IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 6, 2019, accepted December 31, 2019, date of publication January 8, 2020, date of current version January 17, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2964988

Security in Telehealth Systems From a Software Engineering Viewpoint: A Systematic Mapping Study

GASTÓN MÁRQUEZ[1,3], HERNÁN ASTUDILLO[1,3], AND CARLA TARAMASCO[2,3]

[1]Departamento de Informática, Universidad Técnica Federico Santa María, Valparaíso 2520000, Chile
[2]Escuela de Ingeniería Civil Informática, Universidad de Valparaíso, Valparaíso 2520000, Chile
[3]Centro Nacional en Sistemas de Información en Salud (CENS), Área de Calidad, Santiago 8380000, Chile

Corresponding authors: Gastón Márquez (gaston.marquez@sansano.usm.cl) and Carla Taramasco (carla.taramasco@uv.cl)

This work was supported in part by the Comisión Nacional de Investigación Científica y Tecnológica (CONICYT-PCHA) Doctorado Nacional under Grant 2016-21161005, and in part by the Centro Nacional en Sistemas de Información en Salud (CENS).

ABSTRACT Telehealth systems deliver remote care of elderly and physically less able patients as well as remote surgeries, treatments, and diagnoses. In this regard, several systemic properties must be satisfied (such as security) in order to ensure the functionality of Telehealth systems. Although existing studies discuss different security episodes that involve Telehealth systems, it is difficult to have a clear standpoint about which are the most reported security issues and which solutions have been proposed. Furthermore, since Telehealth systems are composed of several software systems, it is not clear which critical areas of Software Engineering are relevant to develop secure Telehealth systems. This article reports a systematic mapping study (SMS) whose purpose is to detect, organize, and characterize security issues in Telehealth systems. Based on the SMS results, we examine how Software Engineering may help to develop secure Telehealth systems. From over a thousand studies, we distinguished and classified 41 primary studies. Results show that (i) four security classifications (*attacks*, *vulnerabilities*, *weaknesses*, and *threats*) concentrate the most reported security issues; (ii) three security strategies (*detect attacks*, *stop or mitigate attacks* and *react to attacks*) characterize security issues, and (iii) the most relevant research themes are related to insecure data transmission and privacy. The SMS's findings suggest that software design, requirements, and models are key areas to develop secure Telehealth systems.

INDEX TERMS Telehealth systems, security, software engineering, systematic mapping study.

I. INTRODUCTION

Telehealth systems are remote technology-based virtual platforms that promote (i) health care, (ii) public health, and (iii) health administration [1]. The term ''telehealth'' is frequently used to incorporate a more extensive definition of remote healthcare services, such as *telemedicine* and *telecare*. In this regard, telemedicine is the use of medical data exchanged from one site to another via electronic communications to enhance patients' health status [2]. At the same time, Telecare offers to care, help, and manage patient recovery via telecommunications technology, through synchronous (such as live video) or asynchronous mechanisms (such as store-and-forward, remote patient monitoring, and others) [3]. In this study, we involved Telemedicine and Telecare when we referred to Telehealth systems.

Since Telehealth systems are composed of software systems, these can include emerging technologies (such as robotics [4], mobile [5], the Internet of Things (IoT) [6], and others) to provide better remote services to their patients. This adoption brings many gains to patient care, but also leads to new challenges, such as security. Telehealth systems involve the communication of sensitive health data among health care providers and patients, which increases potential risks and threats on privacy and security. Although researchers have reported several security issues related to Telehealth systems, there is not a clear perception about which security issues Telehealth systems have faced. Furthermore, it is also not precise which solutions have been proposed for these issues, which limits the ability to structure knowledge to define clear and precise solutions to address security incidents. The previous situation can also be extended to software systems that support Telehealth systems; it is not explicit which Software Engineering areas are critical to developing secure Telehealth systems.

The associate editor coordinating the review of this manuscript and approving it for publication was Aakash Ahmad.

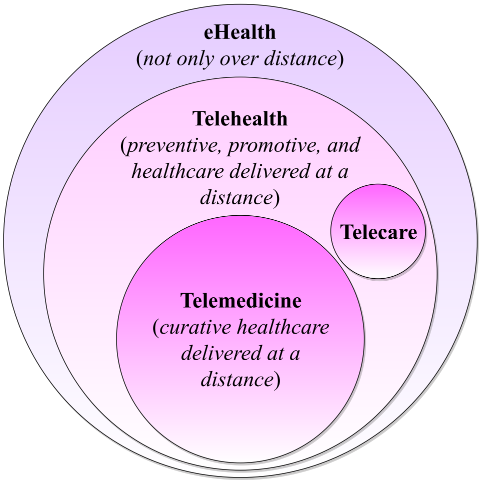

FIGURE 1. Conceptual framework of the relations between eHealth, Telehealth, Telecare and Telemedicine described in [9].

Some studies discuss the contribution of Software Engineering in different domains. For example, Sajjad *et al.* [7] conducted a systematic mapping study focused on adaptive security for mobile computing. The significant results obtained in this research concerning security and mobile devices bring to the fore the motivation to investigate how Software Engineering can help to satisfy security in other domains, such as Telehealth.

This article presents a **systematic mapping study** (SMS) aimed at detecting and categorizing security issues in Telehealth systems. From over a thousand studies, we selected 41 primary studies in order to discuss the role of Software Engineering to address potential security challenges on Telehealth systems.

The main **contribution** of our study is the analysis of how Software Engineering help to develop secure Telehealth systems.

This paper is organized as follows: Section II describes the background of our study; Section III details the systematic mapping protocol; Section IV shows the SMS results; Section V discusses the role of Software Engineering to address security concerns on Telehealth systems; Section VI describes the threats to the validity; Section VII details related work; and Section VIII draws concluding remarks.

II. BACKGROUND

Often, telemedicine and telecare are frequently confused with other terms included in the broad concept of eHealth, being even sometimes considered synonyms and most commonly used interchangeably [8] (see Figure 1). Nevertheless, despite their similarity, each one refers to a different way of using information and communication technologies to deliver healthcare services [9].

A. TELEHEALTH

Telehealth is the set of activities related to health, services, and methods, which are performed remotely with the help of communication technologies. The concept of telehealth usually includes telemedicine, telecare, tele-education, among others. Furthermore, includes organizational and/or procedural aspects of the conventional medical act (e.g., electronic medical record) as well as the extension to all areas of health, dentistry, nutrition, psychology, sports medicine, public health, nursing, and others [10].

B. TELEMEDICINE

According to the World Health Organization, telemedicine is the provision of health care services, where distance is a critical factor, for all health professionals who use information and communication technologies for the exchange of valid information for diagnosis, treatment, and prevention of diseases and injuries, research and evaluation, and for the continuing education of health care providers, for the promotion of the health of individuals and their communities [11].

C. TELECARE

Telecare is the use of telemedicine technology to provide care and practice nursing in order to improve the quality of care. Their advantages rely on the promotion of continuity care and self-management of the disease. It also helps people to understand their health and treatment problems better and improves therapeutic adherence. Furthermore, telecare improves the quality of nurse-patient communication allowing establishing a therapeutic relationship [12].

D. SOFTWARE ENGINEERING

Software engineering is the application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software [13]. Typically, Telehealth systems are surrounded by artifacts and electronic devices (such as servers, networks, routers, mobile devices, sensors, smartphones, medical equipment, and others), which are linked through software tools. This gradual union with other software systems produces the final architecture of Telehealth systems.

III. SYSTEMATIC STUDY DESIGN

The systematic study design is illustrated in Figure 2. In the following sections, we proceed to describe each activity of the SMS.

A. RESEARCH PROCESS

In order to conduct the SMS, we used the guidelines proposed by Petersen *et al.* [14] complemented with the strategies presented by Kitchenham and Charters [15] for performing systematic mapping studies and systematic literature reviews, respectively.

We also used the proposal of Watzlaf *et al.* [16], which describes a protocol for systematic reviews of Telehealth privacy and security research to complement our SMS.

