International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

COLLEGE STUDENTS' PERCEPTION OF PRIVACY IN SMART WEARABLE MEDICAL DEVICES

UNNATI MITTAL

ABSTRACT

This study delves into security and privacy concerns related to smart wearable medical devices among college students. It reveals that over 50% of respondents don't perceive these devices as risky, possibly due to a lack of understanding about data handling. Despite worries about data security, users feel they have little control over their data.

To address these issues, the study suggests:

1. Educational campaigns to raise awareness.
2. Enhanced privacy controls within devices.
3. Collaborations between academia, industry, and regulators to establish standards.
4. Further research to monitor changes and assess emerging technologies.

Implementing these strategies can improve security and privacy practices, fostering greater trust and responsible use of smart wearable medical devices.

INTRODUCTION

Smart medical devices, including wearable sensors, are integral to the Internet of Things (IoT) ecosystem, aiding in health monitoring and facilitating efficient healthcare delivery. Smart wearable devices like smartwatches and fitness bands have gained popularity due to their versatility and consumer appeal. They offer features such as health monitoring, activity tracking, and even fashion appeal. These devices hold promise for various applications in healthcare, promoting healthy lifestyles and empowering individuals to manage their health effectively.

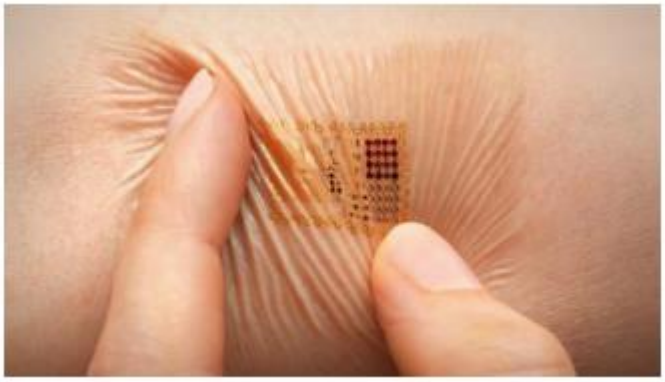
- Wearable fitness trackers, for example, monitor physical activity and heart rate, connecting to mobile apps to provide health advice.

- Smart health watches combine phone functionalities with activity and health tracking features, including blood oxygen saturation and sleep tracking.

- Wearable ECG monitors track atrial fibrillation and provide electrocardiogram results to doctors.

- Wearable blood pressure monitors store readings for analysis and sharing with doctors via a mobile app.

- Biosensors, a newer type of wearable medical device, have shown significant potential in preventing patient deterioration, thus enhancing outcomes and potentially reducing staff workload.



This study explores perceptions of security and privacy regarding smart wearable medical devices among college students and aims to understand factors influencing their adoption or abstention from using these devices. It delves into the rapid evolution and widespread adoption of smart wearables, such as smartwatches and wristbands, which empower users to monitor and transmit personal health and activity data. Despite the surge in demand for smart wearables, adoption rates remain relatively low, with challenges including technological immaturity, unmet expectations, and privacy concerns. The study conducts a Systematic Literature Review (SLR) to examine wearable technology concepts comprehensively and focuses on factors influencing wearable device adoption among college students, a demographic crucial for driving future consumption.

PROBLEM STATEMENT

The study aims to explore the usability of Smart Wearable Medical Devices (SWMDs) by understanding user perceptions, motivations, and security/privacy concerns. Key aspects to consider include varying attitudes towards SWMDs, usability factors influencing adoption, motivations driving usage (e.g., health monitoring, fitness tracking), and paramount security and privacy concerns such as data breaches and unauthorized access. Providing user control, transparency, education, and adherence to regulatory standards are essential for promoting safe and effective SWMD usage in healthcare.

OBJECTIVE OF THE STUDY

The study aims to understand Smart Wearable Medical Devices (SWMDs) usage among college students through four objectives: exploring usage patterns, examining perceptions of security and privacy, understanding protective measures, and proposing improvements for security. SWMDs offer benefits such as health tracking, convenience, personalized experiences, safety features, and fashion appeal. College students' perception of privacy in SWMDs is influenced by technological awareness, personal privacy preferences, trust in manufacturers, and contextual factors like regulations and policies. Addressing these factors is vital for promoting responsible SWMD adoption while respecting privacy rights.

