Evaluating User Perceptions of Privacy Protection in Smart Healthcare Services

Huan Gua, Elias Seid , Yuhong Li , Fredrik Blix

Department of Computer and Systems Sciences

Stockholm University, Sweden

IARIA

Stockholm University

Agenda

01

Introduction

background, research problem, research question

02

Method

research strategy, data collectionmethod, data analysis method, ethicalconsiderations

03

Results

results table, code system

04

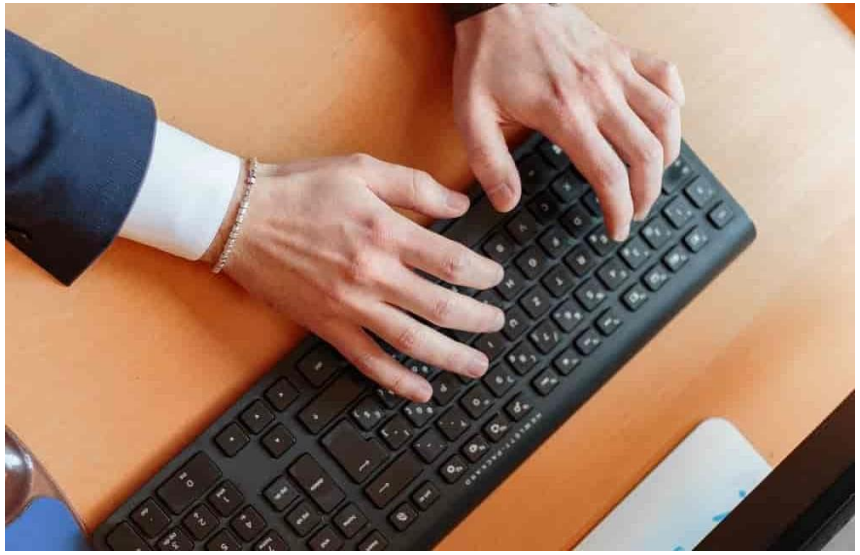
Discussion

discussion of the results, recommendations, ethical and sociteal implications, limitations and future research directions

PART 01

Introduction

background, research problem,
research question, extended background



D. Eckhoff and L Wagner, "Privacy in the Smart City-Applications, Technologies, Challenges, and Solutions," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 489-516, 2018, doi: 10.1109/COMST.2017.2748998.

