Protocol for Systematic Mapping Study on Security and Privacy for mHealth and uHealth

Leonardo Horn Iwaya[a,*], Aakash Ahmad[b], M. Ali Babar[a]

[a] *School of Computer Science, University of Adelaide, Australia*
[b] *College of Computer Science and Engineering, University of Ha'il, Saudi Arabia*

Abstract

An increased adoption of mobile and pervasive technologies empower users to exploit handheld devices and embedded sensors for health care services offered by mobile health (mHealth) and ubiquitous health (uHealth) systems. Despite the provided features such as portable and context sensitive services, m/uhealth class of systems face some critical challenges related to security and privacy of personal information and health critical data. The objective of this research is to identify, classify, compare, and evaluate state-of-the-art on security and privacy specific issues for m/uHealth systems. We have used evidence-based software engineering (EBSE) approach to conduct a systematic mapping study (SMS) of the published research on security and privacy of m/uhealth systems. For the SMS, we qualitatively selected 365 studies to (i) classify the type and demography of research and (ii) synthesise research themes, recurring challenges, prominent solutions (i.e., research outcomes) and their evaluations (i.e., practical validations).

1. Context, Scope and Contributions of the SMS

Context: The future of healthcare is hyper-connected, highly pervasive and personalised. Advanced technologies in mobile health (mHealth) and ubiquitous

*The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

*Corresponding author
Email address: leonardo.iwaya@adelaide.edu.au (Leonardo Horn Iwaya)

health (uHealth) systems provide a full-range of wellness and fitness applications as well as clinical and medical systems, impacting the everyday life of individuals, patients, and healthcare providers. At the center of this technological revolution lies huge amounts of personal health data. If data is the new oil, health data in particular is one of the most valuable assets to m/uHealth players for both competitive innovation as well as to deliver high-quality services.

On the one hand, advances bring great promises of improved health outcomes and increased convenience for individuals. Data-driven applications deliver such promises by leveraging from near real-time data collection and analytics, generating actionable insights to all stakeholders. On the other hand, these data-hungry systems also raise serious concerns with respect to the privacy of individuals.

Privacy data breaches in healthcare information systems have serious negative impacts to its data subjects. Such impacts can range from embarrassment and reputation damage to various forms of discrimination that can adversely affect rights and freedoms as well as physical and mental health of individuals. It is therefore critical to incorporate security and privacy into the design, at the very core of these cutting-edge technologies, so as to avoid common pitfalls and mitigate potential privacy harms.

With that in mind, we adopted Evidence-Based Software Engineering (EBSE) approach to conduct an extensive Systematic Mapping Study (SMS) [1] on the topic of security and privacy for m/uHealth systems. To complement the SMS, we also performed an in-depth thematic analysis of the studies that have been evaluated in practice, discussing these solutions, their evaluation strategies and impacts on industry scale systems. To the best of our knowledge, there is no equivalent survey, systematic review, or mapping study of literature on this topic. Therefore, this SMS identifies, classifies, compares, and communicates existing research and its implications to relevant stakeholders (i.e., researchers, practitioners, policy-makers, healthcare providers, and broader society).

Scope and Contributions: This primary objective of this SMS is to analyse the body of knowledge and provide an overview on the topic in terms of: 1)

research and contribution types; 2) research trends and taxonomy; 3) challenges and solutions for security and privacy controls; 5) m/uHealth application categories; and, 6) role of various devices and technologies in m/uHealth systems. Bibliographical information and trends of research also pinpoint predominant areas of research, under-researched areas and gaps, as well as future dimensions of research. The primary contributions of this SMS are:

- Classify and compare existing and emerging solutions for security and privacy for m/uHealth in the form of systematic maps, classification taxonomy, and illustrative trends.
- Evaluation focused analysis of the solutions - implemented in practice - to identify commons themes and appraising the quality of these evaluation studies.

Research Impact: Empirical evidence, research, and development of security and privacy solutions is lacking and research studies needs to be carefully evaluated before academic solutions can be adopted or extended in an industrial context. The results of this SMS can be beneficial for:

- Researchers who are interested in a quick identification of the existing research that can help to formulate new hypothesis to be tested and propose innovative solutions for emerging challenges of security and privacy of m/uHealth systems.
- Practitioners who want to understand academic solutions in terms of architectural models, implementation strategies, and evaluation frameworks etc. that could be adopted in an industrial context.

2. Research Method and Study Protocol

In order to plan, conduct, and document this SMS, we followed evidence based software engineering approach and specifically adhered to recommendations and guidelines to conduct systematic reviews and mapping studies [1].

An illustrative view of the adopted research method is presented in Figure 1 that highlights three phases of research and each phase comprises of two tasks. Each phase has an outcome. For example, the initial phase named Planning the Mapping Study comprises of two tasks that relate to (i) identification of the needs and (ii) specification of the research questions for the mapping study. The outcome of this phase is scope and objectives of the SMS in terms of research questions that need to be investigated. SMS planning is the precondition for later phases of the methodology. By adopting well-known methodology from [1] as in Figure 1, we aim to strengthen the findings, support objective interpretation of results, minimize any bias and enable reproducible results. In the remainder of this section, we discuss phases of the research methodology.

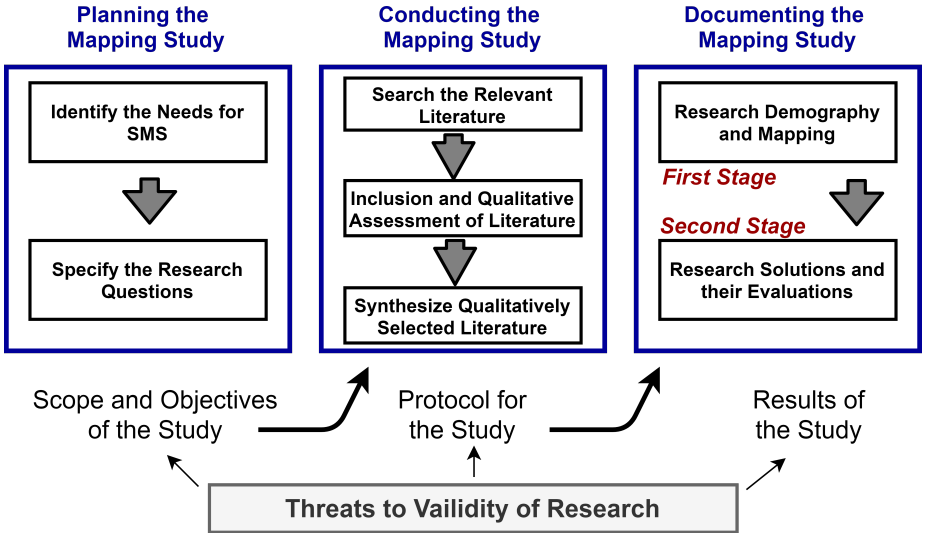

Figure 1: Methodology overview of the mapping process and evaluation focused analyses.

2.1. Phase I – Planning the Mapping Study

2.1.1. Identify the Needs for SMS

Despite lot of attention and published research, there is no effort to systematically identify and investigate a collective impact of the existing research on secure and private m/uHealth systems. An objective investigation of the

state-of-the-art on secure and private m/uHealth systems can highlight research progression maturation, emerging trends and futuristic challenges that are currently lacking in the literature. In order to ensure that no prior survey, mapping study, or systematic review (i.e., secondary studies) have been conducted, we searched the most prominent digital libraries including IEEE, ACM, Springer, Science Direct and Scopus along with indexing engine Google Scholar (search date 02/10/2019). The search string that we executed on these digital libraries and indexing engines to locate any secondary studies on security and privacy of m/uHealth systems is detailed in Listing 1. Based on Listing 1, none of the retrieved literature was related to the outlined research questions in Section 2.1.2 that motivated the needs for the proposed SMS.

```
(‘‘Systematic Literature Review’’ OR ‘‘Systematic Mapping’’
OR ‘‘SMS’’ OR ‘‘SLR’’ OR ‘‘Study’’ OR ‘‘Survey’’) AND
((‘‘ubiquitous health*’’ OR ‘‘uhealth’’ OR ‘‘u-health’’ ) OR
(‘‘mobile health*’’ OR ‘‘mhealth’’ OR ‘‘m-health’’) ) AND
(‘‘secur*’’ OR ‘‘*security’’ OR ‘‘privacy*’’ OR ‘‘crypto*’’ )
```

Listing 1: Search String to Identify Secondary Studies on Secure and Private m/uHealth.