REVIEW OF LITERATURE

This chapter outlines the development of a study addressing security and privacy concerns in smart wearable medical devices. It discusses the relevant literature, methodologies, and proposed frameworks from various studies. Key issues include the need for comprehensive security measures, challenges in IoT and IoMT security, vulnerabilities in

wearable devices, and the paradox of privacy. Various theoretical frameworks and research methodologies are explored to understand user behaviours and privacy concerns. Ultimately, the aim is to investigate and address security and privacy issues in smart wearable medical devices among college students, proposing solutions to enhance privacy protection.

RESEARCH AND METHODOLOGY

Introduction of Methodology and Framework:

- The section introduces the methodology and framework utilized to evaluate college students' attitudes towards privacy concerning Smart Wearable Medical Devices (SWMDs).

Quantitative Approach with Survey:

- The study employs a quantitative approach using a survey.
- The survey covers various aspects of privacy perceptions and security policies related to SWMDs.

Distribution of Survey:

- The survey was distributed to college students across both technical and non-technical departments.

Data Collection and Analysis Tools:

Qualtrics: Used for survey design and data collection.

- Known for reliability and versatility.
- Provides a user-friendly interface.
- Offers various question types and survey design options.
- Facilitates distribution via email, social media, or embedded links.
- Aggregates data in real-time.

Excel: Utilized for data analysis.

- Supports advanced data manipulation and visualization.
- Enables data cleaning and preparation.
- Offers functions for advanced statistical analysis.
- Provides charting tools for data visualization.

Objective of Research:

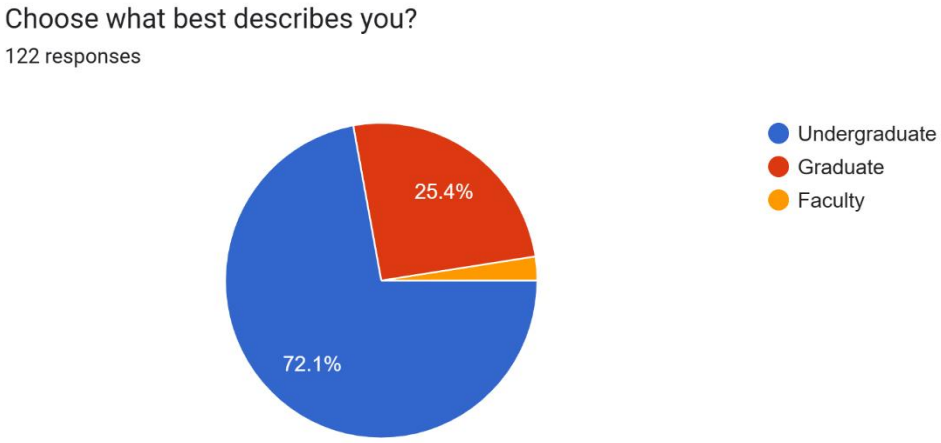
- The primary goal of the research is to gain insights into privacy concerns surrounding SWMDs among college students.

DATA ANALYSIS AND INTERPRETATION

DATA PRESENTATION

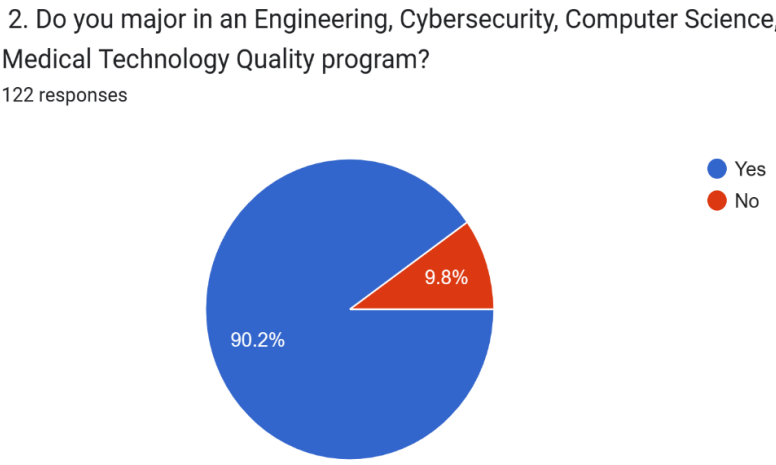
Here's a brief analysis and interpretation of the survey data:

1. Demographics:



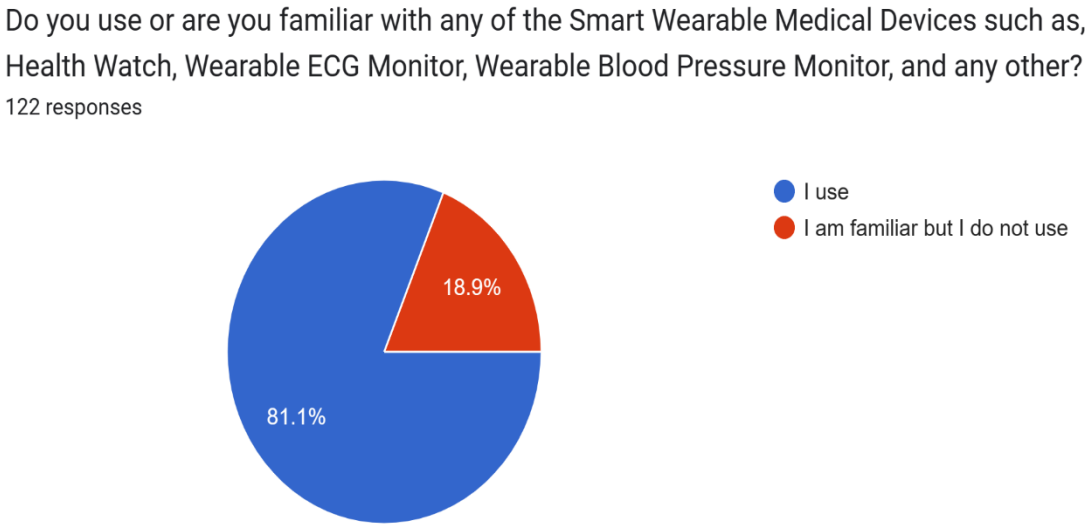
- Undergraduate respondents make up the majority with 88 responses, followed by graduates with 31 responses, and faculty with 3 responses.

2. Field of Study:



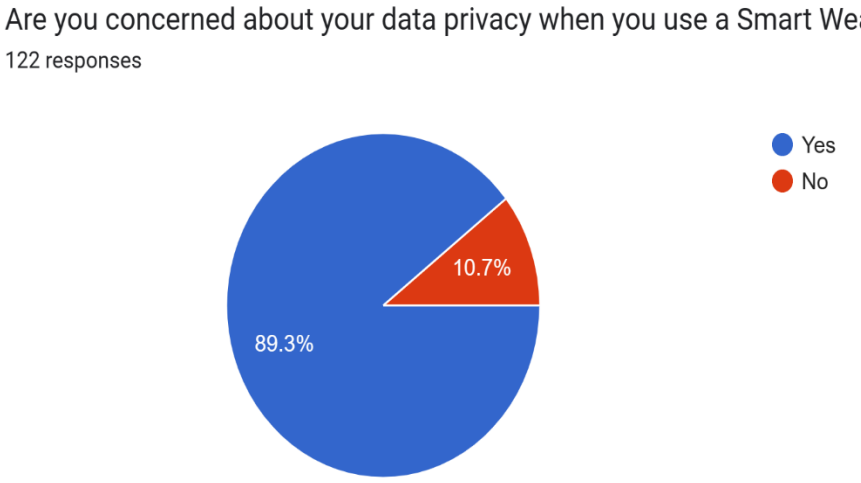
- A majority of respondents, 110, are majoring in fields related to Engineering, Cybersecurity, Computer Science, Information Systems, or Medical Technology Quality programs.

3. Familiarity with Smart Wearable Medical Devices:



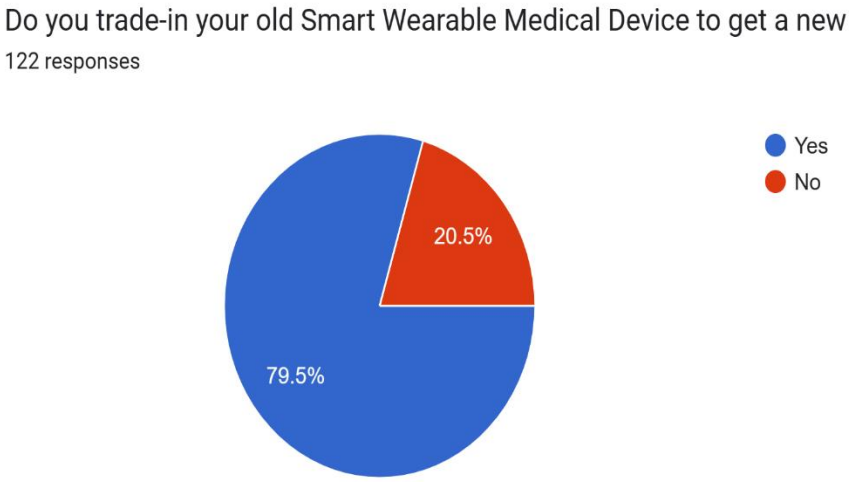
- 99 respondents use Smart Wearable Medical Devices, while 23 are familiar but do not use them.