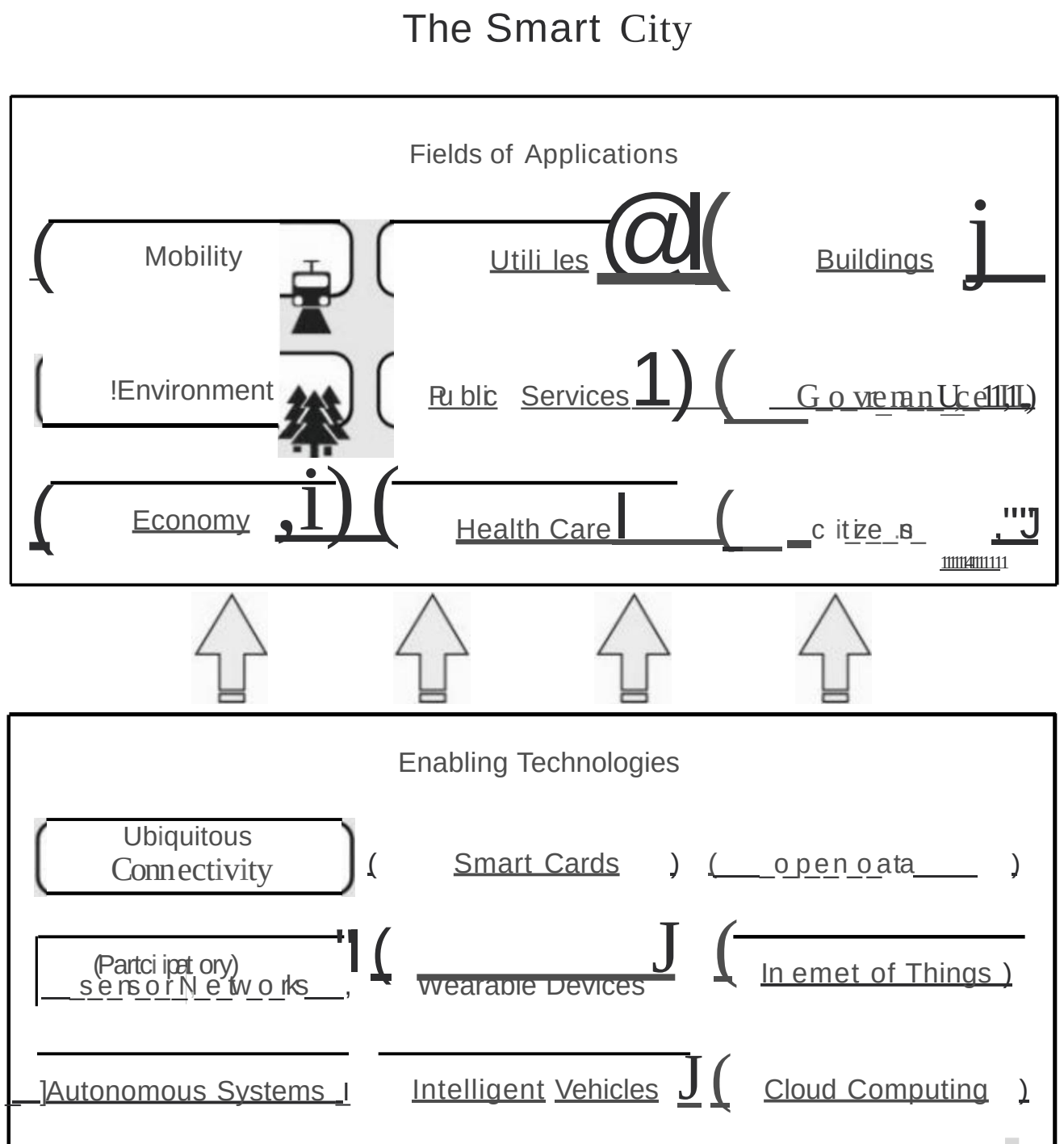


Fig. 1.

smart city applications and enabling technologies

Smart ealthcare

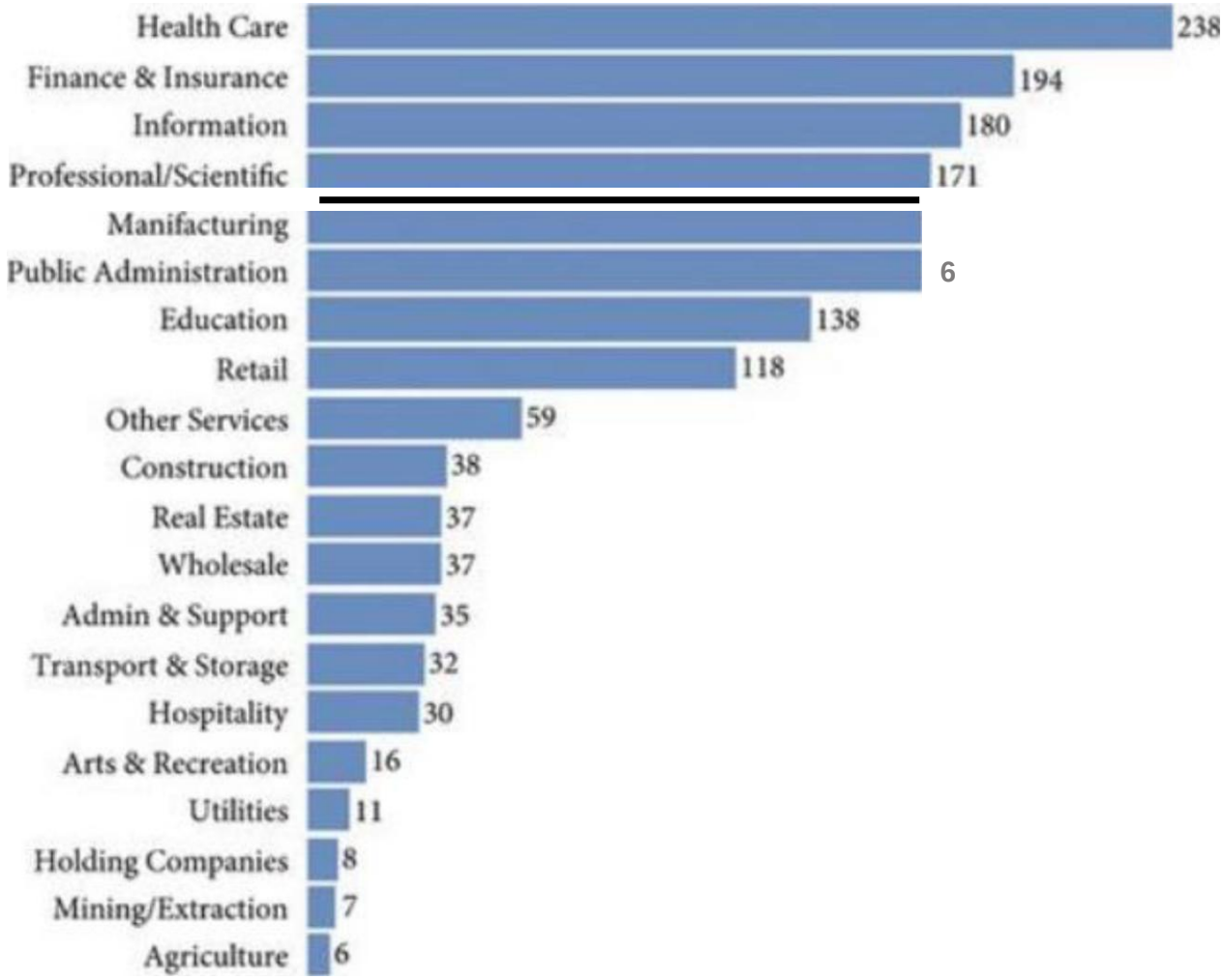
D. El Majdoub1, H. El Bakkal'i. S. Sadki. Z. Maqour, and A. Leghmid, "The Systematic Literature Review of Privacy Preserving Solutions in Smart Healthcare Environment." Security and Communication Networks, vol. 2022, no. 1, p. 5642026, 2022 doi: hts://doi.org/10.1155/2022/5642026.

