raspberry Pi) to ensure high security and privacy by keeping computationally intensive visual data and LLM processing entirely off the cloud.

Key Concepts, Theories and Studies

The development of IoT assistive technologies for visually impaired persons (VIP) is dependent on the principles of Universal Accessibility and User-Centric Design (UCD) (Semary et al., 2024; Rochford, 2019). Privacy- and Security-by-Design are crucial for sensitive data (Rochford, 2019). Yet, many low-energy devices do not have adequate encryption and are

vulnerable (Dian et al., 2020). Certain architectural solutions including broadcast-subscriber solutions and Visible Light Communications (VLC) assist in improving security (Dian et al., 2020; Lavric et al., 2024). Different systems are used in the technology for navigation purposes. IoT architectures enable smart canes to provide real time data (Farooq et al., 2022). For positioning systems GPS will work outdoors, with technology enabling RFID and Bluebooth Low Energy (BLE) for indoor systems (Kovacs et al., 2025; Kunhoth et al., 2019). More recently, VLC (Li-Fi) systems also assist in indoor systems augmenting secure positioning with power saving and data transfer requirements (Siddhi et al., 2024; Lavric et al., 2024). A further methodology includes Edge Computing (EC) for processing data locally on devices which might include Raspberry Pi systems which assists in enhancing user privacy (Yuan et al., 2022; Casanova et al., 2025).

Artificial Intelligence (AI) and Machine Learning (ML) systems have transformed such architecture. Deep learning techniques including convolution neural networks (CNNs) and the methodology seen in YOLO systems enables real time object detection and mapping (Casanova et al., 2025; Tapu et al., 2017). The employment of multimodal techniques with preformance enhancement using Large Language Models (LLMs) indicates a real possibility of new systems with the opportunity to convert information of a complex visual nature to enable natural audioised enhancing audio guidance (Srinivasaiah et al., 2024). While many devices are cloud-based, a trend is toward hybrid and Edge AI for enhanced privacy.

Key Debates and Controversies

The integration of IoT and AI for VIPs has sparked debate about how to balance performance with data privacy and data security; this imbalance affects user trust and adoption ultimately (Rochford, 2019).

The main design dilemma lies in the realm of Cloud Vs. Edge Processing. Cloud systems handle high-level processes well; but, they have latency and security issues, where as, Edge Computing processes data on the unit locally, thus retaining sensitive information on the device (Srinivasaiah et al., 2024). The consensus is toward a hybrid architecture that combines benefits of both Cloud and Edge (Dian et al., 2020; Yuan et al., 2022).

Another main issue is that of Functionality Vs. Privacy. Specially formed navigation systems often require data from VIPs that is sensitive in nature, thus resultant in various forms of surveillance risk (Dian et al., 2020). The conflict between the ethics of Open Connectivity and Data Protection registers as pressing; notably, inexpensive versions of wearable devices typically come with no encryption built into them, and consequently are prone to hacking (Dian et al., 2020). Previous catastrophes, like that of the unencrypted Mascot insulin pump incident, which raised serious doubts abut the level of safety of many devices (Newman, 2019, cited in Rochford, 2019).

Gaps in Existing Knowledge

Present research in the area of IoT assistive technology, with special regard to VIP users, has not indicated sufficient focus on issues of privacy, security and ethics. One of the noteworthy gaps is that of disparate implementation of Privacy- and Security-by-Design throughout. These principles are acknowledged, but little has been done in the experimental validation of these principles in practice (Rochford, 2019). There are many and copious forms of sensitive data being collected from companies producing such IoT devices, yet, very little research has been done on the nature of the informed consent to be obtained from users (Lavric et al., 2024). The non-transparency of learning processes involved in deep learning Strategies also introduces complications of transparency of 'maybe!' violated to other resources too, Socratic but the area of Cellular IoT (CIoT) remains unexplored (Dian et al., 2020). Methodology in the research area also presents severe gaps. For the greater part, experimental aspects of functional performance versus security effectivity or ethical evaluations have received prioritised emphasis in councils. Notably, many prototypes of usable devices of IoT assistive technology have their uses checked for, controlled and tested in laboratory condition where they are subjected to learning evaluations but causal empirical presentations of their usability in VIPs usually become neglected (Casanova et al., 2025; Kovacs et al., 2025).