4. Concerns about Data Privacy:



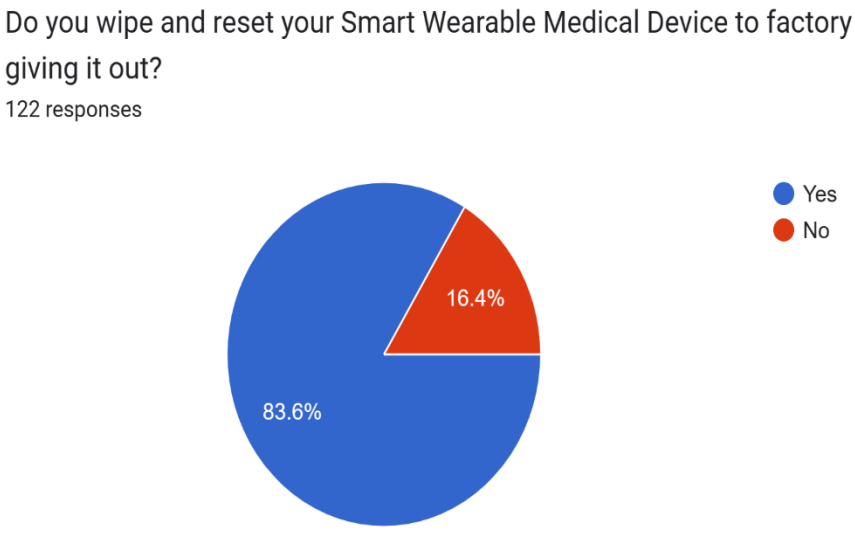
- 109 respondents express concern about their data privacy when using Smart Wearable Medical Devices, while 13 are not concerned.

5. Trade-in Behaviour:



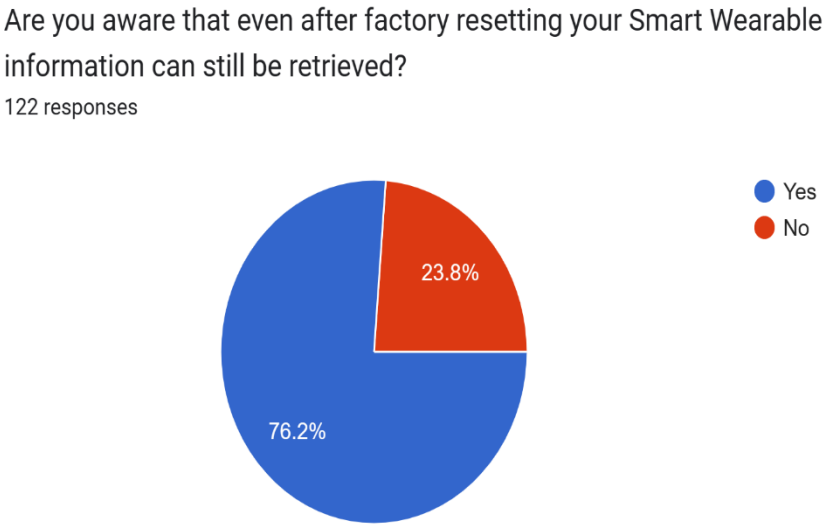
- 97 respondents trade-in their old Smart Wearable Medical Devices to get new ones, while 25 do not.

6. Factory Resetting Devices:



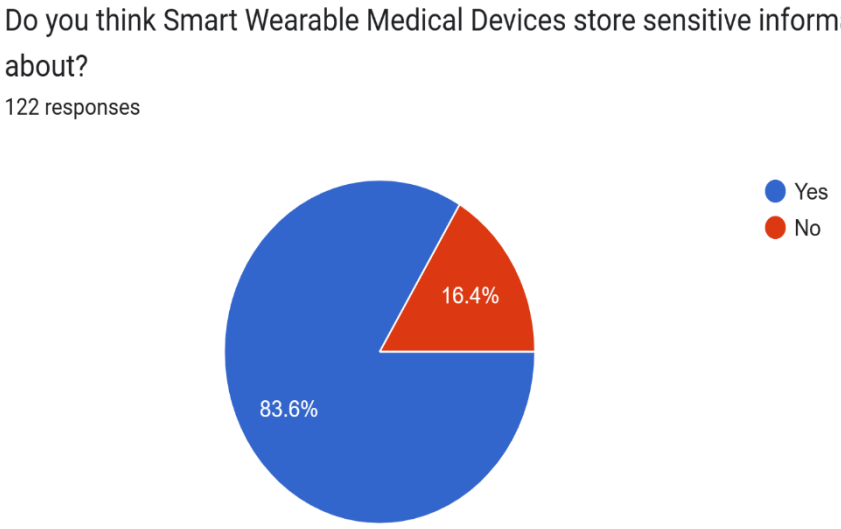
- A majority of respondents, 102, wipe and reset their Smart Wearable Medical Devices to factory reset mode before selling or giving them out, while 20 do not.