Art. 9 GDPR

Processing of s ec1a categories of pers on al data

P ocess,ng of :>ersonal d t revealing t ,al or e hn,c or1g1n, poht,cal o p1111os, rel1g1ous or ph1losoph1cal beliefs, or trade urnon m mbersh1p, and lhe processing of genetic data. biometric data l'O the purpose of uniquely identifying a natu al person, data coocem1n 1 „r dala concerning a natural person's sex life or sexual onentat on shall be proh1b1ted

affect a per on s health and life



he 2021 Mid-Year Data Breach Quick View Report

Research problem

understand users' perceptions of specific privacy protection measures in smart healthcare services

What is the research gap?

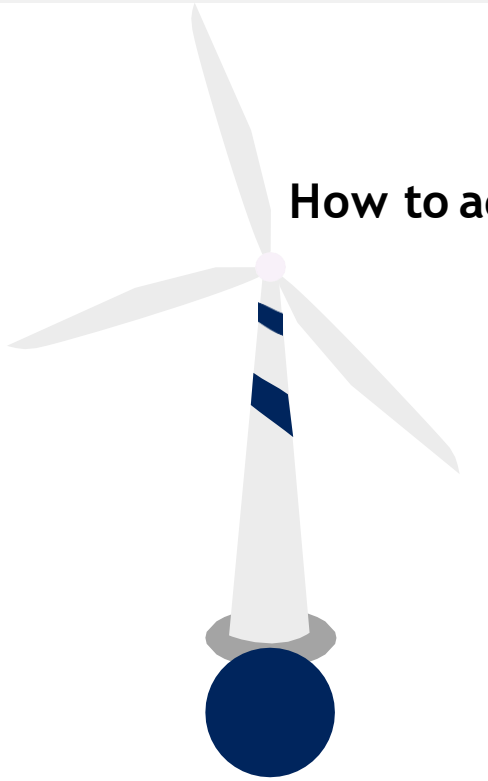
little attention to the human factors involved in healthcare data security.

insufficient studies regarding understanding of privacy protection measures

Why the gap should be addressed ?

perceptions of privacy protection measures—directly impact their intention to accept smart healthcare services and their behavior while using smart healthcare services.

How to address?



first step in this process is ensuring they perceive and recognize the privacy measures in place.