2.1.2. Specifying the Research Questions

To conduct the mapping study and present its results, we specify a number of Research Questions (RQs) for this SMS. Answers to the specified RQs represent results of the SMS and justify the scope of the SMS. In addition, answers to individual RQs help us objectively document the results of the study. In the following, we present the RQs along with outlines objective(s) for each of the RQ that focus on:

A. Demography Analysis – Types, Frequency, and Venues of Research Publications

RQ-1 *What is the type of and frequency of published research in the area of security and privacy of m/uHealth systems?* Objective(s): To understand and highlight the (i) type of published research in terms

of conference proceedings, journal articles, symposium papers etc., and (ii) frequency of published research that reflects progression and growth of research in terms of number of publication over the years.

RQ-2 *What are the prominent venues of research publications in the area under investigation?* Objective(s): To list and analyse the publication venues such as specific conference proceedings, journal articles and special issues along with book chapters that highlight prominent venues of research emergence that are detailed below.

B. Research Mapping – Existing Solutions, their Evaluations, and Validation Research

RQ-3 *What are the proposed solutions of security and privacy of m/uHealth systems?* Objective(s): Identification of the proposed solution represent various research themes – reflecting the body of knowledge – that helps us to investigate the strengths and limitations of existing research.

RQ-4 *What is the state of existing evaluation studies on security and privacy for m/uHealth systems?* Objective(s): Provide a clear picture of the existing research that has been properly evaluated and identify the areas of security and privacy for m/uHealth that are in this the forefront of science.

2.2. Phase II – Conducting the Mapping Study

As per Figure 1, this phase involves searching and qualitative assessment of the relevant literature that is included for review to conduct the SMS, detailed as below.

2.2.1. Search the Relevant Literature

In order to search the relevant literature, we selected the Scopus database as the digital library that indexes more than five thousand publishers, including highly relevant sources such as Elsevier, Springer, MEDLINE, EMBASE, IEEE Xplore and ACM. In order to search literature in Scopus, we considered the

outlined RQs (from Section 2.1.1) to compose the search string based on the key terms that is presented in Table 1.

Table 1: Key terms used divided by groups.

G1	G2	G3
mobile health*	ubiquitous health*	*security
mHealth	uHealth	secur*
m-Health	u-Health	privacy*
		crypto*

Searched articles were also limited to a 5-year period (i.e., from year 2015 - 2019). A pilot search based on search string in Listing 2 suggested little to no relevant publications on the topic before under investigation before the Year 2015. Therefore, in order to avoid exhaustive search and minimize the risk of identifying irrelevant studies, we set the search criteria to only include literature from Year 2015 to 2019 that helped us to retrieve a total of 1249 potentially relevant publications. We also limited the search to peer reviewed scientific publications and book chapters that excludes any white papers, technical report or unpublished work.

```
TITLE-ABS-KEY(
    (("ubiquitous health*" OR "uhealth" OR "u-health")
    OR ("mobile health*" OR "mhealth" OR "m-health"))
    AND (secur* OR *security OR privacy* OR crypto* )
)
```

Listing 2: Composition of Search String for Literature Search.

2.2.2. Study Inclusion – Screening and Qualitative Assessment

Out of 1249 potentially relevant studies, we need to short the most relevant ones to be included for review in the SMS, based on screening and qualitative assessment as in Table 2.

Step I – Screening of the relevant literature: As in Table 2, Step I, i.e., screening have five point criteria to include or exclude the relevant literature

from a total of 1249 publications. The screening was performed based on quickly reviewing the title and abstract of the identified studies. This primary selection of papers was performed by one researcher. When in doubt during the screening process a second researcher is contacted to resolve the inclusion or exclusion of a paper. If any of the criterion from S1 to S5 as in Table 2 resulted in a NO, the publication was excluded immediately. As a result of the screening we identified a total of 539 publications for their qualitative assessment to include or exclude a particular publication.

Step II – Qualitative assessment of screened studies: Qualitative assessment of screened studies allowed us criteria-based assessment of as per the guidelines in [1] and five point criteria as detailed in Table 2. Qualitative assessment criteria helped us to include/exclude studies in a step-wise and objective manner. Specifically, the criterion (Q1 to Q5) enable us to perform quality based ranking and provides a numerical quantification for individual studies. The maximum score for any study can be 1 and minimum as 0. Any study with qualitative assessment score below 0.4 was excluded based on lack of quality to be included in the review. However, during the this screening, we also checked again for consistency following the criterion from S1 to S5 as in Table 2. This revealed that 120 papers were not relevant, because they were not addressing security and/or privacy in their text, even though the title and abstract mentioned it. We also found 36 duplicated studies and for 17 studies the full-text was unavailable. After the qualitative assessment, we select a total of 365 studies to review. Titles and other relevant information about selected 365 studies for the review are in Appendix A.

2.2.3. Synthesize Qualitatively Selected Literature

The last task of Phase II is the classification of the studies in systematic maps. Based on that, we also conducted and evaluation focused analysis of the papers that have been implemented in practice.

Qualitative Assessment and Classification Scheme (Facets): Classification schemes (or facets) contain a set of categories which is representative of

Table 2: Inclusion and exclusion criteria.

Step I – Screening (S) of Relevant Literature	**Yes/No**
S1. Is the study in English language? S2. Is the study a scientific peer-reviewed published research (no white papers or technical reports etc.)? S3. Is the study not a secondary study with no solution proposal (e.g., taxonomy or guidelines)? S4. Is the study not a book? S5. Is the study proposing solutions on security and/or privacy for m/uHealth systems?	
If [Yes] to all five criteria (S1 to S5) then go to Step II, otherwise exclude the study	
Step II – Qualitative (Q) Assessment of Screened Studies	**Y/P/N**
Q1. Are the problem definition and proposed solution(s) clearly presented? Q2. Is the research environment in which the study was carried out properly explained? Q3. Are the research methodology and its organization clearly stated? Q4. Are the contributions of the study properly evaluated? Q5. Are lessons learnt, limitations and future research explicitly mentioned?	

Note: Yes (Y) = 1.0, Partially (P) = 0.5, No (N) = 0.0.

the underlying population. In this SMS we used five facets: (1) research type; (2) contribution type; (3) security and privacy control families; (4) application type; and, (5) used technology. Existing facets already proposed in the literature were adopted instead of creating new classification schemes unnecessarily.

For research type the facet proposed in [2] was used (see Table 3). The contribution type facet was based on [3, 4] (see Table 4). For security and privacy we defined the facet based on the NIST 800-53 (revision 5) standard that provides a broad range of technical and non-technical controls (see Table 5). For m/uHealth we adopted the application categories defined by the World Health Organization in [5] (see Table 6). Lastly, the facet for used technology was the only one created using the keywording method (see Table 7).

Before starting the mapping process, the classification facets were tested for consistency with a subset of 20 papers. In this test, all the papers were classified

using these five facets without difficulties, allowing us to verify our strategy and leverage from existing taxonomies in the literature.

Table 3: Research Type Facet (based on [2]).