Considerable and critical components of the devices' usability, if sustainable, have also received insufficient attention nowadays (Okolo et al., 2024). Further gaps can be seen in regard to governance and the regulation areas. There is no standardized template by which to evaluate privacy within these devices. This leads to further undisciplined comparability being very difficult in comparisons (Okolo et al., 2024). Also the ethical issue of whether and what it is proper to do in relation to the data of "Outlier" persons with disabilities remains underexplored in this sense of algorithms' future development by "better" significance during varied products

(Rochford, 2019). The project-created, thus enables to fill a number of these gaps extant situpose of the security-related, ethical framework being pursued in construct. Thus, matters such as the obtaining of thoroughly expressed consent from users, the highly sensible a thing and use of end-to-end encryption alone and the transparent "Intelligence" utilized f will make protypes ready for production utilisation, nationally.

Research design and methods

This research explores privacy and security issues within IoT (Internet of Things)-based assistive technologies for the visually impaired, and is driven by the following: (a) systematically review and categorize such IoT assistive technologies and the vulnerabilities they have; (b) analyze the privacy and security risks involved, e.g., data manipulation and unauthorized access; (c) review the literature concerning user understanding and awareness of these risks; (d) assess what security measures exist and their inadequacies; (e) make recommendations concerning best practices to ensure designs are secure and user centered. Given the 10-weeks which have been allotted for this project, 5 of which remain post proposal, this section includes a theoretical literature based research design and methods as these will prove the most efficient modes of answering the research questions.

Research Design

The research takes an overall qualitative research design, based on descriptive analysis, and is particularly suited to address complex phenomena, such as privacy and security vulnerabilities within IoT assistive technologies, without the need for experimental manipulation (Creswell & Creswell, 2018) This design seems appropriate in view of the time restrictions placed upon the researcher in this situation, since the research is based on secondary sources rather than primary data, allowing the extensive employment of reviewed literature and technology documents towards answering all the stated objectives. The research design is theoretical synthesizing previously published studies in their addressing of vulnerabilities, user perceptions and inadequacies of control measures in existence (Abidi et al., 2024; Casanova et al., 2025). A very slight quantitative aspect will arise in the form of the descriptive statistics, e.g., error rates, reply times, taken from the literature allowing device performance problems to be indicated quantitatively, such as 60% object recognition rate, or 260 ms response time (Abidi et al., 2024; Gonzales-Saavedra et al., 2025).

Methods and Sources

Population and sample: this study will concentrate on the IoT-based assistive technologies (for instance smart canes, wearable navigation devices, RFID etc.) designed for the visually impaired as presented in the academic literature and technology reports which have appeared between 2019 and 2025. From databases such as, IEEE Xplore, PubMed, SpringerLink, arXiv, a purposive sampling strategy will be used to choose 40-50 peer reviewed papers (and associated technology papers). Particular emphasis will be placed on articles which tackle issues involving privacy, security, usability, and user perceptions (Farooq et al., 2022; Kovacs et al., 2025) and the sample used will serve to ensure relevance of sampling to both research questions and objectives covering such devices as smart canes with ultrasonics sensors, and wearables with VLC (visible light communication).

Research Methods

The following methods will be used to address the research questions and objectives within the 5-week execution period (weeks 6–10):

1. Research Methods The following methods will be employed to answer the research aims and questions over the planned 5-week execution period (weeks 6-10): Systematic Literature Review (Objectives 1, 2, 3 and 4): A systematic review of the literature, using a predetermined protocol (e.g. PRISMA guidance) will be carried out to identify and classify existing IoT assistive technologies, their features and reported vulnerabilities (e.g. unencrypted Bluetooth connections, instability of GPS systems, etc). Search terms

e.g. IoT assistive technology, visually impaired, privacy, security will be deployed to obtain 40-50 sources. This method will address research questions 1, 2 and 4 and will synthesise the evidence of published studies on vulnerabilities (e.g. 60% recognition rates, 260 ms % times) and countermeasures (Abidi et al. 2024; Gonzales-Saavedra et al. 2025). Objective 3 studies concerning user awareness concerning (e.g. perceptions of data breaches etc) will be reviewed to identify existing knowledge gaps (Semary et al. 2024).

Procedure: A relevance check against articles will be made and a matrix (device type, vulnerability, security measure etc will be constructed for the extraction of data from these sources). The findings will be synthesised narratively. Time line: Weeks 6-8 (search, screening, extraction of data). Thematic Analysis of User Perceptions (Objective 3): Qualitative data from the literature regarding user perceptions (e.g. trust, usability experiences) will be subjected to thematic analysis to identify recurring themes, for instance: concerns regarding data and/or complexity in the authentication (Farooq et al. 2022). It will be necessary to employ software e.g. NVIVO to facilitate analysis/coding and development of themes. Procedure: Literature search and extraction of information regarding users, coding for themes (e.g., “trust in devices”, “concerns about privacy”) and extracting gaps in awareness.