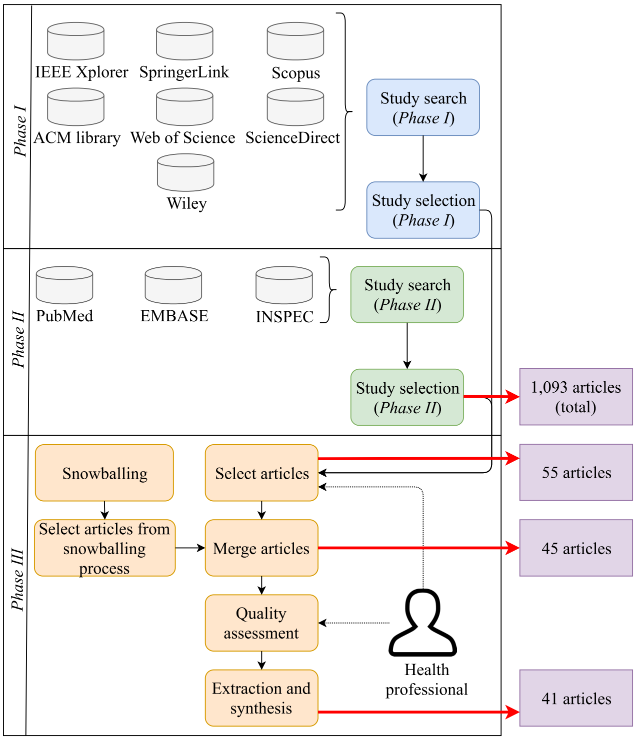

FIGURE 2. SMS process and results.

B. GOAL AND RESEARCH QUESTIONS

This SMS aims to *detect, organize and characterize security issues in Telehealth systems and analyze how Software Engineering can face these issues*. Therefore, we described the following research questions (RQ's).

- **RQ1**: *Which research themes characterize security in Telehealth systems?* Rationale: By answering this RQ, we aim at detecting those research themes that characterize primary studies in order to identify the main security problems that health institutions must face when using Telehealth systems.
- **RQ2**: *Which security issues have been published concerning Telehealth systems?* Rationale: This RQ studies which type of security issues (e.g., attacks, vulnerabilities, threats, among others) Telehealth systems have been faced. Moreover, this RQ aims to describe the Telehealth components as well as the medical supplies affected by security issues.
- **RQ3**: *Which security solutions have been proposed for Telehealth systems?* Rationale: This RQ aims to identify and categorize solutions used to manage security issues. We organized security solutions according to their security strategies.

The research questions will conduct the entire study, influencing the (i) search and selection of primary studies, (ii) data extraction, and (iii) data analysis.

C. RESEARCH EXECUTION

We decided to start the revision from 1997 because in that year, Makris *et al.* [17] published one of the first studies about security in Telemedicine systems. In this starting-point-article, the authors argue that telemedicine applications require robust security mechanisms to ensure medical data confidentiality and integrity. Subsequently, the end of the search period is January 2019.

We explored several databases in order to collect studies with different points of views (e.g., technical, medical, and others). To do this, we defined three phases, where the two first ones contain a set of different electronic databases. In sections III-D, III-E, and III-F, we further describe each phase.

To define the search string, we used the P.I.C.O.C (Population, Intervention, Comparison, Outcome, and Context) framework [18]. This framework helps researchers to connect the different parts of the research question towards a meaningful research string. Therefore, each element of the framework is broken down as follows:

- *Population*: Telehealth + Telemedicine + Telecare + systems
- *Intervention*: Approaches and methodologies related to security in Telehealth systems
- *Comparison*: Not applicable
- *Outcome*: Classification template with primary studies
- *Context*: Academic peer-reviewed articles

We combined each element with logical ANDs and ORs. Consequently, we defined the following search string:

((“telehealth” OR “tele health” OR “tele-health”) OR (“telemedicine” OR “tele medicine” OR “telemedicine”) OR (“telecare” OR “tele care” OR “tele-care”)) AND (“system” OR “application” OR “software”) AND (“security” OR “sec”)

It is essential to mention that in each database we adapt the search string. This means that the search string defined above may undergo slight changes in each database. However, these changes do not affect the results of our SMS.

D. PHASE I

As Kitchenham and Brereton [19] suggest, we explored the following electronic databases (see Figure 2). This set of databases provides the most significant number of studies that will be used in the selection criteria and data analysis.

E. PHASE II

In this phase, we explored databases mentioned in health-related SMS (such as [20] and [21]) (see Figure 2). These databases contain not only technical aspects regarding health (in general) but also clinical ones. This gives the possibility of having a more comprehensive observation about the focus of this SMS.

F. PHASE III

In this phase, we proceed to refine the selection of primary studies. That is to say, we applied selection criteria filters in order to, then, classify them. Subsequently, we analyzed the classified primary studies using a quality assessment. Finally, we proceed to extract the most relevant data.

1) SNOWBALLING PROCESS
To identify more relevant studies, we also executed the snowballing procedure according to the guidelines proposed in [22]. Snowball sampling is a non-probability (non-random) sampling method used when characteristics to be held by samples are rare and difficult to find. It is based on referrals from initial studies to generate additional studies. We performed both backward and forward snowballing (i.e., references, citations) procedures obtaining, finally, nine studies.

2) SELECTION CRITERIA
We defined the following inclusion and exclusion criteria:

- *Inclusion criteria*:
  - Studies related to Telehealth, Telemedicine or Telecare systems.
  - Studies whose primary focus is security issues on Telehealth systems.
  - Studies should provide solutions, techniques, methods or other procedure to handle security issues.
  - Studies should describe how security issues impact on Healthcare organizations and their people (patients, practitioners, administrative staff, and others)
  - Studies should be written in English.
- *Exclusion criteria*:
  - Short articles (less than 3 pages)
  - Studies without full text available
  - Studies structured as tutorial, editorials, and others

In this activity, we invited healthcare professionals to review and discuss the selection criteria; their experience and clinical vision will help to be logical and unbiased.

3) CLASSIFICATION
We classified primary studies based on the following classification scheme:

a: RESEARCH THEMES (RQ1)
We applied the approach proposed by Braun and Clarke [23] to identify main research themes concerning primary studies. Research themes are related to Thematic Analysis (TA), which is a method for systematically identifying, organizing, and offering insight into patterns of meaning (themes) (see Figure 3) and use them to address the research. TA is composed by six steps, which are:

1) *Familiarizing with the data*: In this step, the data is transcribed and read.
2) *Generating initial codes*: The goal of this step is to code relevant features of the data systematically across the entire data set, collating data pertinent to each code.
3) *Searching for themes*: In this step, codes are collated into potential themes, gathering all data relevant to each potential theme.

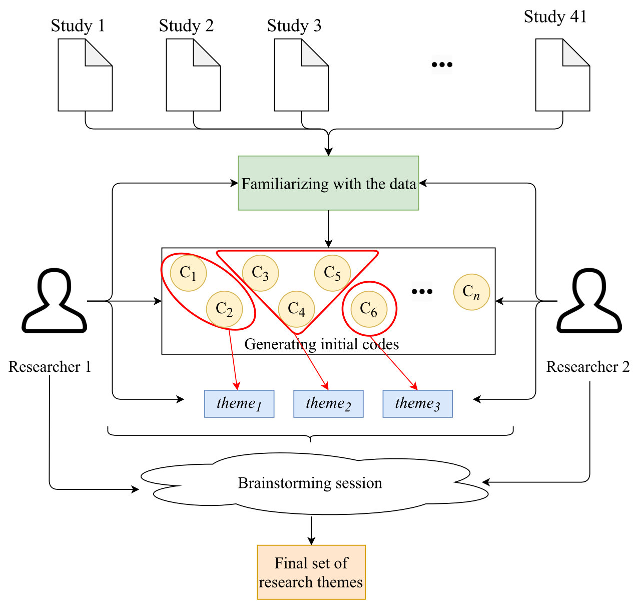

FIGURE 3. Research themes procedure executed in the SMS.

4) *Reviewing themes*: This step checks themes work in relation to the coded extracts and the entire data set, aiming at generating a thematic "map" of the analysis.
5) *Defining and naming themes*: Ongoing analysis to refine the specifics of each theme is conducted in this step, generating clear definitions and names for each theme.
6) *Producing the report*: This step corresponds to introspection. The last analysis is conducted in order to refine themes and characteristics.

Figure 3 describes the process for obtaining research themes. In this process, two researchers led the thematic analysis in order to reduce bias. In turn, brainstorming sessions were instrumental in validating and achieving meaningful results.

b: SECURITY ISSUES (RQ2)
In order to classify security issues, we used as reference the main topic that delineates the following well-known security-based databases: Common Vulnerabilities and Exposure (CVE) [24], Common Weaknesses Enumeration (CWE) [25], Common Attack Pattern Enumeration and Classification (CAPEC) [26], Vulnerability Notes [27], and National Vulnerability [28]. Hence, we classified security issues using the following categories:

- *Attacks*: Information security incident that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission.
- *Vulnerabilities*: Cyber-security term that refers to a flaw in a system that can leave it open to attack.
- *Threats*: Anything that has the potential to cause serious harm to a computer system.