Category	**Description**
Validation Research	Techniques investigated are novel and have not yet been implemented in practice. Techniques used are for example experiments, i.e., work done in the lab.
Evaluation Research	Techniques are implemented in practice and an evaluation of the technique is conducted. That means, it is shown how the technique is implemented in practice (solution implementation) and what are the consequences of the implementation in terms of benefits and drawbacks (implementation evaluation). This also includes to identify problems in industry.
Solution Proposal	A solution for a problem is proposed, the solution can be either novel or a significant extension of an existing technique. The potential benefits and the applicability of the solution is shown by a small example or a good line of argumentation.
Philosophical Papers	These papers sketch a new way of looking at existing things by structuring the field in form of a taxonomy or conceptual framework.
Opinion Papers	These papers express the personal opinion of somebody whether a certain technique is good or bad, or how things should been done. They do not rely on related work and research methodologies.
Experience Papers	Experience papers explain on what and how something has been done in practice. It has to be the personal experience of the author.

Table 4: Contribution Type Facet (based on [3, 4]).

Category	**Description**
Model	Representation of observed reality by concepts after conceptualisation
Theory	Construct of cause-effect relationships
Framework	Frameworks/methods related to security and privacy for m/uHealth
Guideline	List of advice
Lessons Learned	Set of outcomes from obtained results
Advice	Recommendation (from opinion)
Tool	A tool to support security and privacy for m/uHealth

Quality Assessment and Analysis Focused on Evaluation Research:

Table 5: Security and Privacy Control Families Facet. For further details we refer the readers to the standard NIST 800-53 (draft rev5).

ID - Family	**ID - Family**
AC - Access Control	MP - Media Protection
AT - Awareness and Training	PA - Privacy Authorization
AU - Audit and Accountability	PE - Physical and Environmental Protection
CA - Assessment, Authorization, and Monitoring	PL - Planning
CM - Configuration Management	PM - Program Management
CP - Contingency Planning	PS - Personnel Security
IA - Identification and Authentication	RA - Risk Assessment
IP - Individual Participation	SA - System and Services Acquisition
IR - Incident Response	SC - System and Communications Protection
MA - Maintenance	SI - System and Information Integrity

Building on the initial SMS, an in-depth analysis was carried out focusing on the papers categorised as "Evaluation Research" in the research type facet. These are the publications describing technologies that were implemented in practice and an evaluation of the technique is conducted. This also includes evaluation of existing technologies on the market and identifying problems in industry. Evaluation studies were chosen because they comprise the most advanced stage of the research process. It is in the evaluation stage, when things are being implemented in the real world, that the bleeding-edge of technology reveals itself, allowing professionals to decide on the adoption (or rejection) of new solutions.

To that end, a thematic analysis was conducted to identify evaluation approaches reported in the literature, in which all papers were read in full and manually annotated. The thematic analysis method was chosen specially due the variety of research papers and distinct contributions types, eg, as pilot/feasibility studies, proposal of novel m/uHealth systems, security and privacy assessments and/or controls. Given that, the thematic analysis helped to identify, analyze and interpret patterns of meaning (or themes) within this set of papers. NVivo 12 software tool was used to facilitate the management of materials,

Table 6: Application Type Facet (based on the WHO Report [5]).

Category and description
Health call centers/Health care telephone help line: delivery of triage services and health care advice by trained professionals, by means of telephones.
Emergency toll-free telephone services: often used for quick access to health professionals or staff trained to provide guidance during medical emergencies.
Public health emergencies: can be defined as the use of mobile devices to respond to emergency and disaster situations, such as natural disasters and disease outbreaks.
Mobile telemedicine: can be defined as the use of a mobile device's functions (e.g., voice, text, data, imaging, or video) for different situations, such as communication between health professionals for consultation about patients or management of chronic patients living at home.
Appointment reminders: comprise services that rely on voice or SMS (Short Message Service) messages sent to patients, e.g., for scheduling consultations, delivering treatment results, or broadcasting immunisation reminders.
Community mobilisation & health promotion: defined as the use of text messaging for health promotion or to alert target groups of health campaigns.
Treatment compliance: can be described as the delivery of reminder messages, by voice or SMS, aiming to improve treatment compliance, disease eradication, and overcoming challenges such as resistance to taking the required drugs.
Patient records: the use of mobile devices to support the treatment of patients, including collecting and displaying patient records, eg, mobile apps that enable access to electronic medical records (EMRs) at the point-of-care.
Information initiatives: comprises services that provide access to health science publications or databases at the point-of-care, by means of portable devices.
Patient monitoring: defined as using technology to manage, monitor, and treat a patients illness from a distance (eg, diabetes or cardiac conditions). Remote sensors installed in households or imaging devices linked to mobile phones are often used to facilitate data transmission.
Health surveys: consists in the use of mobile devices for collecting and reporting health-related data.
Surveillance: defined as the use of mobile devices for inputting and transmitting data that will be used by surveillance programs to track diseases.
Awareness raising: includes the use of health information products, games, or quiz programs to educate people on relevant health topics such as HIV/AIDS.
Decision support systems: defined as software algorithms that help health providers to make their clinical diagnoses at point-of-care or health managers to take actions based on data gathered from health surveys.

Table 7: Used Technology Facet (based on our keywording classification).

Device-based	**System-based**
Mobile phones, also including personal digital assistants or handheld PCs	Short Message Service (SMS) and other messaging services
Tablets, mobile computer operated by touching the screen	Ambient intelligence, domotics & smart homes
Sensors, Internet of Things & fog computing	Mobile Cloud Computing
Wearable devices incorporated into clothing or worn on the body	Block chain, list of records resistant to modification of the data
Medical devices & Implantable medical devices	

memos and code annotations.

It is worth noting that security and privacy are emphasised in this second-stage analysis, seeking to identify clear evidences of evaluation (or lack thereof) of the security and privacy controls, claimed to be part of the m/uHealth solutions. Apart from that, we also performed a quality assessment for each paper, based on the criteria proposed in [6]. A summary of the quality assessment criteria for these papers is presented in Table 8.

2.3. Phase III – Documenting the Mapping Study

As per Figure 1, the last phase of the SMS, i.e., **Documenting the Mapping Study** is detailed in the remainder of this paper. Results documentation is based on investigating the RQs (in Section 2.1) and presenting their findings. Results documentation is classified as (a) *Research Demography and Mapping* and (b) *Research Solution and their Evaluations*. After presenting the results, Threats to Validity of Research are discussed. The artefacts used and created in this study are publicly available in a replication package. This package can be accessed at [7]. It includes the database search queries, the answer sets of these queries, and the maps of categorised papers and patterns.

Table 8: Quality criteria used in the second-stage analysis (from [6]).

1. Is the paper based on research (or is it merely a "lessons learned" report based on expert opinion)?
2. Is there a clear statement of the aims of the research?
3. Is there an adequate description of the context in which the research was carried out?
4. Was the research design appropriate to address the aims of the research?
5. Was the recruitment strategy appropriate to the aims of the research?
6. Was there a control group with which to compare treatments?
7. Was the data collected in a way that addressed the research issue?
8. Was the data analysis sufficiently rigorous?
9. Has the relationship between researcher and participants been considered to an adequate degree?
10. Is there a clear statement of findings?
11. Is the study of value for research or practice?

References

[1] K. Petersen, R. Feldt, S. Mujtaba, M. Mattsson, Systematic mapping studies in software engineering., in: 12th International Conference on Evaluation and Assessment in Software Engineering, Bari, Italy, 2008.

[2] R. Wieringa, N. Maiden, N. Mead, C. Rolland, Requirements engineering paper classification and evaluation criteria: a proposal and a discussion, Requirements Engineering 11 (1) (2006) 102–107. doi:10.1007/s00766-005-0021-6.
URL https://doi.org/10.1007/s00766-005-0021-6

[3] M. Kuhrmann, P. Diebold, J. Münch, Software process improvement: a systematic mapping study on the state of the art, PeerJ Computer Science 2 (2016) e62.

[4] M. Shaw, Writing good software engineering research papers, in: 25th International Conference on Software Engineering, 2003. Proceedings., 2003, pp. 726–736. doi:10.1109/ICSE.2003.1201262.