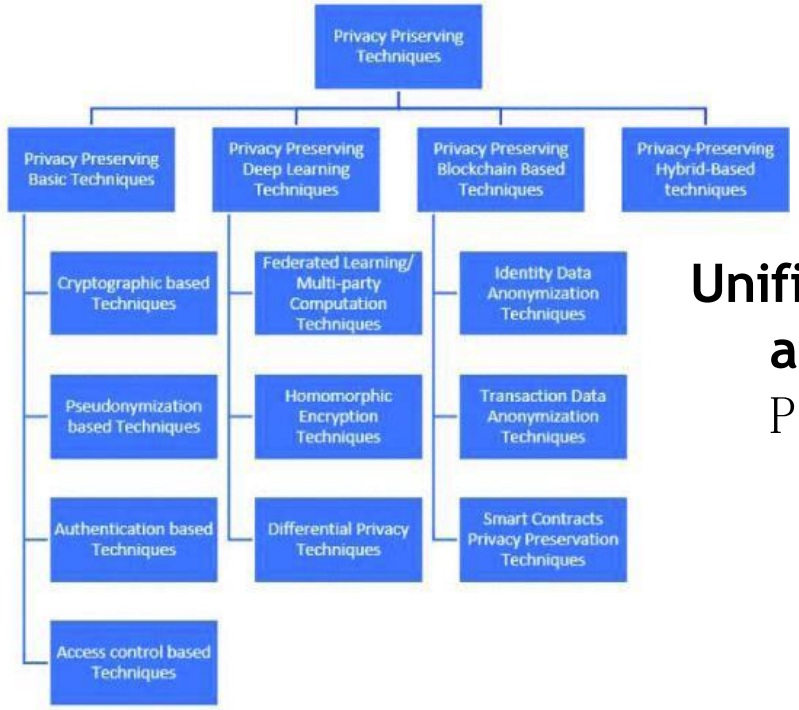
Research question and aim

Question
How do users perceive privacy protection measures in smart healthcare services?

Aim
explore users' concerns and expectations when perceiving privacy protection measures in smart healthcare services.

Extended background

Privacy protection mesures Technical & Organizational



TAM

Technology Acceptance Model

perceived usefulness
perceived ease ofuse

Smart healthcare services

location-based tracking
high-speed communication
network-enabled services
IoT applications
mobile health solutions
AI-driven services
robotic systems
extended reality technologies
and telehealth

UTAUT

Unified Theory of Acceptance and Use of Technology

Performance Expectancy
Effort Expectancy
Social Influence
Facilitating Conditions

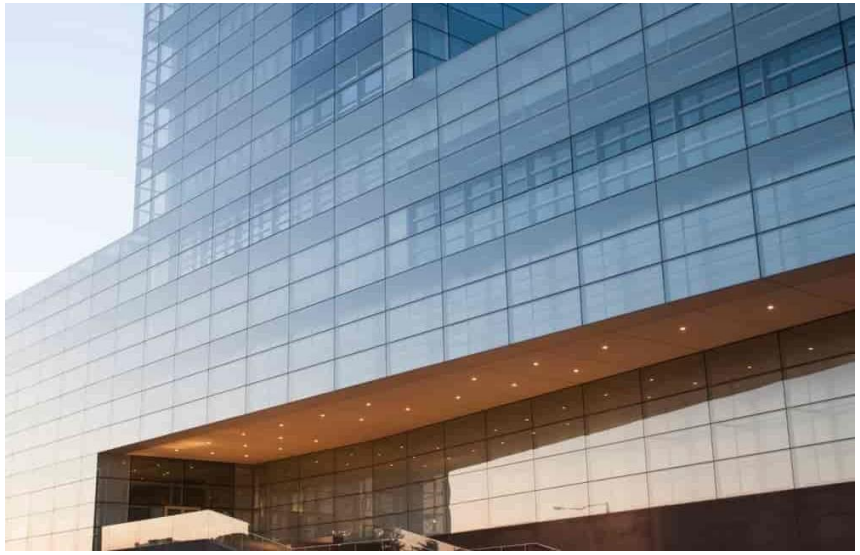
Privacy calculus theory

perceived benefits
perceived privacy risks

PART 02

Method

research strategy, data collection method, data analysis method, ethical considerations



Interview Participants

Participant	Age Group	Gender	Nationality	Industry/Major
1	Middle-aged	Female	Sweden	Manufacturing Industry
2	Middle-aged	Male	India	Food & Beverage Industry
3	Youth	Male	United States	Media Industry
4	Youth	Female	Germany	Engineering Student
5	Older adults	Male	United States	Manufacturing Industry
6	Youth	Female	Sweden	Finance Student
7	Middle-aged	Female	Sweden	Gaming Industry
8	Older adults	Male	China	Retiree
9	Youth	Male	Finland	Medical Industry
10	Older adults	Female	China	Retiree