Timeline: Weeks 6–8 (search, screening, data extraction).

2. Technical Analysis of Security features (Objective 4): Security features that are already availabe (e.g., encryption, authentication) will be analed by examination of the technical documentation and literature (literature predicates: response time, error rates) in respect to the devices. A comparative matrix will analyse the gaps (e.g., little or no encryption available in resource-limited devices (Dian et al., 2020; Okolo et al., 2024)).

   Procedure: Extract user-related findings from literature, code for themes (e.g., “trust in devices,” “privacy concerns”), and synthesize gaps in awareness.

   Timeline: Weeks 7–9.

3. Technical Analysis of Security Measures (Objective 4): Existing security measures (e.g., encryption, authentication) will be evaluated by analyzing technical documentation and literature on device performance (e.g., response times, error rates). A comparative matrix will highlight gaps, such as limited encryption in resource-constrained devices (Dian et al., 2020; Okolo et al., 2024).

Procedure: Collect device specifications, extract metrics (e.g., 22.2% error rate in font recognition), and compare against security standards (Kral et al., 2024).

Timeline: Weeks 7–9.

4. Development of Best Practices (Objective 5): Information drawn from the literature search and technical analysis will create a best-practice model for manufacturers incorporating themes of 'privacy by design', automatic detection of threats, forms of authenticating identity (e.g., via voice, haptic feedback for use as part of the authentication process) (Kovacs et al., 2025) will be incorporated. Recommendations will be synthesized and constructed into a document in abbreviated format which covers best-practice.

   Procedure: Synthesis of existing literature and methodologies into and creating actionable recommendations/codes of practice which have been validated against user needs and technical possibility.
   Timeline: Weeks 9–10.

Rationale for Methods: The literature and thematic analysis to give a good broad but time limited method of synthesising existing knowledge, answering all research questions, means that no primary data collection is necessary which is impractical due to time-frame of development into an implementable strategy which requires a time-frame of 5 weeks. The limited quantitative analysis possible of performance/metric data generated will enable the resultant knowledge-based, due to understanding of technical limitations.

Data Collection and Analysis

The gathering and analysis of data will be from weeks 6-8 gathering is focused on a literature search, and the downloading of documents which will be held by academic databases (i.e. peer reviewed articles). Analysis will occur between weeks 7-9 in a combination of thematic analysis of qualitative data (users views) and descriptive statistics of quantitative metrics (e.g., error rates, response times gathered out of studies). A narrative synthesis of information will formulate findings academically from this in relation to vulnerabilities in devices, user awareness etc. and security, upon which best practices will be compiled in week 10. Software packages (e.g. NVivo, Excel) will ensure a smooth process of coding, extraction and collation of data.

Practical Considerations

Time and Resources

The study fits within the 5-week execution period (weeks 6–10):

- Weeks 6–7: Literature search and screening (10–15 hours/week).
- Weeks 7–8: Data extraction and thematic/technical analysis (15 hours/week).
- Weeks 9–10: Synthesis and best practice development (10–12 hours/week).
  Resources include access to academic databases (via institutional subscriptions) and software (NVivo, Excel). No participant recruitment or lab facilities are required, minimizing costs.

Access to Sources

Access to peer-reviewed literature will be secured through university library subscriptions to IEEE Xplore, PubMed, and SpringerLink. Open-access sources like arXiv will supplement the sample. Potential obstacles, such as paywalled articles, will be mitigated by requesting interlibrary loans or contacting authors for preprints.

Obstacles and Limitations

- Obstacles: Limited access to recent 2025 publications may restrict the sample. This will be addressed by prioritizing open-access sources and leveraging institutional networks.
- Limitations: The reliance on secondary data may miss emerging technologies or real-time user feedback. This is mitigated by focusing on recent studies (2019–2025) and including arXiv preprints (e.g., Srinivasaiah et al., 2024). The theoretical approach limits generalizability to specific user experiences, but it aligns with the timeline and objectives.
- Ethical Issues: No primary data collection eliminates ethical concerns like participant consent or data privacy. However, the study will ensure proper citation to avoid plagiarism and acknowledge limitations of secondary data to maintain academic integrity.
- Practical Issues: Time constraints may limit the depth of analysis. A structured PRISMA protocol and predefined search criteria will ensure efficiency. If fewer than 40 sources are found, the scope will be adjusted to 30 sources without compromising rigor.