- *Weaknesses*: Flaws, faults, bugs, and other errors in software implementation, code, design, or architecture that if left unaddressed could result in systems and networks being vulnerable to attack.

c: SOLUTIONS (RQ3)

Aiming at classifying security solutions reported by primary studies, we introduce the concept of *security strategies*. These strategies outline where the solutions described in the primary studies to mitigate security incidents are aimed. To define these strategies, we draw on the categories that classify *security tactics* [29]. These tactics are design decisions that enable security to be satisfied in different types of systems. Therefore, we define the following security strategies:

- *Detect attacks*: Solutions characterized by this strategy aim to identify potential attacks.
- *Stop or mitigate attacks*: This strategy intends to describe primary studies whose solutions aim to resist attacks.
- *React to attacks*: The goal of this strategy is to identify primary studies whose solutions attempt to respond to potential attacks.
- *Recover from attacks*: This strategy describes solutions that restore systems once it has detected and attempted to resist an attack.

G. QUALITY ASSESSMENT

In order to assess the primary studies' quality, we established quality criteria. As in Section III-F2, we also invited health professionals to this activity. Each quality criterion have the following values: Y (yes, *value* = 1), P (partially, *value* = 0, 5), and N (no, *value* = 0). As a result, we defined the following quality criteria:

- **QC1:** The primary study has a clear description of the aims of the research.
- **QC2:** The primary study includes research, practices or recommendations related to security.
- **QC3:** The primary study describes how security issues compromise Healthcare organizations.
- **QC4:** The primary study describes solutions to handle security issues in Telehealth systems

H. DATA EXTRACTION

Table 1 describes the data extraction scheme used in this SMS.

Data items I1 to I5 collect the primary data of each study. Regarding I6, this data item identifies the empirical strategies used by each primary study. For this, we used the Wohlin *et al.* [31] empirical organization to perform the aforementioned empirical identification. Subsequently, I7 classify the research type of each study. In this regard, we used the proposal of Wieringa *et al.* [30], which classify research type as follow:

TABLE 1. Data items to be extracted.

ID	Data item	Description	RQ
I1	Author(s)	The authors' full name	Demographics
I2	Title	The study's title	
I3	Year	Publication year	
I4	Venue	Name of the publishing venue	
I5	Publication type	Journal, conference, workshop, or book chapter	
I6	Validation type	Case study, experimental study, survey, empirical strategies comparison, replications, and others	
I7	Research classification	Classification criteria proposed by Wieringa et al. [30]	
I8	Research themes	Thematic analysis proposed by Braun et al. [23]	RQ1
I9	Security issues	Attacks, vulnerabilities, threats, and weaknesses	RQ2
I10	Solutions	Detect attacks, stop or mitigate attacks, react to attacks or recover from attacks	RQ3

- *Evaluation research*: Addresses the investigation of a problem in practice or implementation of a technique in practice.
- *Proposal of solution*: Proposes a solution technique and argue for its relevance, without a full-blown validation.
- *Validation research*: Investigates the properties of a solution proposal that has not yet been implemented in practice.
- *Philosophical papers*: Sketches a new way of looking at things, a new conceptual framework, etc.
- *Opinion papers*: Contains the author's opinion about what is wrong or good about something, how we should do something, etc.
- *Personal experience papers*: The emphasis is on what and not on why. The experience may concern one project or more, but it must be the author's personal experience.

Regarding data items I8, I9 and I10, the rationale of theses items were explained in Section III-F3.a, III-F3.b, and III-F3.c.

I. DATA ANALYSIS

The goal of this activity is to understand and to analyze security issues reported in Telehealth systems. For this purpose, we used descriptive statistics and frequency analysis. Furthermore, we tabulated data in order to obtain insight about primary studies. In addition, this analysis serves as a basis for discussing key findings among potential security challenges in Telehealth systems.

J. REPLICABILITY

We created a replication package[1] in order to replicate and validate our study. This package contains (i) the SMS protocol of our study (ii) and the description of each primary study.

IV. RESULTS

This section outlines the results concerning RQs. We found 41 primary studies from the SMS process (see Figure 2).

[1]https://doi.org/10.5281/zenodo.3547857

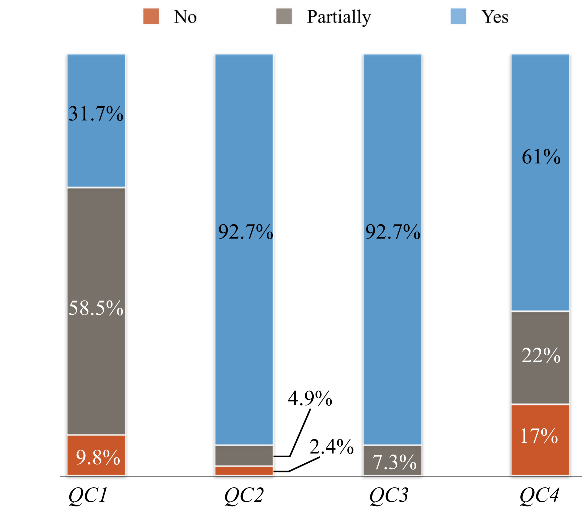

FIGURE 4. Quality assessment scores.

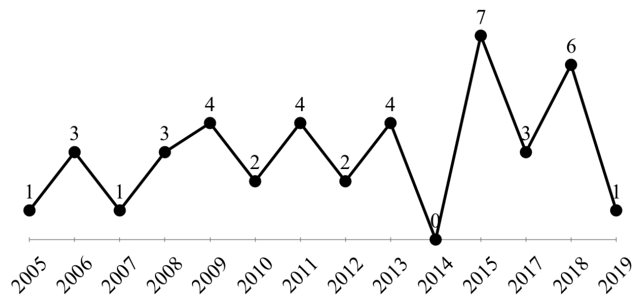

FIGURE 5. Publication years.

We detail each primary study in the Appendix section. We labeled each article using the letter "A".

Figure 4 illustrates the quality assessments results. Regarding QC1, almost 60% of primary studies partially describe the aims of the research. Although authors present significant results, they are not clear in defining which security goals they want to address. On the other hand, both in QC2 and QC3, authors clearly describe security recommendations and how security issues affect the environment where they conduct the research, respectively. Finally, QC4 illustrates more than 60% of primary studies describe procedures, techniques, or methods for handling security.

Figure 5 depicts the publication years. We found studies from 2005 to 2019. Since 2015, there is an expansion in publications, which afterward is kept during 2018 with a gap in 2014. Likewise, most publications focused on conferences and journals (see Figure 5).

Table 2 describes the distribution of primary studies per research classification. Almost half of primary studies (44%) propose solutions to security problems surrounding Telehealth systems. This demand arises from the need of Healthcare organizations to protect the assets of storage, access, and transmission of information related to the treatment and care of patients.

Subsequently, 29% of primary studies investigated new techniques that have not been implemented, such as

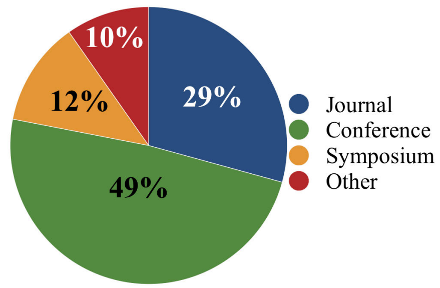

FIGURE 6. Publication venues.

TABLE 2. Research strategies results.

Research classification	Studies	%
Validation research	A1, A10, A13, A14, A15, A17, A20, A27, A28, A29, A30, A39	29%
Evaluation research	A7, A16, A23, A25, A26, A32, A34, A35, A37, A38, A40	27%
Proposal of solution	A2, A3, A4, A5, A6, A8, A9, A11, A12, A18, A19, A21, A22, A24, A31, A33, A36, A41	44%

robust encryption, security policies, biometric authentication, among others. This group of primary studies aims to propose novel techniques to expand the gamma of security solutions that can be used by Telehealth systems.

Another group of primary studies (27%) evaluate techniques and methods that are already implemented in practice. These primary studies conducted empirical studies to analyze the advantages and disadvantages of specific techniques and methods in Telehealth systems in the security context. From these analyzes, authors obtain relevant conclusions, such as the relationship between users and security mechanism, if very sophisticated security techniques can cause frustration in users, the need to use security filters for specific clinical processes, among other conclusions.

We do not identify primary studies that correspond to philosophical articles, opinion articles, or personal experience articles.

Regarding validation types, case studies (56%) are the trend as a validation method. Most articles conducted case studies to simulate or test the performance of their applications or solutions. Some, on the other hand, studied security scenarios where they test their proposals under controlled environments. 24% of primary studies do not describe what type of validation they used to analyze their proposals.