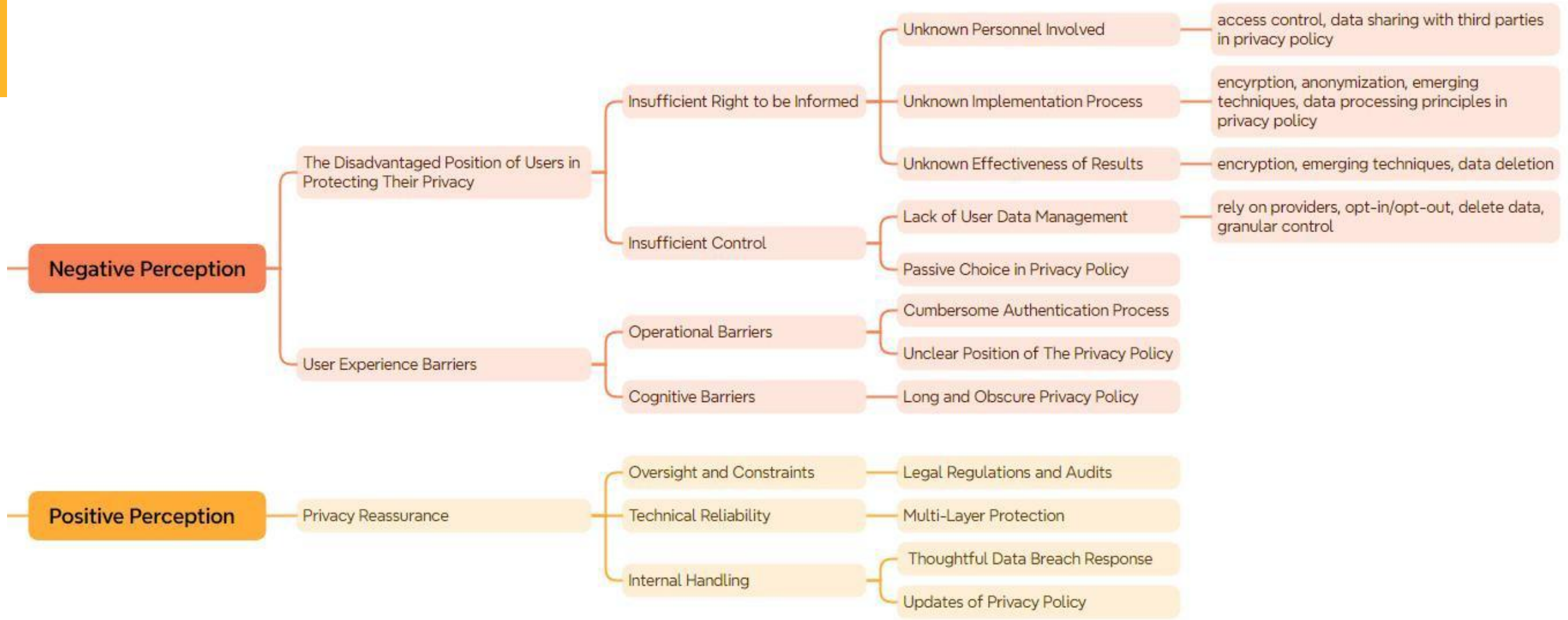
- Research strategy
- Data collection method
- Data analysis method
- Ethical considerations

PART 03

Results

results table, code system

Themes Subthemes Codes



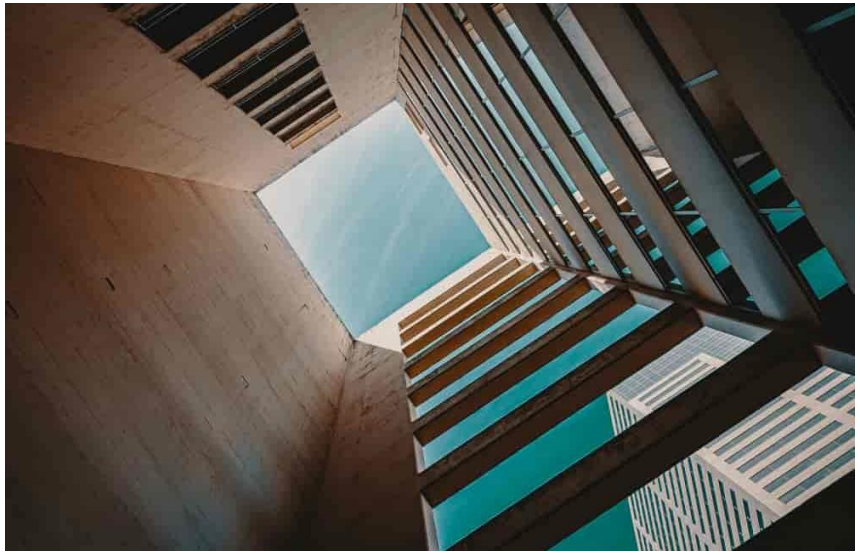
Code Systems

Codes	Sources	References
The Disadvantaged Position of Users in Protecting Their Privacy	10	201
Insufficient Control	10	78
lack of user data management	10	49
passive choice in privacy policy	10	29
Insufficient Right to be Informed	10	100
unknown personnel involved	10	44
unknown implementation process	10	84
unknown effectiveness of results	10	73
Privacy Reassurance	10	147
Technical Reliability	7	26
multi-layer protection	7	21
Oversight and Constraints	10	39
legal regulations and audits	10	28
Internal Handling	10	31
thoughtful data breach response	10	21
updates of privacy policy	8	23
User Experience Barriers	10	152
Cognitive Barriers	10	54
long and obscure privacy policy	10	27
Operational Barriers	10	35
cumbersome authentication process	10	25
unclear position of the privacy policy	2	2