[5] WHO, mhealth: New horizons for health through mobile technologies: second global survey on ehealth (2011).

[6] T. Dybå, T. Dingsøyr, Empirical studies of agile software development: A systematic review, Information and Software Technology 50 (9) (2008) 833 – 859. doi:https://doi.org/10.1016/j.infsof.2008.01.006.
URL http://www.sciencedirect.com/science/article/pii/S0950584908000256

[7] Replication package (2020).
URL https://github.com/lhiwaya/SMS-SecPri-mHealth-uHealth

Appendix A. Complete list of primary studies

[P1] A privacy protection for an mHealth messaging system. 2015.

[P2] OWASP inspired mobile security. 2015.

[P3] Watermarking of Parkinson disease speech in cloud-based healthcare framework. 2015.

[P4] CPLM: Cloud facilitated privacy shielding leakage resilient mobile health monitoring. 2015.

[P5] Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges. 2015.

[P6] Systematic information flow control in mHealth systems. 2015.

[P7] RSA-DABE: A novel approach for secure health data sharing in ubiquitous computing environment. 2015.

[P8] Security and privacy issues in implantable medical devices: A comprehensive survey. 2015.

[P9] Security aspects of cloud based mobile health care application. 2015.

[P10] Power consumption aware software architecture for M-health applications with adaptive security of network protocols. 2015.

[P11] Securing XML with role-based access control: Case study in health care. 2015.

[P12] Reducing energy consumption of mobile phones during data transmission and encryption for wireless body area network applications. 2015.

[P13] Secure M-health patient monitoring and emergency alert system framework. 2015.

[P14] Privacy issues and techniques in e-health systems. 2015.

[P15] Verifiable privacy-preserving monitoring for cloud-assisted mHealth systems. 2015.

[P16] A Lightweight Encryption Scheme Combined with Trust Management for Privacy-Preserving in Body Sensor Networks. 2015.

[P17] Secu Wear: An Open Source, Multi-component Hardware/Software Platform for Exploring Wearable Security. 2015.

[P18] Lightweight and privacy-preserving agent data transmission for mobile Healthcare. 2015.

[P19] EPPS: Efficient and privacy-preserving personal health information sharing in mobile healthcare social networks. 2015.

[P20] MHealth through quantified-self: A user study. 2015.

[P21] Novel key management for secure information of ubiquitous healthcare domains to APT attack. 2015.

[P22] Security of personal bio data in mobile health applications for the elderly. 2015.

[P23] Security testing for Android mHealth apps. 2015.

[P24] On the privacy, security and safety of blood pressure and diabetes apps. 2015.

[P25] Service intelligence and communication security for ambient assisted living. 2015.

[P26] Privacy-preserving mobile access to Personal Health Records through Google's Android. 2015.

[P27] Legal, Regulatory, and Risk Management Issues in the Use of Technology to Deliver Mental Health Care. 2015.

[P28] Privacy preserving classification of ECG signals in mobile e-health applications. 2015.

[P29] An Elliptic Curve Cryptography-Based RFID Authentication Securing E-Health System. 2015.

[P30] An effective and secure user authentication and key agreement scheme in m-healthcare systems. 2015.

[P31] Recommendation-based trust management in body area networks for mobile healthcare. 2015.

[P32] Privacy and Security in Mobile Health Apps: A Review and Recommendations. 2015.

[P33] Exploring mobile health in a private online social network. 2015.

[P34] Too Much Information: Visual Research Ethics in the Age of Wearable Cameras. 2015.

[P35] Health Care Providers' Perspectives on a Weekly Text-Messaging Intervention to Engage HIV-Positive Persons in Care (WelTel BC1). 2015.

[P36] Development of mHealth system for supporting self-management and remote consultation of skincare eHealth/ telehealth/ mobile health systems. 2015.

[P37] BlinkToSCoAP: An end-to-end security framework for the Internet of Things. 2015.

[P38] A Taxonomy of mHealth apps - Security and privacy concerns. 2015.

[P39] Designing for scalability and trustworthiness in mHealth systems. 2015.

[P40] An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks Using RelAODV. 2015.

[P41] 'The phone reminder is important, but will others get to know about my illness?' Patient perceptions of an mHealth antiretroviral treatment support intervention in the HIVIND trial in South India. 2015.

[P42] Citizen Science on Your Smartphone: An ELSI Research Agenda. 2015.

[P43] A novel decentralized trust evaluation model for secure mobile healthcare systems. 2015.

[P44] Polynomial based light weight security in wireless body area network. 2015.

[P45] SmartHealth-NDNoT: Named data network of things for healthcare services. 2015.

[P46] Trust, Perceived Risk, Perceived Ease of Use and Perceived Usefulness as Factors Related to mHealth Technology Use. 2015.

[P47] A review and comparative analysis of security risks and safety measures of mobile health apps. 2015.

[P48] How trustworthy are apps for maternal and child health?. 2015.

[P49] On using a von neumann extractor in heart-beat-based security. 2015.

[P50] Know your audience: Predictors of success for a patient-centered texting app to augment linkage to HIV care in rural Uganda. 2015.

[P51] SecourHealth: A delay-tolerant security framework for mobile health data collection. 2015.

[P52] Availability and quality of mobile health app privacy policies. 2015.

[P53] An open-access mobile compatible electronic patient register for rheumatic heart disease ('eRegister') based on the World Heart Federation's framework for patient registers. 2015.

[P54] Mobile early detection and connected intervention to coproduce better care in severe mental illness. 2015.

[P55] 'Trust but verify' - five approaches to ensure safe medical apps. 2015.

[P56] A framework for secured collaboration in mHealth. 2015.

[P57] Security and privacy for mobile healthcare networks: From a quality of protection perspective. 2015.

[P58] Security and privacy framework for ubiquitous healthcare IoT devices. 2016.

[P59] Security in Cloud-Computing-Based Mobile Health. 2016.

[P60] Mobile health (m-Health) system in the context of IoT. 2016.

[P61] A Telemonitoring Framework for Android Devices. 2016.

[P62] Real-Time Tele-Monitoring of Patients with Chronic Heart-Failure Using a Smartphone: Lessons Learned. 2016.

[P63] Mobile admittance of health information with privacy and analysis in telemedicine. 2016.

[P64] Preserving patient's anonymity for mobile healthcare system in IoT environment. 2016.

[P65] Patient monitoring system for cardiovascular disease based on smart mobile healthcare environments. 2016.

[P66] A trust-based framework for information sharing between mobile health care applications. 2016.

[P67] An information privacy risk index for mHealth apps. 2016.

[P68] Realising the technological promise of smartphones in addiction research and treatment: An ethical review. 2016.

[P69] PMHM: Privacy in Mobile Health Monitoring using identity based encryption for mHealth: A Paper for mHealth systems. 2016.

[P70] Improving security in portable medical devices and mobile health care system using trust. 2016.

[P71] A smart health application and its related privacy issues. 2016.

[P72] An efficient MAC-based scheme against pollution attacks in XOR network coding-enabled WBANs for remote patient monitoring systems. 2016.

[P73] Flexible authentication protocol with key reconstruction in WBAN environments. 2016.

[P74] On the security of "verifiable privacy-preserving monitoring for cloud-assisted mhealth systems". 2016.

[P75] Private Data Analytics on Biomedical Sensing Data via Distributed Computation. 2016.

[P76] Privacy-preserving mhealth data release with pattern consistency. 2016.

[P77] Efficient attribute-based secure data sharing with hidden policies and traceability in mobile health networks. 2016.

[P78] A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth. 2016.

[P79] Ethical guidelines for mobile app development within health and mental health fields. 2016.

[P80] Authentication and key relay in medical cyber-physical systems. 2016.

[P81] The extent to which the POPI act makes provision for patient privacy in mobile personal health record systems. 2016.