7. Awareness of Data Retrieval After Factory Reset:



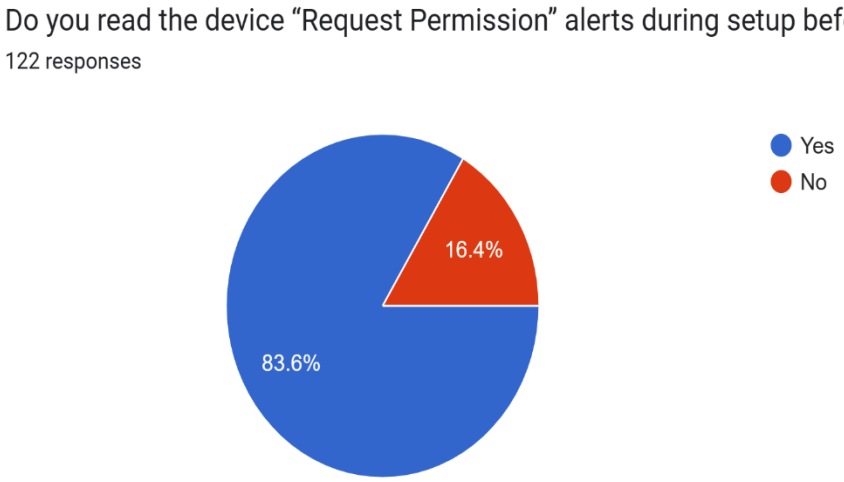
- 93 respondents are aware that even after factory resetting their Smart Wearable Medical Devices, their information can still be retrieved, while 29 are not aware.

8. Perception of Stored Sensitive Information:



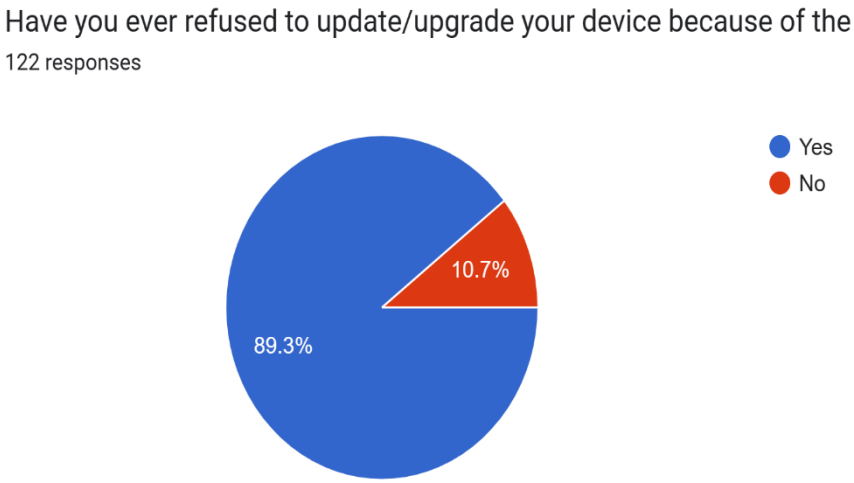
- 102 respondents believe that Smart Wearable Medical Devices store sensitive information they should be worried about, while 20 do not.