A. RQ1: RESEARCH THEMES

We identified seven research themes, which are: Insecure data transmission, Privacy, Interoperability, Trust, Integration, Security requirements and Risk management (see Figure 8 and Table 3). There were unanimous agreements in the first five due to the fact that primary studies, associated with these research topics, clearly describe the analysis and objectives of each investigation.

Nevertheless, regarding the two last ones (security requirements and risk management), it was necessary to argue the

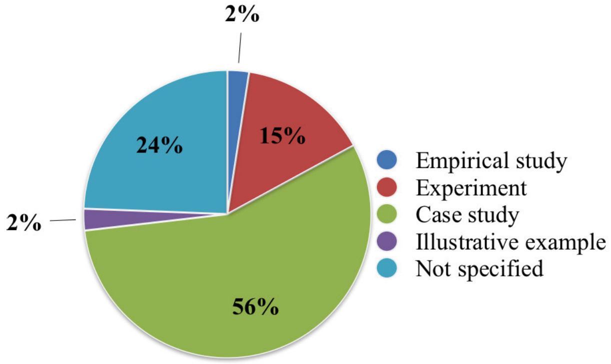

FIGURE 7. Primary studies' validation type.

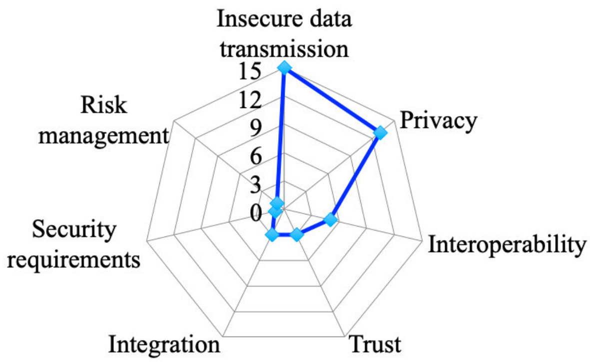

FIGURE 8. Research themes identified.

TABLE 3. Research themes and primary studies.

Research theme	Primary study
Insecure data transmission	A1, A4, A6, A10, A12, A18, A21, A23, A26, A31, A32, A34, A35, A36, A40
Privacy	A3, A5, A7, A9, A13, A14, A19, A22, A25, A29, A33, A38, A41
Interoperability	A8, A11, A16, A17, A39
Trust	A24, A28, A37
Integration	A2, A27, A30
Security requirements	A20
Risk management	A15

reason why they should be considered as research themes because there were little primary studies related to these research themes. Finally, after several brainstorming sessions, it was concluded that both research topics should be considered given their relevance in Software Engineering. In the following sections, we discussed the research themes thoroughly.

1) INSECURE DATA TRANSMISSION
37% of primary studies focus on investigating the context of insecure data transmission. This research theme discusses security issues when connecting Telehealth systems to a wireless router or access point to a computer or other mobile device. Telehealth systems must be especially careful concerning data transmission because the data transmitted is sensitive patient data. Primary studies remarks that it is necessary to protect all the network traffic data, such as medical records, stream data, and camera control messages via HTTPS connection. HTTPS protocols implements SSL/TLS to secure communication by encrypting the payloads of packets.

2) PRIVACY
Privacy is related to the personal life of each patient and must be maintained in an intimate and secret way. An individual has the right to have privacy in his life, that is, the person can perform actions, which he does not necessarily have to share with others [29]. 32% of primary studies are concerned about how to provide privacy in Telehealth systems. Mainly, primary studies investigate which security mechanisms are applied to telemedicine networks in order to guarantee the confidentiality, integrity, and availability of patients' medical information.

3) INTEROPERABILITY
According to [32], interoperability is the ability of two or more systems or components to exchange information and use the information that has been exchanged. Mainly, primary studies address interoperability between fog and cloud computing platforms by (i) proposing a framework for a standardized exchange of information between healthcare entities (ii) designing and implementing a software tool to be integrated into medical data dissemination protocols to ensure interoperability and (iii) evaluating the impact of the software tool on the transport of data when exchanging healthcare information using "in-band" and "out-band" transport over the IEEE802.15.4/ZigBee and WiFi protocols.

4) TRUST
Trust is the security or firm hope that someone has of another individual or something [33]. In this research theme, primary studies focused on PKI-like infrastructure for establishing trust between users using biometrics-based authentication and hierarchies of trust. Furthermore, other studies discuss the introduction of a unique identity-based authentication scheme and thus, eliminating the need for a third-party user in order to increase trust in mobile e-Health networks.

5) INTEGRATION
Systems integration is defined as the set of related or interacting elements that allow the implementation and attainment of policies and objectives of an organization, in terms of various aspects such as quality, environment, security, health, or other management disciplines [34]. Primary studies discuss how to build platforms to satisfy healthcare needs by integrating modules for telemedicine. In this context, medical processes are modeled following the HL7 Reference Information Model, which has allowed easy inclusion of many specialties such as dermatology, radiology, cardiology, pathology, and infection diseases, among others.

6) SECURITY REQUIREMENTS
Security requirements are statements made to make security assessments. According to ISO 27001 [35], the information

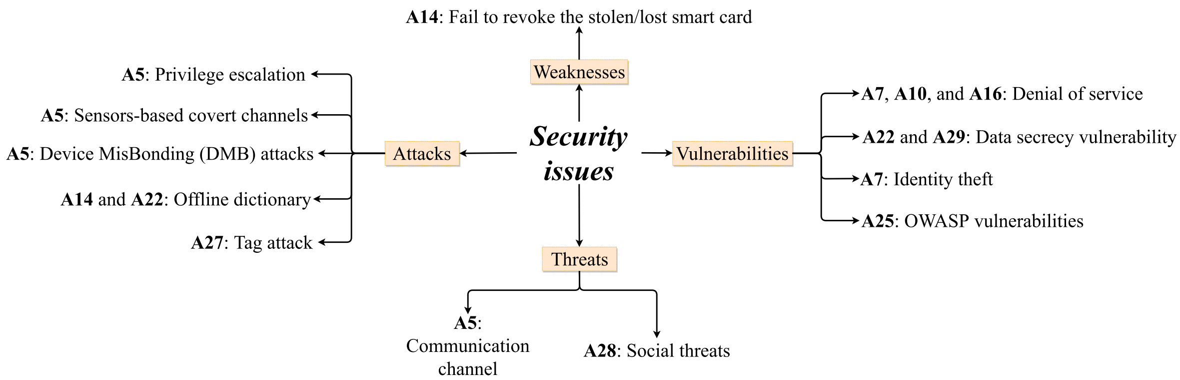

FIGURE 9. Security issues.

security and specification establish that the security requirements are aimed at protecting the information.

A20 discusses an extension of SysML requirements diagram. The authors propose CompASRE, a comprehensive SRE approach that incorporates the strengths and best practices related to security requirements engineering.

7) RISK MANAGEMENT

Risk management is the process of identifying, analyzing, and responding to risk factors throughout the life of a project and for the benefit of its objectives [36]. Proper risk management involves the control of possible future events. In addition, risk management is proactive, rather than reactive.

A15 suggests a model aiming at managing risks in telemedicine environments. The authors use the Dempster and Shafer Theory to process security management evidence for the purpose of forecasting risks associated with the continual feasibility of a telemedicine system.

B. RQ2: SECURITY ISSUES

Few studies (24%) reported which security issue they address in their proposals (see Figure 9).

1) ATTACKS

According to [37], a privilege escalation attack takes advantage of programming errors or design flaws to give the attacker elevated accesses to networks. There are two kinds of privilege escalation: vertical and horizontal.

- *Vertical privilege escalation* requires the attacker to grant himself higher privileges. This kind of attack is achieved by performing kernel-level operations that allow the attacker to run unauthorized code.
- *Horizontal privilege escalation* requires the attacker to use the same level of privileges he already has been granted, but assume the identity of another user with similar privileges.

Covert channels are means to transfer information, which were neither designed nor perceived as communication channels [38]. Examples of covert channels include file locks, hardware settings, and modulated execution-time delays. If both applications have enough permission to cause and/or note changes in a shared resource, it could be challenging to detect a smart and creative exploit of that channel. Concerning sensor-based threats, these kinds of threats are related to the attacks to sensors-based privacy and security which use covert channels as a medium of sharing information.

About device mis-bonding attacks, these are related to the lack of bonding between an external device and its official app. In the absence of operating system level protection, this threat can only be addressed by the app-device authentication developed by individual device manufacturers [39].