Implications and Contributions to Knowledge

This research will contribute to the growing body of knowledge on security and data privacy in IoT-based assistive technologies for visually impaired individuals. While previous studies have mainly focused on improving device functionality and navigation accuracy, this project emphasizes the data transmission and security vulnerabilities that arise when sensitive user information—such as location and behavioral patterns is exchanged across IoT systems. The findings will bridge the gap between technical innovation and ethical responsibility, encouraging the design of safer and more privacy-conscious IoT ecosystems.

By integrating perspectives from existing literature, this project will contribute to theoretical discussions about data ethics, secure communication models, and trust in assistive technologies, offering new insights into how technology can empower users without compromising their autonomy or safety.

Practical Implications

The outcomes of this study will provide practical guidance for developers, policymakers, and organizations working on IoT solutions for visually impaired users. The findings can inform the

development of secure design frameworks and data protection protocols tailored to assistive devices such as smart canes, wearables, and indoor navigation systems.

Moreover, the project's recommendations can help regulators establish privacy standards and encourage manufacturers to adopt stronger encryption and anonymization measures. Ultimately, this work aims to improve user trust, promote inclusivity, and ensure compliance with global data protection principles such as the General Data Protection Regulation (GDPR) and ethical AI design practices (Abidi et al., 2024; Farooq et al., 2022; Lavric et al., 2024).

Theoretical Implications

From a theoretical perspective, this research will deepen understanding of IoT data security frameworks in assistive contexts by examining how different transmission methods—such as Bluetooth, RFID, Wi-Fi, and UWB affect vulnerability levels. The study will contribute to refining existing risk assessment models for IoT systems, offering a conceptual basis for future theoretical exploration of privacy-by-design principles.

It will also challenge current assumptions that prioritize device performance over security by proposing a balanced model that integrates usability, accessibility, and data integrity. This theoretical contribution may serve as a foundation for future studies exploring the intersection of cybersecurity, human-centered design, and disability inclusion (Dian et al., 2020; Okolo et al., 2024; Semary et al., 2024).

References

Abidi, M. H., Siddiquee, A. N., Alkhalefah, H., & Srivastava, V. (2024). A comprehensive review of navigation systems for visually impaired individuals. *Heliyon, 10*, e31825. https://doi.org/10.1016/j.heliyon.2024.e31825

Casanova, E., Guffanti, D., & Hidalgo, L. (2025). Technological advancements in human navigation for the visually impaired: A systematic review. *Sensors, 25*(7), 2213. https://doi.org/10.3390/s25072213

Cheraghi, S. A., Namboodiri, V., & Walker, L. (2017). GuideBeacon: Beacon-based indoor wayfinding for the blind, visually impaired, and disoriented. In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)* (pp. A2, 386). IEEE.

Chumkamon, S., & Keeratiwintakorn, P. (2008). A blind navigation system using RFID for indoor environments. In *Proceedings of the 2008 International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTICON)*. IEEE. https://doi.org/10.1109/ECTICON.2008.4600543

Dian, F. J., Vahidnia, R., & Rahmati, A. (2020). Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A survey. *IEEE Access, 8*, 65053–65070. https://doi.org/10.1109/ACCESS.2020.2986329

Farooq, M. S., Shafi, I., Khan, H., Díez, I. D. L. T., Breñosa, J., Espinosa, J. C. M., & Ashraf, I. (2022). IoT-enabled intelligent stick for visually impaired people for obstacle recognition. *Sensors, 22*(22), 8914. https://doi.org/10.3390/s22228914

Gonzales-Saavedra, H., Garcia-Hurtado, K., Gallegos-Pinedo, C., Tenazoa-Bardales, R., Ordinola-Sinarahua, A., Hilario-Putpaña, D., & Diaz-Delgado, D. (2025). Inclusive innovation: Implementation of low-cost proximity sensors for canes. *Revista Científica de Sistemas e Informática, 5*(1), e838. https://doi.org/10.51252/rcsi.v5i1.838

Han, J., Zhang, Z., Boldini, A., Beheshti, M., Porfiri, M., & Rizzo, J.-R. (2024). Embodiment considerations for assistive technology for persons with blindness and low vision: Handheld, head-mounted, and body-mounted approaches. *Assistive Technology, 36*(1), 60–63. https://doi.org/10.1080/10400435.2023.2205490