9. Attention to Permission Alerts During Setup:



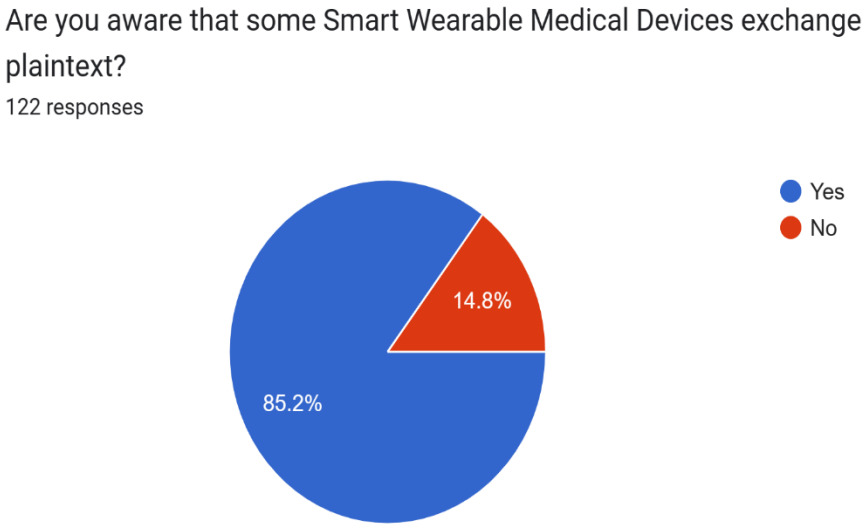
- 102 respondents read the device 'Request Permission' alerts during setup before accepting or ignoring them, while 20 do not.

10. Impact of Permission Alerts on Updates/Upgrades:



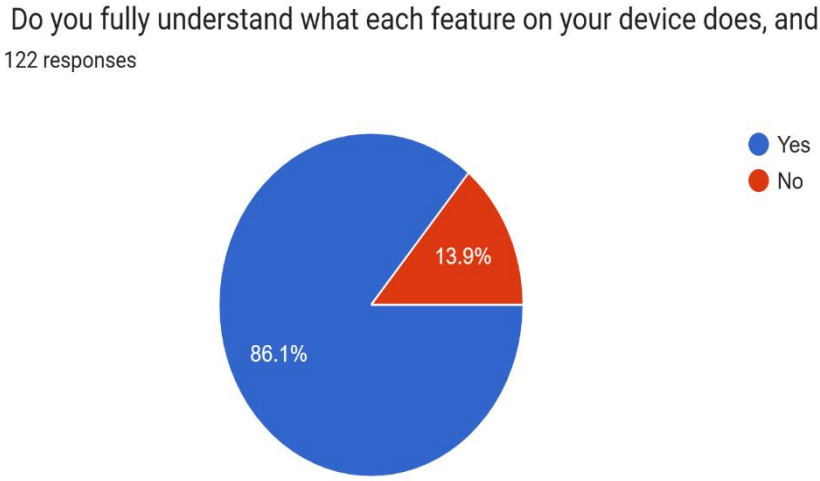
- 109 respondents have refused to update/upgrade their device because of the 'Request Permission', while 13 have not.

11. Awareness of Data Exchange in Plaintext:



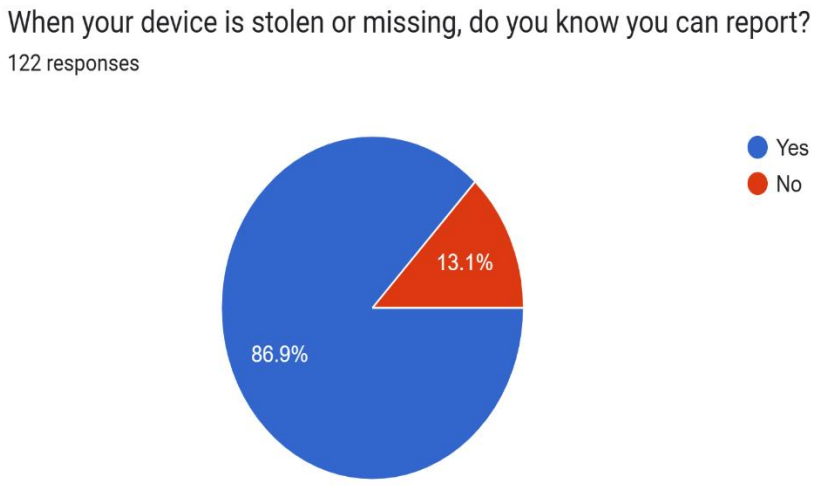
- 109 respondents have refused to update/upgrade their device because of the 'Request Permission', while 13 have not.