Offline dictionary attacks are related to the steal of password storage files from the target system. The idea is to intent to find the key necessary to decrypt an encrypted message or document [40].

Tags attacks are related to Radio Frequency Identification Systems (RFID). These systems refer to technologies whereby a reader captures digital data encoded in RFID tags or smart labels via radio waves. In this regard, A27 describes a comprehensive survey on security and privacy issues in RFID systems and their solutions.

2) VULNERABILITIES

A Denial of Service (DoS) is intended to prevent access to an organization's services and resources for an indefinite period [41]. Generally, these types of attacks are aimed at a company's servers, so that they cannot be used or consulted. Its objective is not to recover or alter data, but to damage the reputation of companies with an Internet presence and potentially impede the normal development of their activities if they are based on a computer system.

Data Secrecy means to protect any data which is essential to an organization or specific people. It can also be important to other organizations that certain data is kept private as obligated by contracts, such as non-disclosure agreements, which require internal corporate data to be handled stringently [42].

According to [43], identity theft (also known as *identity fraud*) is a crime in which an imposter obtains key pieces of personally identifiable information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, patient records, and services in the name of the victim, or to provide the thief with false credentials.

The Open Web Application Security Project (OWASP[2]) is a worldwide not-for-profit charitable organization focused on improving the security of software. The OWASP mission is to make software security visible so that individuals and organizations are able to make informed decisions. Regularly, OWASP releases a ranking about the top ten of security risks. In this context, A25 analyzes how web-based telemedicine services are affected by security OWASP risks.

3) THREATS

Communication channel threat compromises the guarantee of messages that travel from a source node to a destination through several intermediate computers on the network (A5).

A28 and A5 (partially) discusses how social threats (also known as *community threats*) compromise security in Telehealth systems. The authors describe three kinds of threats in this context:

- *Technical threats*: Technical threats target both the information repository and the operational infrastructure of the virtual medical community. A virtual medical community is susceptive to a variety of attacks. From outside malicious users gaining unauthenticated access to inside users gaining unauthorized access control to sensitive patient information, all these threats are a significant issue that concerns both the CIA (confidentiality, integrity, availability) model and community trust.
- *Ethical*: The goal of a virtual healthcare community is mainly to provide patients with medical consultation. Nevertheless, if a particular doctor improperly uses patient information to perform genetic or biomedical experiments, or provides medications that violate accepted policies, then critical ethical issues arise.
- *Legal issues*: Virtual healthcare communities usually cross national borders, and as such, they face several legal issues, such as licensing, accreditation, concerns of identity deception and dependency, which are difficult to be adequately addressed by legislative entities.

4) WEAKNESSES

Traditional verification session processes must be anonymous, unlinkable to other sessions, and revealing no personal or traceable information. In contrast, some situations involve the circumstances when the electronic ID card is lost, stolen, or destroyed. In these cases, the credential must be revoked in order to be not used any time in the future. A14 examines the impact of the lack of mitigation strategies when smart cards with password authentication mechanisms are stolen or lost.

5) COMPONENTS AND MEDICAL SUPPLIES AFFECTED BY SECURITY ISSUES

Figure 10 illustrates the Telehealth components compromised by security issues. According to the SMS results, 51% of the primary studies do not describe which components are affected, which means that authors, in general, describe the main security issues faced by Telehealth systems, but they do not specify which components should be put more effort into to mitigate security incidents.

[2]https://www.owasp.org/index.php/Main_Page

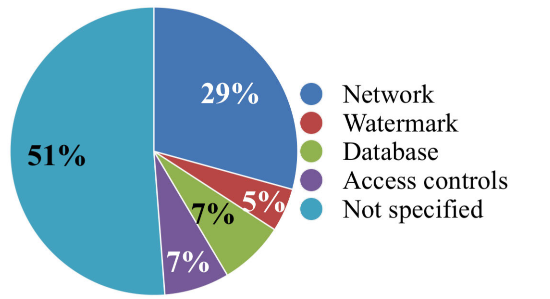

FIGURE 10. Telehealth components affected by security issues.

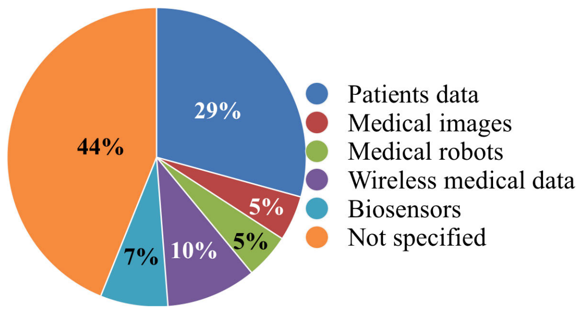

FIGURE 11. Medical supplies affected by security issues.

On the other hand, the most mentioned component is the network. In Telehealth systems, networks consist of several protocols, such as HTTP (Hypertext Transfer Protocol) and FTP (File Transfer Protocol). Each system requires specific requirements in the network, which are developed based on parameters that evaluate the quality of services (QoS) such as bandwidth, loss rate, time used, and others. It is worth mentioning that these parameters vary according to the level of traffic that the application has since it can be transmitted using synchronous or asynchronous methods. Therefore, as a component becomes more complex, it is more susceptible to security incidents.

Although other components (watermark, database, and access control) are mentioned in security incidents, primary studies do not thoroughly discuss the importance and impact of violating aforementioned components in Telehealth systems.

Complementing Figure 10, Figure 11 describes medical supplies compromised by security issues. Like Figure 10, there is a significant number of primary studies (44%) that does not clearly describe which security incidents compromise medical supplies. The rest of studies mention that the electronic patient record is the most affected supply.

C. RQ3: SOLUTIONS

Figure 12 illustrates that most proposals point to detect attacks and stop or mitigate attacks. Nevertheless, we do not

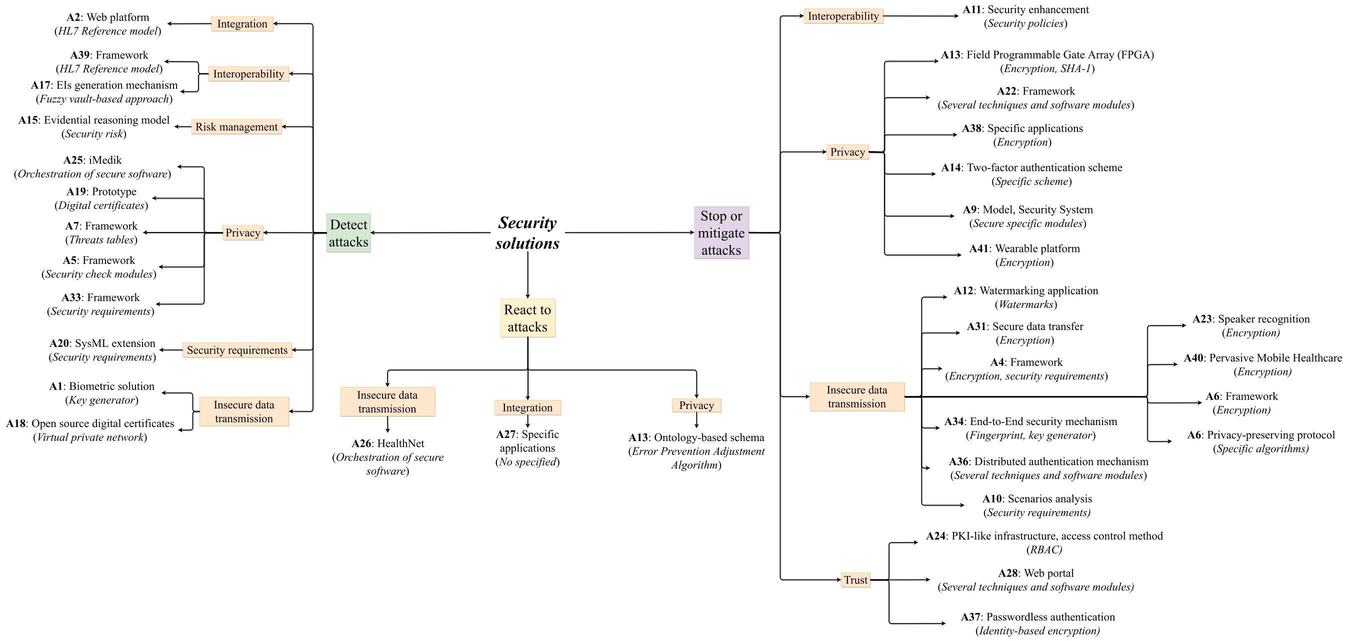

FIGURE 12. Telehealth solution map.