PART 04

Discussion

discussion of the results,
recommendations,
ethical and societal implications,
limitations and future research directions

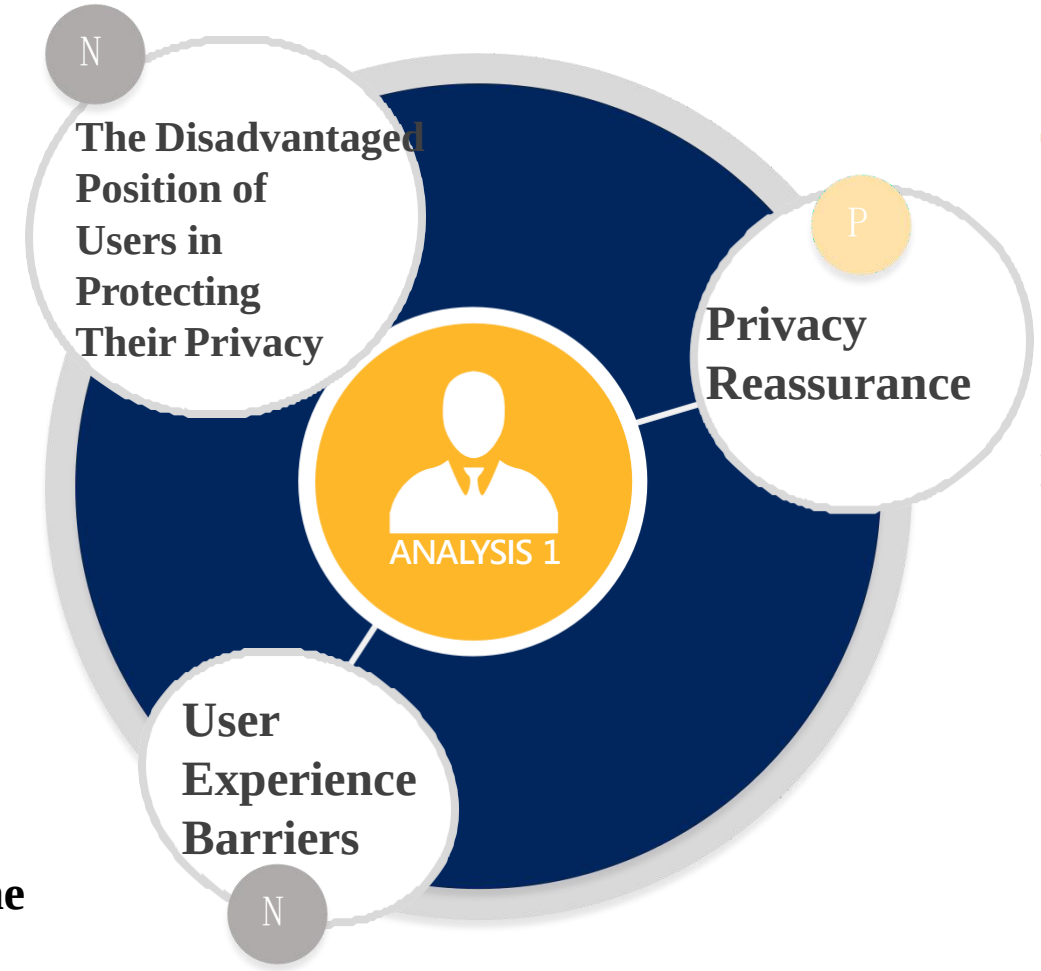


Discussion of the results

P positive perceptions

N negative perceptions

insufficient right to be informed & insufficient control → perceived privacy risks in privacy calculus theory



Technical Reliability → multi-layer protection→ "performance expectancy"（PE）in the UTAUT model

Cognitive barriers → Long and Obscure Privacy Policy→"facilitating condition"（FC）and "effort expectancy"（EE）factors in the UTAUT model.