12. Understanding of Device Features:



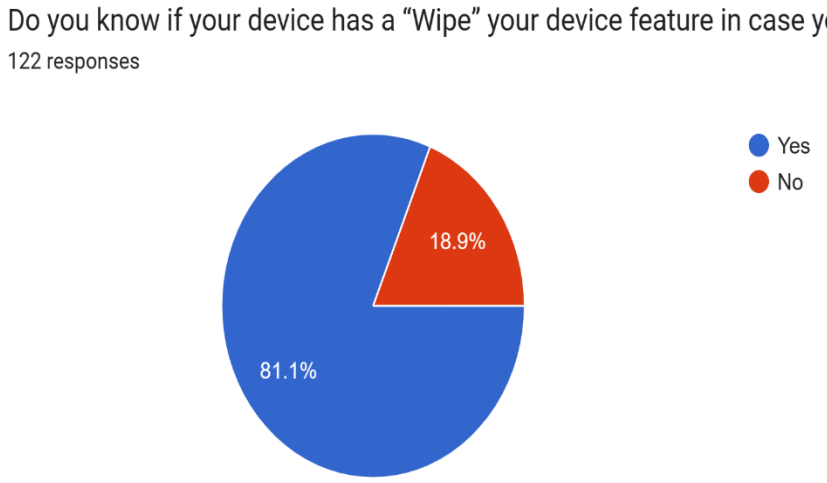
- 105 respondents fully understand what each feature on their device does and how it works, while 17 do not.

13. Knowledge of Reporting Lost or Stolen Devices:



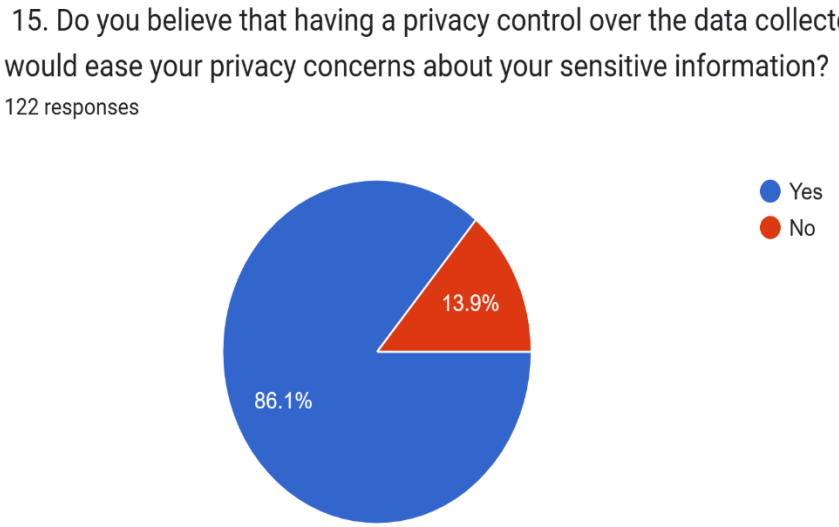
- 106 respondents know they can report when their device is stolen or missing, while 16 do not.

14. Awareness of Device Wiping Feature:



- A significant portion (75) knows if their device has a "Wipe" feature in case it is stolen or lost.

15. Impact of Privacy Controls on Concerns:



- The majority (80) believe that having privacy controls over the data collected or saved by their devices would ease their privacy concerns about sensitive information.

ALL RESPONSES ARE TRUE AND GENUINE

LIMITATIONS

The above text provides a comprehensive overview of smart wearable medical devices, their applications, and the objectives of a study aimed at understanding college students' perceptions and usage patterns of such devices. However, it could benefit from addressing a few limitations:

1. Scope Limitation: The text focuses primarily on college students' perspectives and does not discuss the views of other demographic groups. It's important to acknowledge that perceptions of security and privacy may vary across different age groups, professions, or cultural backgrounds.

2. Generalization: While the study aims to understand perceptions and behaviours related to smart wearable medical devices among college students, it may not capture the full diversity of opinions within this demographic. College students come from varied backgrounds and may have different experiences, attitudes, and concerns regarding these devices.

3. Data Collection Methods: The text mentions the distribution of the survey to random college students via email, QR codes, and social media platforms. While this approach can reach a broad audience, it may introduce selection bias, as only those who are active online or willing to participate in surveys may respond. Additionally, relying solely on self-reported data may limit the study's validity.

4. Cultural and Contextual Factors: The text does not explicitly address how cultural or contextual factors may influence perceptions and behaviours related to smart wearable medical devices. Cultural norms, trust in technology,

and healthcare systems can significantly impact individuals' attitudes towards these devices and their willingness to share personal health data.

5. Technology Evolution: The text briefly mentions the rapid growth of smart wearable devices but does not delve into recent advancements or emerging technologies in this field. As technology continues to evolve, new features, functionalities, and security challenges may arise, which could affect users' perceptions and behaviours.

6. Ethical Considerations: The text does not explicitly discuss ethical considerations related to data privacy, informed consent, or potential biases in the study design or analysis. Addressing these ethical concerns is crucial for ensuring the integrity and validity of the research findings.