Kovacs, I.-F., Karolyi, A.-C., Stângaciu, C.-S., Stângaciu, V., Nimară, S., & Curiac, D.-I. (2025). An RFID-based indoor guiding system for visually impaired people. *Information, 16*(3), 220. https://doi.org/10.3390/info16030220

Kral, R., Jacko, P., & Vince, T. (2024). Low-cost multifunctional assistive device for visually impaired individuals. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024

Kunhoth, J., Karkar, A., Al-Maadeed, S., & Al-Attiyah, A. (2019). Comparative analysis of computer vision and BLE technology-based indoor navigation systems for people with visual impairments. *International Journal of Health Geographics, 18*(1), 29. https://doi.org/10.1186/s12942-019-0193-9

Lavric, A., Beguni, C., Zadobrischi, E., Căilean, A.-M., & Avătămănit,ei, S.-A. (2024). A comprehensive survey on emerging assistive technologies for visually impaired persons: Lighting the path with visible light communications and artificial intelligence innovations. *Sensors, 24*(15), 4834. https://doi.org/10.3390/s24154834

Messaoudi, M. D., Menelas, B.-A. J., & Mcheick, H. (2022). Review of navigation assistive tools and technologies for the visually impaired. *Sensors, 22*(20), 7888. https://doi.org/10.3390/s22207888

Okolo, G. I., Althobaiti, T., & Ramzan, N. (2024). Assistive systems for visually impaired persons: Challenges and opportunities for navigation assistance. *Sensors, 24*(11), 3572. https://doi.org/10.3390/s24113572

Panazan, C.-E., & Dulf, E.-H. (2024). Intelligent cane for assisting the visually impaired. *Technologies, 12*(6), 75. https://doi.org/10.3390/technologies12060075

Rochford, J. (2019). Accessibility and IoT: Smart and connected communities. *AIS Transactions on Human-Computer Interaction, 11*(4), 253–263. https://doi.org/10.17705/1thci.00124

Rosiak, M., Kawulok, M., & Maćkowski, M. (2024). The effectiveness of UWB-based indoor positioning systems for the navigation of visually impaired individuals. *Applied Sciences, 14*(13), 5646. https://doi.org/10.3390/app14135646

Semary, H. E., Al-Karawi, K. A., Abdelwahab, M. M., & Elshabrawy, A. M. (2024). A review on Internet of Things (IoT)-related disabilities and their implications. *Journal of Disability Research, 3*, e20240012. https://doi.org/10.57197/JDR-2024-0012

Srinivasaiah, S., Nekkanti, S. K., & Nedhunuri, R. R. (2024). Turn-by-turn indoor navigation for the visually impaired https://doi.org/10.48550/arXiv.2410.19954 Diaconia LLC.

Zare, F., Sedighi, P., & Delrobaei, M. (2023). A wearable RFID-based navigation system for the visually impaired. *IEEE Transactions on Instrumentation and Measurement.*

Research schedule

Research Schedule

The following research schedule outlines the planned phases, objectives, and deadlines for the proposed study on *enhancing data security and privacy in IoT-based assistive technologies for visually impaired users*. The schedule ensures a structured and achievable approach that aligns with the research objectives and academic requirements.

Research phase	**Objectives**	**Deadline**
Phase 1 — Background research & literature review	• Conduct comprehensive literature review on IoT assistive technologies and data transmission methods (Bluetooth, Wi-Fi, RFID, UWB, etc.). • Identify gaps in security and privacy research and refine research questions. • Refine the research problem and establish theoretical and ethical frameworks.	Oct 15, 2025
Phase 2 — Threat analysis & risk identification	• Systematically analyse data transmission vulnerabilities (eavesdropping, MitM, spoofing, weak encryption).	25 October 2025

	• Produce threat matrix, DFD and 3–5 attack vignettes.	
Phase 3 — Privacy & ethical perspectives	Evaluate privacy implications, legal and ethical frameworks (GDPR, HIPAA), and user vulnerability issues. • Produce ethical recommendations and inputs for mitigation trade-offs.	2 November 2025
Phase 4 — Stakeholder & user-centered analysis	Map stakeholder perspectives (users, developers, policymakers). • Collect user-centred requirements and accessibility constraints to inform mitigations.	10 November 2025

Phase 5 — Theoretical model development & recommendations	Synthesize findings into a conceptual framework (risk assessment model, layered security recommendations). • Draft final recommendations and policy suggestions.	15 November 2025
Phase 6 — Integration, proofreading & final submission	Integrate all sections, check APA 7 formatting, proofread, and prepare presentation materials. • Submit final proposal.	18 November 202