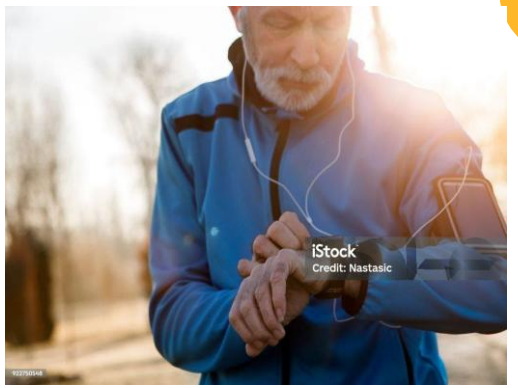
Oversight and Constraints → Legal and audit constraints → "facilitating conditions"（FC）in the UTAUT model

Operational barriers → Cumbersome Authentication Process & Unclear Position of The Privacy Policy → low level of perceived ease of use in the TAM model

Internal Handling → updates its privacy policy & thoughtful data breach response → "facilitating conditions"（FC）in the UTAUT model

Perceptions across multiple smart healthcare services

wearable devices



telehealth platforms

medical history → health information sensitivity → perceived privacy risk

mobile health management applications

medicine delivery system

offline delivery scenario

Recommendations

Improve the perceptibility of privacy protection measures.

based on insufficient right to be informed

Optimize the user experience concerning the barriers associated with the use of privacy protection measures.

base on user experience barriers

Enhance user participation in data processing activities.

based on insufficient control

Strengthen and educate users' awareness of privacy protection measures.

Ethical and Societal Implications

The Disadvantaged Position of Users in Protecting Their Privacy

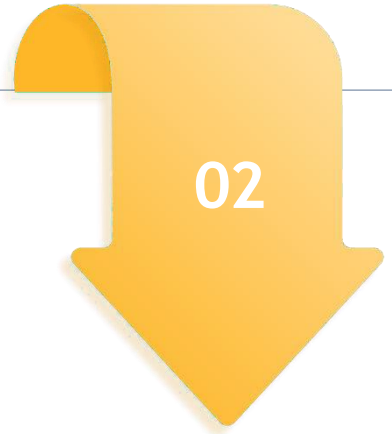
Ethical: Providers continue to reinforce their control over user data rather than genuinely empowering users with privacy autonomy.

Societal: not only hinder the wider adoption of the services but also negatively affect the relationship between users and other stakeholders within smart healthcare.

Contributions

Theoretical

helps address the research problem by complementing the user perspective on privacy protection measures in smart healthcare



Practical

identifies the limitations of current privacy protection measures in smart healthcare services and offers concrete recommendations to alleviate users' concerns

Limitations and Future Research Directions

qualitative analysis and small sample size

combines qualitative interviews with a larger-sample quantitative questionnaire, a comparative analysis between older people in Europe and those in Asia can better explore the socio-cultural contexts that may shape participants' privacy perceptions.

lack of comparative analysis of privacy protection measures

users' potential varying perceptions of different types of encryptions used in telehealth platforms and mobile health management applications can be investigated.