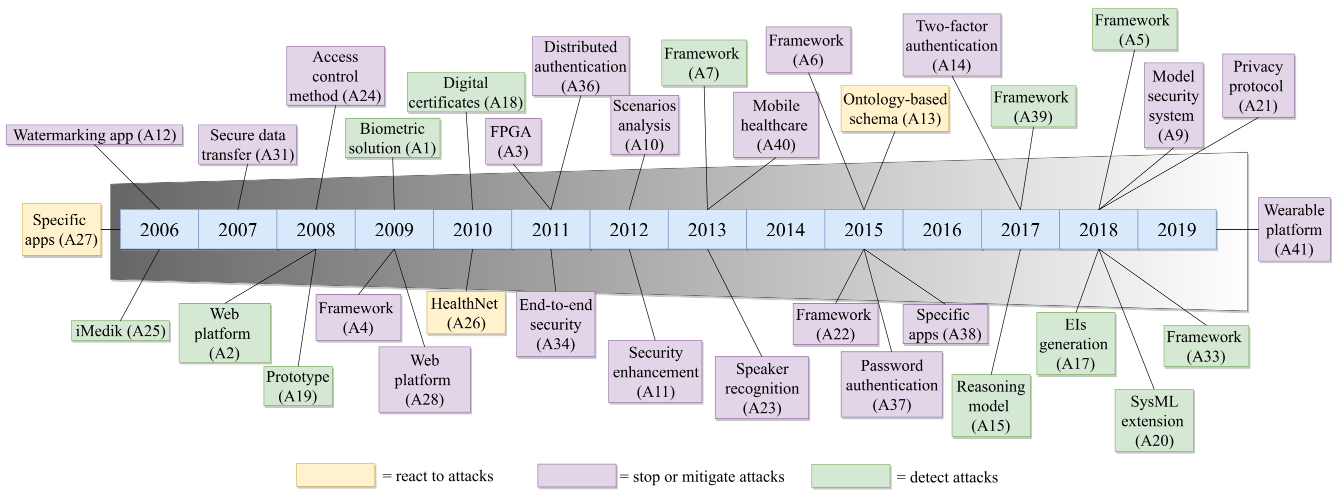

FIGURE 13. Evolution of Telehealth system security solutions over the years.

find studies where their solutions concern about recover from attacks.

Figure 13 describes the distribution of solutions over the years. It is possible to appreciate that most of the solutions are mainly concerned with stop or mitigate attacks. The solutions related to this strategy seek to create concrete action plans that help counteract attacks by cybercriminals. Primary studies emphasize that in the health business, Telehealth systems are susceptible to attacks because their main goal is to steal sensitive information from patients in order to committing fraud (A28, A41). But, some primary studies go further. Apart from sensitive patient data, there are other motivations to attack Telehealth systems. Mainly, these motivations lie in economic reasons and industrial espionage related to health providers. Therefore, primary studies that focus on stop or mitigate attacks aim for health institutions to identify the need for serious, strategic, and structural measures to protect their environment from attacks. Failure or unavailability of technologies and equipment can result in a severe threat to the operational continuity of the health organization and, consequently, in timely and quality patient care.

Regarding solutions aimed at detecting attacks, between 2006 and 2010, a couple of primary studies addressed this security strategy. However, between 2011 and 2016, except for one in 2013, there is a deficit of primary studies. Nevertheless, from 2017 to 2018, there is an increase in publications because primary studies point to include new topics, such as artificial intelligence, as defense mechanisms in order to detect attacks. On the other hand, other proposals, such as

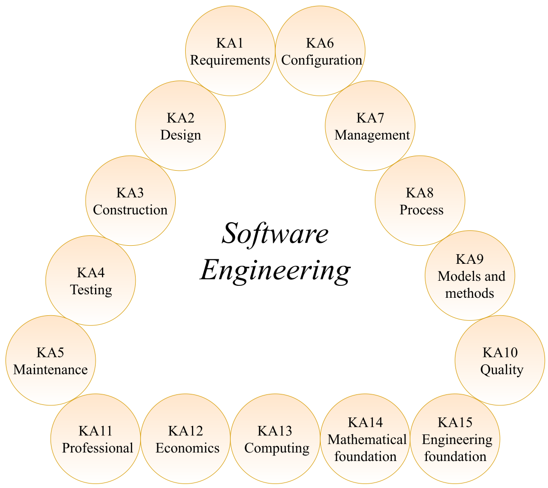

FIGURE 14. Software engineering key areas.

the one described in A20, attempt to expand models already created to detect attacks.

Concerning solutions which their strategy is to react to attacks, we found three primary studies (A27, A26, A13). The main idea of these studies is to provide response plans for situations related to security incidents. In this regard, the mitigation plans referenced by these three primary studies involve taking action plans according to local policies and regulations defined by health institutions. This means that mitigation plans depend on how health institutions set their own administrative security policies.

V. DISCUSSION

In Section IV, we illustrated security aspects (research themes, issues, and solutions) concerning Telehealth systems. Therefore, taking as reference the findings of the previous section, this section discusses how Software Engineering can contribute to building secure Telehealth systems. To conduct the analysis, we used the SWEBOK (Software Engineering Body of Knowledge) [13] as a basis, which is a guide that describes generally accepted knowledge about software engineering. SWEBOK describes 15 knowledge areas (KA) (see Figure 14).

We reviewed each KA aiming at identifying which KAs are critical to handle security issues in Telehealth systems. In our analysis, we considered the solutions described in Figure 12. For each primary study, two researchers rated the studies using the following range: "Strongly agree", "Agree", "Neither agree nor disagree", "Disagree", and "Strongly disagree" in order to define if a specific primary study is related (or not) to Software Engineering KAs. Then, in brainstorming sessions, each particular decision was analyzed, and a final decision was determined for each article (related or unrelated). Consequently, Figure 15 depicts the detailed result of the final analysis between primary studies and KAs.

According to Figure 15, the KAs that cover primary studies are *Software Design* (KA2, 31/41), then *Software Requirement* (KA1, 11/41), *Software Engineering Models and Methods* (K9, 7/41), *Software Construction* (KA3, 1/41) and *Software Engineering Professional Practice* (KA11, 1/41). Regarding KAs 3 and 11, these primary studies investigate about legal (KA11) and secure software construction (KA3) aspects in the context of security and Telehealth systems. In the following sections, we further discuss the KAs with the highest number of primary studies.

A. SOFTWARE DESIGN

Software design is the software engineering life cycle activity in which software requirements are analyzed in order to produce a description of the software's internal structure that will serve as the basis for its construction [13]. In this context, security issues can be handled in the *software architecture* level. According to Bass *et al.* [32], the software architecture of a system is the set of structures needed to reason about the system, which compromises software elements, relations among them, and properties of both.

Telehealth systems are fashioned of software systems that have their designs to meet particular purposes. Moreover, these software systems are surrounded by a large number of components (such as servers, medical equipment, and tablets) and stakeholders (patients, physicians, nurses, and others). In this context, we distinguished two significant absences:

- *Discussion about architectural styles*: Architectural styles are particular solutions which typically centers on how to organize code and components created for the software. It is the granularity of the highest level that focuses on creating the layers and modules of the software and allowing a proper interaction between the various modules for giving the right results upon implementation [32]. Some architectural styles are: blackboard, peer-to-peer, pipes and filters, microservices, and others. RQ3 revealed that security solutions provided by primary studies are *ad-hoc* solutions to particular problems. Each proposal is distinctive and does not allow conceiving if a specific architectural style helps to handle security issues in Telehealth systems.
- *Key stakeholders identification*: Primary studies whose solutions require the creation of architectures do not mention how they identified the key stakeholders that surround Telehealth systems. According to [32], for an architecture to be prosperous, the architect must consider all key stakeholders' viewpoints. Nevertheless, we realized that solutions reported in RQ3 point to satisfy the needs of physicians and nurses primarily, leaving aside other key stakeholders, such as health managers, health administration professionals, laboratories, and others.