[P82] An approach to automate health monitoring in compliance with personal privacy. 2016.

[P83] An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud. 2016.

[P84] Providing security and fault tolerance in P2P connections between clouds for mHealth services. 2016.

[P85] Assessing pairing and data exchange mechanism security in the wearable internet of things. 2016.

[P86] Security enhancement on an authentication scheme for privacy preservation in Ubiquitous Healthcare System. 2016.

[P87] Attribute-based traceable anonymous proxy signature strategy for mobile healthcare. 2016.

[P88] Open source based privacy-proxy to restrain connectivity of mobile apps. 2016.

[P89] Analyzing privacy risks of mhealth applications. 2016.

[P90] Simulation environment for testing security and privacy of mobile health apps. 2016.

[P91] Security Recommendations for mHealth Apps: Elaboration of a Developer's Guide. 2016.

[P92] Integration of smart wearable mobile devices and cloud computing in South African healthcare. 2016.

[P93] Power attack: An emerging threat in health-care applications using medical body area networks. 2016.

[P94] Secure and privacy preserving mobile healthcare data exchange using cloud service. 2016.

[P95] Privacy challenges and goals in mHealth systems. 2016.

[P96] Efficient data integrity auditing for storage security in mobile health cloud. 2016.

[P97] Analysis of ISO/IEEE 11073 built-in security and its potential IHE-based extensibility. 2016.

[P98] Privacy, Trust and Security in Two-Sided Markets. 2016.

[P99] Georeferenced and secure mobile health system for large scale data collection in primary care. 2016.

[P100] Resolving conflicting privacy policies in M-health based on prioritization. 2016.

[P101] mSieve: Differential behavioral privacy in time series of mobile sensor data. 2016.

[P102] Mutual authentication protocol for secure NFC based mobile healthcard. 2016.

[P103] A spatio-situation-based access control model for dynamic permission on mobile applications. 2016.

[P104] Harnessing teams and technology to improve outcomes in infants with single ventricle. 2016.

[P105] Improved population health surveillance and chronic disease management using secure email: Application of the DIRECT, IEEE 11073, HITSP, and IHE standards and protocols. 2016.

[P106] Lightweight and confidential data aggregation in healthcare wireless sensor networks. 2016.

[P107] Secure candy castle - A prototype for privacy-aware mHealth apps. 2016.

[P108] Security analysis of the IEEE 802.15.6 standard. 2016.

[P109] Context-aware, knowledge-intensive, and patient-centric Mobile Health Care Model. 2016.

[P110] Analysis of Security Protocols for Mobile Healthcare. 2016.

[P111] The introduction and evaluation of mobile devices to improve access to patient records: A catalyst for innovation and collaboration. 2016.

[P112] U-prove based security framework for mobile device authentication in eHealth networks. 2016.

[P113] Sharing mHealth data via named data networking. 2016.

[P114] A Secure System for Pervasive Social Network-Based Healthcare. 2016.

[P115] On the Deployment of Healthcare Applications over Fog Computing Infrastructure. 2017.

[P116] Information classification scheme for next generation access control models in mobile patient-centered care systems. 2017.

[P117] Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks. 2017.

[P118] Mapping Security Requirements of Mobile Health Systems into Software Development Lifecycle. 2017.

[P119] Exploring the usability, security and privacy taxonomy for mobile health applications. 2017.

[P120] An access control framework for secure and interoperable cloud computing applied to the healthcare domain. 2017.

[P121] A provably secure RFID authentication protocol based on elliptic curve signature with message recovery suitable for m-Health environments. 2017.

[P122] New watermarking/encryption method for medical images full protection in m-Health. 2017.

[P123] Smartphone application for medical images secured exchange based on encryption using the matrix product and the exclusive addition. 2017.

[P124] Towards secure and flexible EHR sharing in mobile health cloud under static assumptions. 2017.

[P125] A compressive multi-kernel method for privacy-preserving machine learning. 2017.

[P126] Managing secure personal mobile health information. 2017.

[P127] Security analysis of a mHealth app in Android: Problems and solutions. 2017.

[P128] Anonymity-preserving methods for client-side filtering in position-based collaboration approaches. 2017.

[P129] Smartphones to access to patient data in hospital settings: Authentication solutions for shared devices. 2017.

[P130] An authentication scheme for wireless healthcare monitoring sensor network. 2017.

[P131] Improving the information security of personal electronic health records to protect a patient's health information. 2017.

[P132] A secure framework for mHealth data analytics with visualization. 2017.

[P133] A proposal to improve the authentication process in m-health environments. 2017.

[P134] Feasibility of a secure wireless sensing smartwatch application for the self-management of pediatric asthma. 2017.

[P135] Smartphone-based continuous blood pressure monitoring application-robust security and privacy framework. 2017.

[P136] Security of ePrescriptions: Data in transit comparison using existing and mobile device services. 2017.

[P137] Efficient privacy-preserving dot-product computation for mobile big data. 2017.

[P138] A privacy-preserving data sharing solution for mobile healthcare. 2017.

[P139] Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System. 2017.

[P140] Secure and Privacy-Preserving Data Sharing and Collaboration in Mobile Healthcare Social Networks of Smart Cities. 2017.

[P141] Preserving patients' privacy in health scenarios through a multicontext-aware system. 2017.

[P142] Efficient end-to-end authentication protocol for wearable health monitoring systems. 2017.

[P143] Exploring the need for a suitable privacy framework for mHealth when managing chronic diseases. 2017.

[P144] Lightweight trusted authentication protocol for Wireless Sensor Network in e-Health. 2017.

[P145] Security and privacy requirements engineering for human centric IoT systems using eFRIEND and Isabelle. 2017.

[P146] The t2rol access control model for mobile health systems in developing countries. 2017.

[P147] Privacy Requirements for mobile e-Service in the Health Authority-Abu Dhabi (HAAD). 2017.

[P148] Protection against wormhole attack using smart protocol in MANET. 2017.

[P149] Cybersecurity of Wearable Devices: An Experimental Analysis and a Vulnerability Assessment Method. 2017.

[P150] Trusted sensor signal protection for confidential point-of-care medical diagnostic 2017.

[P151] Effective? Engaging? secure? applying the orcha-24 framework to evaluate apps for chronic insomnia disorder. 2017.

[P152] Development of a web-based epidemiological surveillance system with health system response for improving maternal and newborn health: Field-testing in Thailand. 2017.

[P153] Protecting mobile health records in cloud computing: A secure, efficient, and anonymous design. 2017.

[P154] A collaborative privacy-preserving deep learning system in distributed mobile environment. 2017.

[P155] Secure authentication and Prescription Safety Protocol for telecare health services using ubiquitous IoT. 2017.

[P156] Developing countries and Internet-of-Everything (IoE). 2017.

[P157] A Privacy-Preserving Multi-Authority Attribute-Based Encryption Approach for Mobile Healthcare. 2017.

[P158] PlaIMoS: A remote mobile healthcare platform to monitor cardiovascular and respiratory variables. 2017.

[P159] SoTRAACE - Socio-technical risk-adaptable access control model. 2017.

[P160] Pseudonym-based privacy protection for Steppy application. 2017.

[P161] My smart age with HIV: An innovative mobile and IoMT framework for patient's empowerment. 2017.

[P162] A survey on IoT applications, security challenges and counter measures. 2017.

[P163] Using Attribute-Based Access Control for Remote Healthcare Monitoring. 2017.

[P164] Accelerometer and Fuzzy Vault-Based Secure Group Key Generation and Sharing Protocol for Smart Wearables. 2017.

[P165] Patients' data management system protected by identity-based authentication and key exchange. 2017.

[P166] An Efficient Activity Recognition Framework: Toward Privacy-Sensitive Health Data Sensing. 2017.

[P167] Secure internet of things-based cloud framework to control zika virus outbreak. 2017.

[P168] Enhancing Heart-Beat-Based Security for mHealth Applications. 2017.