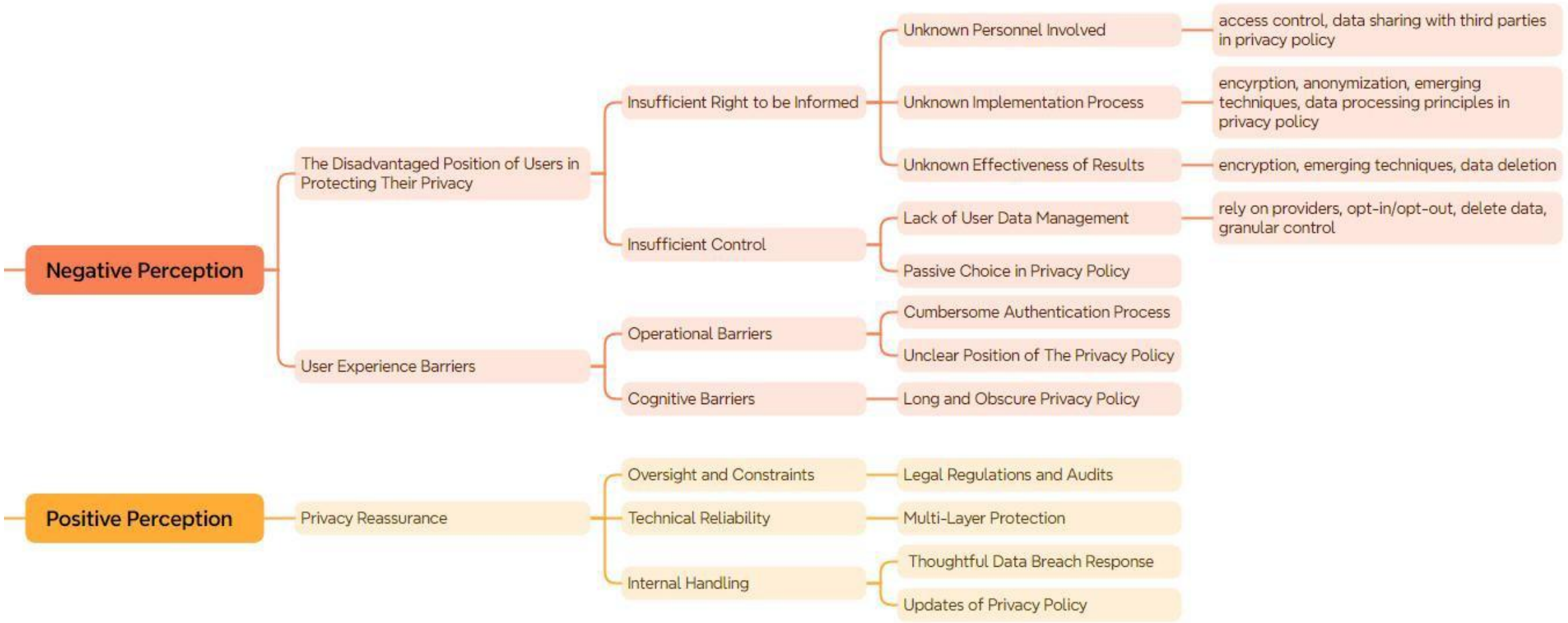
theoretical depth

refine the perceived privacy risks within the privacy calculus theory, proposing the construct related to the perceived opacity of privacy protection measures to validate its impact on trust and acceptance of multiple smart healthcare services

recommendation specificity

a case study exploring how to embed a user-centric end-to-end encryption design into a particular telehealth platform.

Conclusions



References

F. Tazi, A. Nandakumar, J. Dykstra, P. Rajivan, and S. Das, "SoK: Analyzing Privacy and Security of Healthcare Data from the User Perspective," *ACM Trans. Comput. Healthcare*, vol. 5, no. 2, p. Article 11, 2024, doi: 10.1145/3650116.

E. M. Schomakers, C. Lidynia, and M. Ziefle, "Listen to My Heart? How Privacy Concerns Shape Users' Acceptance of e-Health Technologies," in *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 21-23 Oct. 2019 2019, pp. 306-311, doi: 10.1109/WiMOB.2019.8923448.

M. Duckert and L. Barkhuus, "Protecting Personal Health Data through Privacy Awareness: A study of perceived data privacy among people with chronic or long-term illness," *Proc. ACM Hum.-Comput. Interact.*, vol. 6, no. GROUP, p. Article 11, 2022, doi: 10.1145/3492830.

M. N. Alraja, H. Barhamgi, A. Rattrout, and M. Barhamgi, "An integrated framework for privacy protection in IoT — Applied to smart healthcare," *Computers & Electrical Engineering*, vol. 91, p. 107060, 2021/05/01/ 2021, doi: https://doi.org/10.1016/j.compeleceng.2021.107060.

H. Kwon *et al.*, "Review of smart hospital services in real healthcare environments," *Healthcare informatics research*, vol. 28, no. 1, pp. 3-15, 2022.

B. R. Louassef and N. Chikouche, "Privacy preservation in healthcare systems," in *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)*, 20-21 Nov. 2021 2021, pp. 1-6, doi: 10.1109/AI-CSP52968.2021.9671083.

References

V. Garcia-Font, "SocialBlock: An architecture for decentralized user-centric data management applications for communications in smart cities," *Journal of Parallel and Distributed Computing*, vol. 145, pp. 13-23, 2020/11/01/ 2020, doi: https://doi.org/10.1016/j.jpdc.2020.06.004.

D. Eckhoff and I. Wagner, "Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 489-516, 2018, doi: 10.1109/COMST.2017.2748998.

V. Zimmermann, "Smart cities as a testbed for experimenting with humans? - Applying psychological ethical guidelines to smart city interventions," *Ethics and Information Technology*, vol. 25, no. 4, p. 54, 2023/10/24 2023, doi: 10.1007/s10676-023-09729-3.

J. Sanghavi, "Review of Smart Healthcare Systems and Applications for Smart Cities," in *ICCCE 2019*, Singapore, A. Kumar and S. Mozar, Eds., 2020// 2020: Springer Singapore, pp. 325-331.

E. Union, "General Data Protection Regulation (GDPR)," ed, 2016.

THANK YOU