Hence, to face security incidents in Telehealth systems, software systems must have suitable architectures to protect patient's data and information from unauthorized access while still granting access to authorized health professionals and systems. To achieve this, architectural evaluation techniques (such as Software Architecture Analysis Method

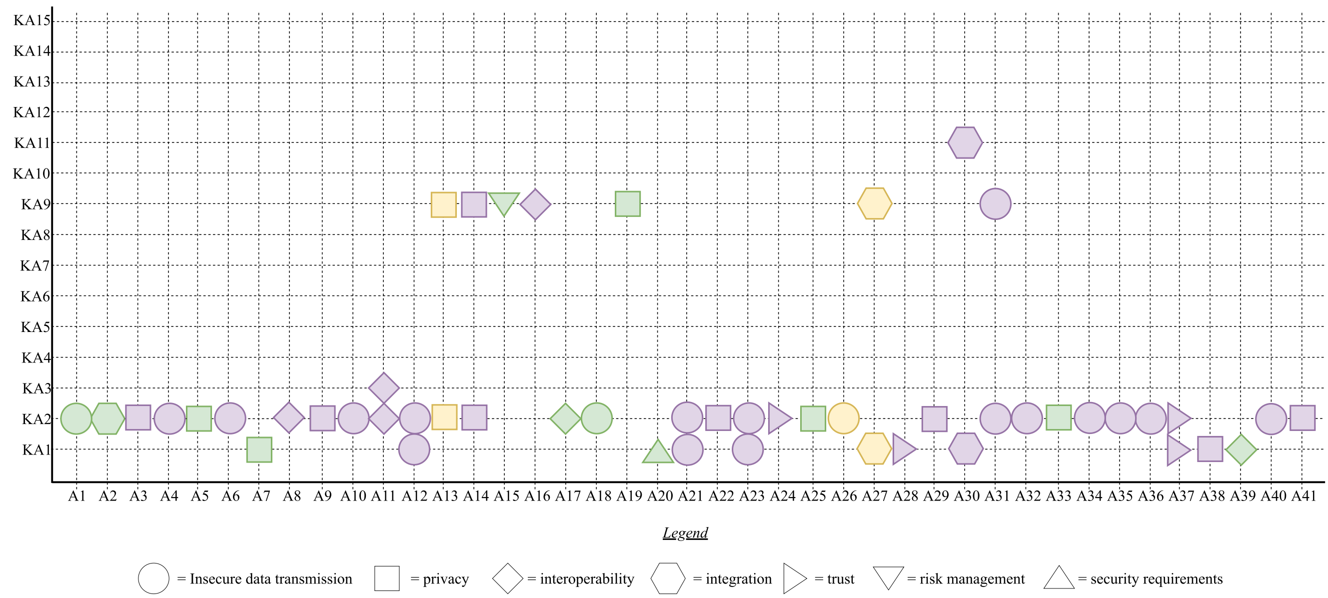

FIGURE 15. Software engineering key areas and primary studies. As in Figures 12 and 13, green symbols indicate "Detect attacks" strategies; purple indicates "Stop or mitigate attacks"; yellow indicates "React to attacks".

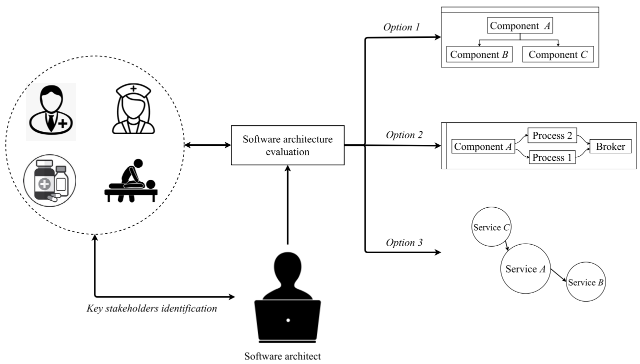

FIGURE 16. Software architecture evaluation overview.

(SAAM) [32], Architecture Trade-off Analysis Method (ATAM) [32], and others) must be conducted in order to satisfy the Telehealth system stakeholders' needs (see Figure 16). The goal of evaluating architectures is to identify and analyze several architectures instead of selecting a unique one.

In order to complement architectural styles, security patterns emerge as an alternative to make security decisions in order to build secure Telehealth systems. Security patterns represent solutions to the problem of controlling a set of specific threats through some security mechanism, defined in a given context [44]. Security patterns provide best practices for avoiding security-related design flaws in software.

For example, Figure 17 describes the RBAC (Role Based Access Control) security pattern. This pattern can be used when it is required to control access based on roles. Therefore, the solution provided by this pattern is to extend the Authorization security pattern [44], so users are assigned roles, and roles have rights.

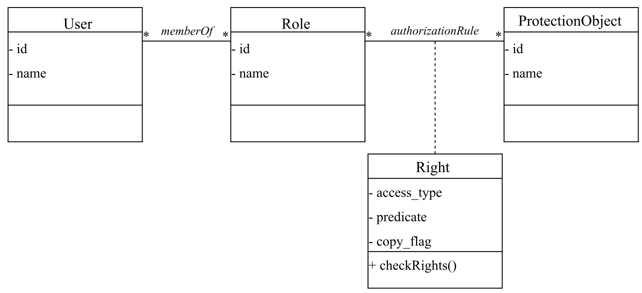

FIGURE 17. RBAC security pattern.

Including security patterns as part of the software development and architecture process helps to systematize security knowledge, allowing to manage and expand the behavior of security and their incorporation at very early stages of the development of secure Telehealth systems. Furthermore, security patterns help build the traceability of security requirements. If the security requirement change, for example, due to changes in security policies or domain requirements, it is possible to describe and follow the impact of these changes up to the design stage through the definition of security patterns.

B. SOFTWARE REQUIREMENTS

Often, the success or failure of a software system depends on adequate requirements elicitation. In the security context, security requirements are conditions over the phenomenon of the environment that it is wished to make true by installing the system in order to mitigate risks [45]. Furthermore, security requirements define what level of security is expected from the system with respect to some threat or malicious attack.

Primary studies that mentioned the importance of the requirements to handle security issues (A20, A23, and A37) agree that the developers' inexperience produces some of the security incidents on specific telehealth domains, such as telecommunication, sensors, robotics, among others. Generally, primary studies discuss that poor elicitation of requirements in telehealth is caused by several factors, such as:

- *Lack of resources*: few health institutions have the necessary resources to conduct effective requirements management and elicitation.
- *Limited knowledge*: Other studies, such as [46], open the discussion about the lack of capacity and resources that health institutions have to identify security requirements adequately

Although it is not possible to attribute all security issues to incorrect requirements elicitation, some studies (such as A20) suggest that advanced models of security requirements for Telehealth systems assist in mitigating security incidents. Moreover, if models consider international standards, such as Health Level Seven - Clinical Document Architecture (HL7-CDA,[3]) inherent attacks could be identified and analyzed in the early stages of Telehealth systems development.

C. SOFTWARE ENGINEERING MODELS AND METHODS

This KA is concerned about structures on Software Engineering with the goal of making activities more systematic, repeatable, and ultimately more success-oriented.

Primary studies related to this KA are not intended to propose new methodologies and software development models for the Telehealth system. What they recommend is to include the concept of security as a methodology and culture for the development of Telehealth systems and adapt highly used standards (such as HL7) in the development methodology.

At this point, the concept of *security by design* is emerging as a system development philosophy given the increase in data and devices and new complex challenges that this entails [47]. This concept suggests that software must be designed securely from the beginning. Academic and grey literature describe different security design principles; however, Whitman and Mattord [47] summarize them:

- *Economy of mechanism*: Keep the design as simple and small as possible.
- *Fail-safe defaults*: Base access decisions on permission rather than exclusion.
- *Complete mediation*: Every access to every object must be checked for authority.
- *Open design*: The design should not be secret, but rather depend on the possession of keys or passwords.
- *Separation of privilege*: Where feasible, a protection mechanism should require two keys to unlock, rather than one.
- *Least privilege*: Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- *Least common mechanism*: Minimize mechanisms (or shared variables) common to more than one user and depended on by all users.
- *Psychological acceptability*: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

Using these principles in the development of Telehealth software systems may help to mitigate potential security incidents that compromise not only the whole Telehealth system but also the patient's integrity and health.

D. EMERGING CHALLENGES

In the previous sections, we discussed which Software Engineering KAs are relevant to address security issues in Telehealth systems. However, another guideline that merits analysis is about the challenges concerning security that primary studies describe.

1) EXPONENTIAL GROWTH OF MEDICAL DATA

Currently, numerous sources of heterogeneous data provide large amounts of information related to patients, diseases, and health centers. The application of Big Data techniques allows inferring a layer of intelligence that anticipate patients' needs and offer more effective medical care. Therefore, in this context, a significant challenge is how to create Telehealth software systems that achieve confidentiality, integrity, and availability in order to protect a vast amount of patients' data.

Software architectures for Big Data may help to address this challenge. In this regard, virtualized cloud architectures can provide several advantages for handling big data in order to provide scalability, security, performance, and other quality attributes. Furthermore, new emerging challenges, such as rethinking architectural solutions to meet functional and non-functional requirements related to volume, variety, and velocity, incite to expand the research background of Software Engineering to propose new methods and techniques [48].