[P169] ABE based raspberry pi secure health sensor (SHS). 2017.

[P170] Review on communication security issues in iot medical devices. 2017.

[P171] A multimodal biometric identification method for mobile applications security. 2017.

[P172] Extended provisioning, security and analysis techniques for the ECHO health data management system. 2017.

[P173] Trustworthy access control for wireless body area networks. 2017.

[P174] Utilizing fully homomorphic encryption to implement secure medical computation in smart cities. 2017.

[P175] The new wave of privacy concerns in the wearable devices era. 2017.

[P176] Toward improving electrocardiogram (ECG) biometric verification using mobile sensors: A two-stage classifier approach. 2017.

[P177] A security framework for mobile health applications. 2017.

[P178] Optimized and Secured Transmission and Retrieval of Vital Signs from Remote Devices. 2017.

[P179] Soft real-time smartphone ECG processing. 2017.

[P180] An efficient secure communication for healthcare system using wearable devices. 2017.

[P181] Developing a comprehensive information security framework for mHealth: a detailed analysis. 2017.

[P182] Blockchain as an enabler for public mHealth solutions in South Africa. 2017.

[P183] Secure-EPCIS: Addressing Security Issues in EPCIS for IoT Applications. 2017.

[P184] The design of an m-Health monitoring system based on a cloud computing platform. 2017.

[P185] Lightweight Sharable and Traceable Secure Mobile Health System. 2017.

[P186] mHealth quality: A process to seal the qualified mobile health apps. 2017.

[P187] Scalable Role-Based Data Disclosure Control for the Internet of Things. 2017.

[P188] Context aware based user customized light therapy service using security framework. 2017.

[P189] Privacy-preserving design for emergency response scheduling system in medical social networks. 2017.

[P190] Distributed Big Data Analytics in Service Computing. 2017.

[P191] Light-Weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems. 2017.

[P192] DFP: A data fragment protection scheme for mhealth in wireless network. 2017.

[P193] Anonymous anti-sybil attack protocol for mobile healthcare networks analytics. 2017.

[P194] Towards privacy protection and malicious behavior traceability in smart health. 2017.

[P195] Attribute-based encryption with non-monotonic access structures supporting fine-grained attribute revocation in m-healthcare. 2017.

[P196] Secure framework for patient data transmission on mobile-cloud platform. 2018.

[P197] A Secure Crypto Base Authentication and Communication Suite in Wireless Body Area Network (WBAN) for IoT Applications. 2018.

[P198] Designing a secure architecture for m-health applications. 2018.

[P199] Towards an architecture to guarantee both data privacy and utility in the first phases of digital clinical trials. 2018.

[P200] A stochastic game for adaptive security in constrained wireless body area networks. 2018.

[P201] Context-aware authorization and anonymous authentication in wireless body area networks. 2018.

[P202] Game-Based Adaptive Remote Access VPN for IoT: Application to e-Health. 2018.

[P203] Spatially-resolved estimation of personal dosage of airborne particulates for ambulatory subjects using wearable sensors. 2018.

[P204] A Physical Layer Security Scheme for Mobile Health Cyber-Physical Systems. 2018.

[P205] Evaluating the Privacy Policies of Mobile Personal Health Records for Pregnancy Monitoring. 2018.

[P206] An efficient implementation of next generation access control for the mobile health cloud. 2018.

[P207] Secure sharing of mobile personal healthcare records using certificateless proxy re-encryption in cloud. 2018.

[P208] Quality of publicly available physical activity apps: Review and content analysis. 2018.

[P209] Using Mobile Phone Sensor Technology for Mental Health Research: Integrated Analysis to Identify Hidden Challenges and Potential Solutions. 2018.

[P210] Secured cloud computing for medical data based on watermarking and encryption. 2018.

[P211] Are mHealth Apps Secure? A Case Study. 2018.

[P212] Challenges and solutions implementing an SMS text message-based survey CASI and adherence reminders in an international biomedical HIV PrEP study (MTN 017). 2018.

[P213] Threat modeling for mobile health systems 2018.

[P214] RoFa: A Robust and Flexible Fine-Grained Access Control Scheme for Mobile Cloud and IoT based Medical Monitoring. 2018.

[P215] Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control. 2018.

[P216] A real-time, automated and privacy-preserving mobile emergency-medical-service network for informing the closest rescuer to rapidly support mobile-emergency-call victims. 2018.

[P217] A Simple Approach for Securing IoT Data Transmitted over Multi-RATs. 2018.

[P218] On the cybersecurity of m-Health IoT systems with LED bitslice implementation. 2018.

[P219] mHealth applications for goal management training - Privacy engineering in neuropsychological studies. 2018.

[P220] A Secured Smartphone-Based Architecture for Prolonged Monitoring of Neurological Gait. 2018.

[P221] A patient-held smartcard with a unique identifier and an mhealth platform to improve the availability of prenatal test results in rural Nigeria: Demonstration study. 2018.

[P222] Using mobile location data in biomedical research while preserving privacy. 2018.

[P223] Evaluating authentication options for mobile health applications in younger and older adults. 2018.

[P224] Comparative analysis between different facial authentication tools for assessing their integration in m-health mobile applications. 2018.

[P225] A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network. 2018.

[P226] Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing. 2018.

[P227] Privacy preserved spectral analysis using iot mhealth biomedical data for stress estimation. 2018.

[P228] A security framework for mHealth apps on Android platform. 2018.

[P229] Assessing the privacy of mhealth apps for self-tracking: Heuristic evaluation approach. 2018.

[P230] Skin care management support system based on cloud computing. 2018.

[P231] Toward privacy-preserving symptoms matching in SDN-based mobile healthcare social networks. 2018.

[P232] Securing Medical Images for Mobile Health Systems Using a Combined Approach of Encryption and Steganography. 2018.

[P233] Toward privacy in IoT mobile devices for activity recognition. 2018.

[P234] New Engineering Method for the Risk Assessment: Case Study Signal Jamming of the M-Health Networks. 2018.

[P235] Smart Chair-A Telemedicine Based Health Monitoring System. 2018.

[P236] Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. 2018.

[P237] Cost-Effective and Anonymous Access Control for Wireless Body Area Networks. 2018.

[P238] Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors. 2018.

[P239] Towards blockchain empowered trusted and accountable data sharing and collaboration in mobile healthcare applications. 2018.

[P240] ETAP: Energy-Efficient and Traceable Authentication Protocol in Mobile Medical Cloud Architecture. 2018.

[P241] Secure and efficient querying over personal health records in cloud computing. 2018.

[P242] Attribute-based handshake protocol for mobile healthcare social networks. 2018.

[P243] A traceable threshold attribute-based signcryption for mHealthcare social network. 2018.

[P244] Efficient Fine-Grained Data Sharing Mechanism for Electronic Medical Record Systems with Mobile Devices. 2018.

[P245] Certificateless searchable public key encryption scheme for mobile healthcare system. 2018.

[P246] A vulnerability study of Mhealth chronic disease management (CDM) applications (apps). 2018.

[P247] A design thinking approach to implementing an android biometric unique identification system for infant treatment follow-up in a resource limited setting. 2018.

[P248] My Smart Remote: A Smart Home Management Solution for Children. 2018.

[P249] Detecting insider attacks in medical cyber-physical networks based on behavioral profiling. 2018.

[P250] Privacy Issues in Smartphone Applications: An Analysis of Headache/Migraine Applications. 2018.

[P251] An authentication protocol for smartphone integrated Ambient Assisted Living system. 2018.

[P252] Secure and lightweight remote patient authentication scheme with biometric inputs for mobile healthcare environments. 2018.

[P253] Real-Time Remote Health Monitoring Systems Using Body Sensor Information and Finger Vein Biometric Verification: A Multi-Layer Systematic Review. 2018.

[P254] OpSecure: A secure unidirectional optical channel for implantable medical devices. 2018.