CONCLUSION AND RECOMMEDATIONS

The study delved into the multifaceted landscape of Smart Wearable Medical Devices (SWMDs) among college students, aiming to understand their usage patterns, perceptions of security and privacy, protective measures, and strategies for improving security. Through an analysis of survey data and discussions, several key findings emerged.

Firstly, the motivations behind college students' adoption or rejection of SWMDs were diverse, with factors such as price considerations, convenience, and perceived necessity influencing their decisions. Additionally, concerns regarding security and privacy played a significant role in shaping attitudes towards these devices.

Secondly, college students exhibited varying perceptions of the security and privacy implications associated with SWMDs. While some were comfortable with data collection and sharing practices, others expressed apprehensions about potential breaches of privacy or security vulnerabilities. This underscores the importance of addressing these concerns to foster greater trust and confidence in SWMDs.

Thirdly, college students employed a range of protective measures to mitigate security risks associated with SWMDs. These measures included adjusting privacy settings, utilizing additional security features, and seeking out information on best practices for safeguarding personal data.

Finally, recommendations for enhancing security in the usage of SWMDs were proposed. These recommendations encompassed both technical measures, such as implementing stronger encryption protocols and improving data handling practices, as well as educational initiatives aimed at raising awareness about security risks and promoting responsible use of SWMDs.

Based on the findings of the study, several recommendations are put forth to promote the safe and responsible use of Smart Wearable Medical Devices among college students and beyond:

1. Manufacturers should prioritize the implementation of robust security measures, including encryption protocols and secure data handling practices, to protect users' personal information from unauthorized access.

2. Clear and transparent communication regarding data collection, sharing practices, and security measures should be provided to users to foster trust and confidence in SWMDs.

3. Educational initiatives aimed at raising awareness about security risks associated with SWMDs should be developed and promoted among college students. These initiatives could include workshops, seminars, and informational campaigns on best practices for safeguarding personal data.

4. Collaboration between stakeholders, including manufacturers, policymakers, healthcare providers, and consumer advocacy groups, is essential to address security and privacy concerns related to SWMDs comprehensively.

5. Further research is warranted to continue exploring the evolving landscape of SWMDs, including emerging security threats and innovative solutions for enhancing security and privacy protections.

By implementing these recommendations, stakeholders can work towards creating a safer and more secure environment for the adoption and utilization of SWMDs, ultimately contributing to improved healthcare outcomes and enhanced user experiences.

REFERENCES

Adelowo, E. (2021, june). *College Students Perception of Privacy in Smart Wearable Medical Devices*. Retrieved from plumx metrics: https://repository.stcloudstate.edu/msia_etds/118/

Geoffrey S. Ginsburg, R. W. (2024, march 20). *Key Issues as Wearable Digital Health Technologies Enter Clinical Care*. Retrieved from https://www.nejm.org/doi/full/10.1056/NEJMra2307160

Hashem A. Almusawi, C. M. (2021, August 01). *Wearable Technology in Education: A Systematic Review*. Retrieved from https://dl.acm.org/doi/abs/10.1109/TLT.2021.3107459

James Ives, M. (2019, April 30). *Study reveals older women's perceptions of wearable and smart home activity sensors*. Retrieved from https://www.news-medical.net/news/20190430/Study-reveals-older-womens-perceptions-of-wearable-and-smart-home-activity-

Matthew Smuck, C. A. (2021). *The emerging clinical role of wearables: factors for successful implementation in healthcare*. Retrieved from https://www.nature.com/articles/s41746-021-00418-3

Md Ismail Hossain, A. F. (2022, march 30). *Understanding Wearable Device Adoption: Review on Adoption Factors and Directions for Further Research in Smart Healthcare*. Retrieved from https://link.springer.com/chapter/10.1007/978-3-030-98741-1_54

Naghmeh Niknejad, W. B. (n.d.). *A comprehensive overview of smart wearables: The state of the art literature, recent advances, and future challenges*. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0952197620300348

Samira Farivar, M. A. (2020, august 04). *Wearable device adoption among older adults: A mixed-methods study*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7402656/

Sanjit Thapa, A. B. (2023, april 14). *Security Risks and User Perception towards Adopting Wearable Internet of Medical Things*. Retrieved from Int J Environ Res Public Health. : https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10139409/

Sanjit Thapa, A. B. (2023, april 14). *Security Risks and User Perception towards Adopting Wearable Internet of Medical Things*. Retrieved from https://www.mdpi.com/1660-4601/20/8/5519

Shi, D. J. (2021, feb 5). *Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7884134/

Vidhi Kapoor, R. S. (2020, april 2). *Privacy Issues in Wearable Technology: An Intrinsic Review*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3566918