[P255] Translating GDPR into the mHealth Practice. 2018.

[P256] Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. 2018.

[P257] HR-auth: Heart rate data authentication using consumer wearables. 2018.

[P258] Privacy Issues and Solutions for Consumer Wearables. 2018.

[P259] An Improved Asymmetric Key Based Security Architecture for WSN. 2018.

[P260] Spatial Blockchain-Based Secure Mass Screening Framework for Children with Dyslexia. 2018.

[P261] Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. 2018.

[P262] A service oriented healthcare architecture (SOHA-CC) based on cloud computing. 2018.

[P263] Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things. 2018.

[P264] Implementation of cloud-assisted secure data transmission in WBAN for healthcare monitoring. 2018.

[P265] Dynamic Connectivity Establishment and Cooperative Scheduling for QoS-Aware Wireless Body Area Networks. 2018.

[P266] SMEAD: A secured mobile enabled assisting device for diabetics monitoring. 2018.

[P267] How could commercial terms of use and privacy policies undermine informed consent in the age of mobile health?. 2018.

[P268] Assessment criteria for parents to determine the trustworthiness of maternal and child health apps: a pilot study. 2018.

[P269] Attacks on heartbeat-based security using remote photoplethysmography. 2018.

[P270] ECG-Based Secure Healthcare Monitoring System in Body Area Networks. 2018.

[P271] A public-key protection scheme using in the wireless module of the digital stethoscope. 2018.

[P272] Centralized Fog Computing security platform for IoT and cloud in healthcare system. 2018.

[P273] FoG assisted secure De-duplicated data dissemination in smart healthcare IoT. 2018.

[P274] A cyber-physical approach to trustworthy operation of health monitoring systems. 2018.

[P275] Tiger hash based AdaBoost machine learning classifier for secured multicasting in mobile healthcare system. 2018.

[P276] ACMHS: Efficient access control for mobile health care system. 2018.

[P277] P3ASC: Privacy-preserving pseudonym and attribute-based signcryption scheme for cloud-based mobile healthcare system. 2018.

[P278] Identity-Based Fast Authentication Scheme for Smart Mobile Devices in Body Area Networks. 2018.

[P279] Enabling efficient and privacy-preserving health query over outsourced cloud. 2018.

[P280] EPSMD: An Efficient Privacy-Preserving Sensor Data Monitoring and Online Diagnosis System. 2018.

[P281] Development of a just-in-time adaptive mhealth intervention for insomnia: Usability study. 2018.

[P282] A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. 2018.

[P283] Securing mobile healthcare data: A smart card based cancelable Finger-Vein Bio-Cryptosystem. 2018.

[P284] Big Data and IoT for U-healthcare security. 2018.

[P285] An evolutionary game-theoretic approach for assessing privacy protection in mHealth systems. 2018.

[P286] Fusing identity management, HL7 and blockchain into a global healthcare record sharing architecture. 2019.

[P287] Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems. 2019.

[P288] Security vulnerabilities in mobile health applications. 2019.

[P289] Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. 2019.

[P290] The development of an Arabic weight-loss app akser waznk: Qualitative results. 2019.

[P291] Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications. 2019.

[P292] Verifying a secure authentication protocol for IoT medical devices. 2019.

[P293] What data are smartphone users willing to share with researchers?: Designing and evaluating a privacy model for mobile data collection apps. 2019.

[P294] Privacy in mobile health applications for breast cancer patients. 2019.

[P295] Secure application for health monitoring. 2019.

[P296] A multivariant secure framework for smart mobile health application. 2019.

[P297] A secure framework for IoT-based healthcare system. 2019.

[P298] Study of out-of-hospital access to his system: A security perspective. 2019.

[P299] Collaborative and secure transmission of medical data applied to mobile healthcare. 2019.

[P300] A mobile phone app for bedside nursing care: Design and development using an adapted software development life cycle model. 2019.

[P301] WYZ: A pilot study protocol for designing and developing a mobile health application for engagement in HIV care and medication adherence in youth and young adults living with HIV 2019.

[P302] Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and iot based continuous glucose monitoring system for diabetes mellitus research and care. 2019.

[P303] MedCop: Verifiable computation for mobile healthcare system. 2019.

[P304] Reliable and secure data transfer in IoT networks. 2019.

[P305] Secure sharing of mHealth data streams through cryptographically-enforced access control. 2019.

[P306] Privacy-preserving voice-based search over mHealth data. 2019.

[P307] Trustworthy Delegation Toward Securing Mobile Healthcare Cyber-Physical Systems. 2019.

[P308] Data security and raw data access of contemporary mobile sensor devices. 2019.

[P309] Review of security and privacy for the internet of medical things (IoMT): Resolving the protection concerns for the novel circular economy bioinformatics. 2019.

[P310] CAMPS: Efficient and privacy-preserving medical primary diagnosis over outsourced cloud. 2019.

[P311] Mobile health systems for community-based primary care: identifying controls and mitigating privacy threats. 2019.

[P312] E-consent for data privacy: Consent management for mobile health technologies in public health surveys and disease surveillance. 2019.

[P313] An access control framework for protecting personal electronic health records. 2019.

[P314] Detecting Suicidal Ideation with Data Protection in Online Communities. 2019.

[P315] A lightweight CLAS scheme with complete aggregation for healthcare mobile crowdsensing. 2019.

[P316] A multi-level data sensitivity model for mobile health data collection systems. 2019.

[P317] A review of privacy and usability issues in mobile health systems: Role of external factors. 2019.

[P318] A reversible and secure patient information hiding system for IoT driven e-health. 2019.

[P319] A secure mutual batch authentication scheme for patient data privacy preserving in WBAN. 2019.

[P320] Effective engagement of adolescent asthma patients with mobile health-supporting medication adherence. 2019.

[P321] Amulet: An open-source wrist-worn platform for mHealth research and education. 2019.

[P322] Secure IoT e-Health applications using VICINITY framework and GDPR guidelines. 2019.

[P323] A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. 2019.

[P324] MSCryptoNet: Multi-Scheme Privacy-Preserving Deep Learning in Cloud Computing. 2019.

[P325] PatientConcept App: Key Characteristics, Implementation, and its Potential Benefit. 2019.

[P326] Fine-grained multi-authority access control in IoT-enabled mHealth. 2019.

[P327] EdgeCare: Leveraging Edge Computing for Collaborative Data Management in Mobile Healthcare Systems. 2019.

[P328] Lightweight and Privacy-Preserving Medical Services Access for Healthcare Cloud. 2019.

[P329] An efficient anonymous authentication scheme based on double authentication preventing signature for mobile healthcare crowd sensing. 2019.

[P330] Development of a security layer in a mobile health system. 2019.

[P331] Server-Focused Security Assessment of Mobile Health Apps for Popular Mobile Platforms. 2019.

[P332]Security of an Electronic Heal Thcare System which Facilitates the Detection of Preeclampsia Through a Smart Bracelet. 2019.

[P333] Secure and scalable mhealth data management using blockchain combined with client hashchain: System design and validation. 2019.

[P334] Mobile apps for people with dementia: Are they compliant with the general data protection regulation (GDPR)?. 2019.

[P335] MHealth applications: Can user-adaptive visualization and context affect the perception of security and privacy?. 2019.

[P336] Eliciting design guidelines for privacy notifications in mHealth environments. 2019.

[P337] A Novel Privacy Framework for Secure M-Health Applications: The Case of the GDPR. 2019.

[P338] Group-Based Key Exchange for Medical IoT Device-to-Device Communication (D2D) Combining Secret Sharing and Physical Layer Key Exchange. 2019.

[P339] Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. 2019.

[P340] Needs analysis for a parenting app to prevent unintentional injury in newborn babies and toddlers: Focus group and survey study among Chinese caregivers. 2019.

[P341] Reviewing the data security and privacy policies of mobile apps for depression. 2019.

[P342] Achieving Mobile-Health Privacy Using Attribute-Based Access Control. 2019.

[P343] How private is your mental health app data? An empirical study of mental health app privacy policies and practices. 2019.

[P344] LISA: Visible light based initialization and SMS based authentication of constrained IoT devices. 2019.

[P345] Reliable Healthcare Monitoring System Using SPOC Framework. 2019.

[P346] RADAR-base: Open source mobile health platform for collecting, monitoring, and analyzing data using sensors, wearables, and mobile devices. 2019.

[P347] Availability, readability, and content of privacy policies and terms of agreements of mental health apps. 2019.

[P348] A secure mHealth application for attention deficit and hyperactivity disorder. 2019.

[P349] Technical guidance for clinicians interested in partnering with engineers in mobile health development and evaluation. 2019.

[P350] Lightweight and Secure Three-Factor Authentication Scheme for Remote Patient Monitoring Using On-Body Wireless Networks. 2019.

[P351] Sensor-Based mHealth Authentication for Real-Time Remote Healthcare Monitoring System: A Multilayer Systematic Review. 2019.

[P352] Towards a cooperative security system for mobile-health applications. 2019.

[P353] How to Realize Device Interoperability and Information Security in mHealth Applications. 2019.

[P354] End to end light weight mutual authentication scheme in IoT-based healthcare environment. 2019.

[P355] Robust secure communication protocol for smart healthcare system with FPGA implementation. 2019.

[P356] Flexible and efficient authenticated key agreement scheme for BANs based on physiological features. 2019.

[P357] Fog-Enabled Smart Health: Toward Cooperative and Secure Healthcare Service Provision. 2019.

[P358] How to use relevant data for maximal benefit with minimal risk: Digital health data governance to protect vulnerable populations in low-income and middle-income countries. 2019.

[P359] Achieve Privacy-Preserving Priority Classification on Patient Health Data in Remote eHealthcare System. 2019.

[P360] An efficient and privacy-Preserving pre-clinical guide scheme for mobile eHealthcare. 2019.

[P361] BYOD in Hospitals-Security Issues and Mitigation Strategies. 2019.

[P362] Why reviewing apps is not enough: Transparency for trust (T4T) principles of responsible health app marketplaces. 2019.

[P363] PDVocal: Towards privacy-preserving Parkinson's disease detection using non-speech body sounds. 2019.

[P364] An improved lightweight certificateless generalized signcryption scheme for mobile-health system. 2019.

[P365] Barriers to and facilitators of the use of mobile health apps from a security perspective: Mixed-methods study. 2019.

Appendix B. Evaluation Research list of relevant papers

[ER01] Security vulnerabilities in mobile health applications. 2019.

[ER02] The development of an Arabic weight-loss app akser waznk: Qualitative results. 2019.

[ER03] Real-Time Tele-Monitoring of Patients with Chronic Heart-Failure Using a Smartphone: Lessons Learned. 2016.

[ER04] Evaluating the Privacy Policies of Mobile Personal Health Records for Pregnancy Monitoring. 2018.

[ER05] What data are smartphone users willing to share with researchers?: Designing and evaluating a privacy model for mobile data collection apps. 2019.

[ER06] Privacy in mobile health applications for breast cancer patients. 2019.

[ER07] Quality of publicly available physical activity apps: Review and content analysis. 2018.

[ER08] Using Mobile Phone Sensor Technology for Mental Health Research: Integrated Analysis to Identify Hidden Challenges and Potential Solutions. 2018.

[ER09] Challenges and solutions implementing an SMS text message-based survey CASI and adherence reminders in an international biomedical HIV PrEP study (MTN 017). 2018.

[ER10] An information privacy risk index for mHealth apps. 2016.

[ER11] Security analysis of a mHealth app in Android: Problems and solutions. 2017.

[ER12] A mobile phone app for bedside nursing care: Design and development using an adapted software development life cycle model. 2019.

[ER13] WYZ: A pilot study protocol for designing and developing a mobile health application for engagement in HIV care and medication adherence in youth and young adults living with HIV. 2019.

[ER14] Comparative analysis between different facial authentication tools for assessing their integration in m-health mobile applications. 2018.

[ER15] Privacy-preserving mhealth data release with pattern consistency. 2016.

[ER16] Data security and raw data access of contemporary mobile sensor devices. 2019.

[ER17] Security of ePrescriptions: Data in transit comparison using existing and mobile device services. 2017.

[ER18] Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System. 2017.

[ER19] Assessing the privacy of mhealth apps for self-tracking: Heuristic evaluation approach. 2018.

[ER20] Security testing for Android mHealth apps. 2015.

[ER21] Effective engagement of adolescent asthma patients with mobile health-supporting medication adherence. 2019.

[ER22] PatientConcept App: Key Characteristics, Implementation, and its Potential Benefit. 2019.

[ER23] Cybersecurity of Wearable Devices: An Experimental Analysis and a Vulnerability Assessment Method. 2017.

[ER24] Effective? Engaging? secure? applying the orcha-24 framework to evaluate apps for chronic insomnia disorder. 2017.

[ER25] Development of a web-based epidemiological surveillance system with health system response for improving maternal and newborn health: Field-testing in Thailand. 2017.

[ER26] Assessing pairing and data exchange mechanism security in the wearable internet of things. 2016.

[ER27] A vulnerability study of Mhealth chronic disease management (CDM) applications (apps). 2018.

[ER28] Detecting insider attacks in medical cyber-physical networks based on behavioral profiling. 2018.

[ER29] Analyzing privacy risks of mhealth applications. 2016.

[ER30] Privacy Issues in Smartphone Applications: An Analysis of Headache/Migraine Applications. 2018.

[ER31] Mobile apps for people with dementia: Are they compliant with the general data protection regulation (GDPR)?. 2019.

[ER32] Health Care Providers' Perspectives on a Weekly Text-Messaging Intervention to Engage HIV-Positive Persons in Care (WelTel BC1). 2015.

[ER33] Server-Focused Security Assessment of Mobile Health Apps for Popular Mobile Platforms. 2019.

[ER34] Reviewing the data security and privacy policies of mobile apps for depression. 2019.

[ER35] My smart age with HIV: An innovative mobile and IoMT framework for patient's empowerment. 2017.

[ER36] Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. 2018.

[ER37] How private is your mental health app data? An empirical study of mental health app privacy policies and practices. 2019.

[ER38] RADAR-base: Open source mobile health platform for collecting, monitoring, and analyzing data using sensors, wearables, and mobile devices. 2019.

[ER39] Availability, readability, and content of privacy policies and terms of agreements of mental health apps. 2019.

[ER40] 'The phone reminder is important, but will others get to know about my illness?' Patient perceptions of an mHealth antiretroviral treatment support intervention in the HIVIND trial in South India. 2015.

[ER41] Georeferenced and secure mobile health system for large scale data collection in primary care. 2016.

[ER42] A review and comparative analysis of security risks and safety measures of mobile health apps. 2015.

[ER43] How trustworthy are apps for maternal and child health?. 2015.

[ER44] Attacks on heartbeat-based security using remote photoplethysmography. 2018.

[ER45] Harnessing teams and technology to improve outcomes in infants with single ventricle. 2016.

[ER46] Know your audience: Predictors of success for a patient-centered texting app to augment linkage to HIV care in rural Uganda. 2015.

[ER47] Availability and quality of mobile health app privacy policies. 2015.

[ER48] Security analysis of the IEEE 802.15.6 standard. 2016.

[ER49] An open-access mobile compatible electronic patient register for rheumatic heart disease ('eRegister') based on the World Heart Federation's framework for patient registers. 2015.

[ER50] Development of a just-in-time adaptive mhealth intervention for insomnia: Usability study. 2018.

[ER51] Mobile early detection and connected intervention to coproduce better care in severe mental illness. 2015.

[ER52] The introduction and evaluation of mobile devices to improve access to patient records: A catalyst for innovation and collaboration. 2016.