2) CONNECTED TELEHEALTH DEVICES

More and more, the quantity of devices that surround Telehealth systems grows. These devices encompass cyber-physical systems, robots, sensors, and others. Therefore, the emerging challenge is how to build highly interoperable, secure, and scalable Telehealth systems. In this context, new emerging architectural styles, such as *microservices*, provides features to build software systems considering the characteristics mentioned above.

According to Newman [49], microservices is an architectural style that is regarded as ideal when it is necessary to support across a wide array of platforms as well as devices across the web, such as Internet of Things (IoT), mobiles, wearables, and others.

3) "MONOLITHIC" TELEHEALTH SYSTEMS

"Monolithic" is referred to when the software systems' components are interconnected rather than loosely coupled, which implies that if any software component must be updated,

[3]http://www.hl7.org

added or deleted, the entire application has to be rewritten. In Telehealth systems, this situation can involve the patient's life if a component or process fails. Therefore, the question is how to build non-monolithic Telehealth systems. Like the previous challenge, microservices provide properties in order to ensure flexible architectures.

VI. THREATS TO VALIDITY

This section aims to discuss the threats to the validity of our SMS [31].

A. INTERNAL VALIDITY

Threats to internal validity describe factors that could affect the study's results. We addressed the following threats with specific mitigation plans:

- *Study search*: To mitigate this threat, we used the predefined search string on major electronic databases. Before taking an actual search on the place, we also performed a pilot search on all selected databases to verify the accuracy of our search string.
- *Bias on study selection*: The studies selection has been made by applying explicitly defined inclusion and exclusion criteria. To avoid the possible bias, we also performed the cross-check validation for all selected studies.
- *Bias on data extraction*: To obtain data consistency and avoid bias in data extraction, we defined the data extraction template (see Table 1). Initially, two authors equally distributed the number of studies and then they obtained the data according to the data extraction form. The same two authors regularly discussed and shared their findings to avoid data extraction bias.
- *Bias on research themes classification*: We identified the research themes by using guidelines of thematic analysis proposed by Braun *et al.* [23]. Furthermore, these guidelines provide qualitative analytic methods to obtain research themes in primary studies. In turn, two researchers conducted this activity.

B. EXTERNAL VALIDITY

Threats to external validity are restrictions that restrict the ability to generalize results. The inherent threat related to external validity is about if primary studies represent security issues in Telehealth systems. We mitigated this threat by choosing peer-reviewed studies and excluding grey literature (white papers, editorials, and others). Furthermore, we used feedback from healthcare professionals to validate the inclusion and exclusion criteria.

C. CONCLUSION VALIDITY

Threats to the conclusions validity are concerned with issues that affect the ability to draw the correct conclusions. Although we used the guidelines of Kitchenham and Charters [15], which already assumes that not all relevant primary studies that exist can be identified, we handled this validity threat by discussing our results in several brainstorming sessions with healthcare professionals. The number of primary studies obtained in this SMS allowed us to analyze each primary study critically.

D. CONSTRUCT VALIDITY

Construct validity is related to the generalization of the result to the concept or theory behind the study execution [31]. The main threat is the subjectivity of our results. To mitigate this threat, two researchers conducted (independently) the main steps of our SMS. Subsequently, they discussed their results in order to converge in a consensus.

VII. RELATED WORK

This section explores the related work concerning security in Telehealth Systems.

Zeadally *et al.* [50] conducted a literature review about security attacks on Electronic Health Systems (E-Health). The authors mentioned that telecommunications technology used by E-Healths applications are prone to advanced attacks. Furthermore, they argue that recent attacks in the various domains of E-health correspond to security and privacy. The authors conclude their research by mentioning that it is imperative that researchers thoroughly address these security challenges.

Ida *et al.* [51] investigated security in IoT and Cloud. The authors discussed the gap between IoT systems and vulnerabilities in the context of E-Health systems. In addition, the authors discussed different vulnerabilities of IoT in a cloud context in order to present novel solutions to protect health information.

Garg and Brewer [52] conducted a systematic review concerning security in Telemedicine. The authors focused on physical security and issues related to legalities, policies, and standards. Key findings reported by the authors rely on the impact of reliability and availability on critical life-supporting systems. Furthermore, the authors mentioned that it is also essential to maintain the usability of these systems without compromising security.

In the context of network communication, Kompara and Holbl [53] surveyed security issues surrounding body sensor networks. The authors illustrated a list of possible attacks related to intra-body area network communication.

Notwithstanding the significant contribution of previous studies, our study diverges from the previous ones in the discussion about security issues, Telehealth Systems, and Software Engineering. Preceding studies focused on investigating security from a clinical and operational prospect, but they do not discuss which features of Software Engineering are critical to developing secure Telehealth Systems.

VIII. CONCLUSION

This article reports the results of an SMS about security issues related to Telehealth Systems. Furthermore, based on the SMS's findings, it provides a discussion about the role of

Software Engineering in developing Telehealth Systems. The research questions that support our SMS are:

- **RQ1**: *Which research themes characterize security in Telehealth systems?*
- **RQ2**: *Which security issues have been published concerning Telehealth systems?*
- **RQ3**: *Which security solutions have been proposed for Telehealth systems?*

Regarding RQ1, we identified seven research themes, where the most significant number of primary studies are concentrated in two, insecure data transmission and privacy. For the first, research focused on how to protect communication in Telehealth systems from security incidents. And the second one points out how Telehealth systems should satisfy the privacy of patient data. Concerning RQ2, we identified attacks, vulnerabilities, threats, and weaknesses. However, the vast majority of primary studies do not describe which security issues they handle, which leaves a bias in proposing solutions. Furthermore, few primary studies explicitly describe which components, both of Telehealth and medical, are compromised by security incidents. Finally, in RQ3, we illustrated a map of security solutions proposed for Telehealth systems. We organized the solutions in four categories: detect attacks, stop or mitigate attacks, react to attacks, and recovery from attacks.

Subsequently, we analyzed the RQs' results from a Software Engineering perspective. We identified critical key areas that address security aspects in Telehealth systems. Similarly, we identified emerging challenges from the analysis of security and Telehealth systems and we discussed how Software Engineering could contribute to achieving these challenges.

To further our research we are exploring software architectural techniques and design principles to build secure Telehealth Systems and Internet of Medical Things (IoMT) platforms. More precisely, we want to use the findings of this study to establish methodologies in order to develop and deploy secure IoMT platforms for Ambient Assisted Living (AAL) systems focused on the monitoring and care of elderly patients.

On the other hand, we are in the process of investigating quality instruments that allow us to measure the degree of satisfactory compliance concerning quality standards and regulations (mainly focused on functionality, security, and usability) that Telehealth Systems and IoMT platforms in health institutions must address.

ACKNOWLEDGMENT

The authors would like to thank the help provided by M. Pacheco for this article. They would also like to thank the National Center for Health Information Systems (*Centro Nacional en Sistemas de Información en Salud, CENS*), Chile, for supporting this article.

APPENDIX A PRIMARY STUDIES

A1: Zhang, G. H., Poon, C., Li, Ye., and Zhang, Y. T., *A Biometric Method to Secure Telemedicine Systems*, Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2009. Doi: 10.1109/IEMBS.2009.5332470

A2: Sánchez, C., Triana, E. and Romero E., *A flexible web oriented Telehealth platform using a RIM-HL7 Based Model*, Euro American Conference on Telematics and Information Systems (EATIS), 2008. Doi: 10.1145/1621087.1621094

A3: Thamrin, N., Ahmad, I. and Hani, M. *A Secure Field Programmable Gate Array Based System-on-Chip for Telemedicine Application*, International Conference on Information Society (i-Society), 2011.

A4: Boonyarattaphan, A., Bai, Y., and Chung, S. *A Security Framework for e-Health Service Authentication and e-Health Data Transmission*, International Symposium on Communications and Information Technology, 2009. Doi: 10.1109/ISCIT.2009.5341116

A5: Hussain, M., Al-Haiqi, A., Zaidan, A., Zaidan, B., Kiah, M., Iqbal, Sa., Iqbal, S., and Abdulnabi, M. *A security framework for mHealth apps on Android platform*, Computers & security, 2018. Doi: 10.1016/j.cose.2018.02.003

A6: Zaidan, B., Haiqi, A., Zaidan, A., Abdulnabi, M., Kiah, M., and Muzamel, H., *A Security Framework for Nationwide Health Information Exchange based on Telehealth Strategy*, Journal of Medical Systems, 2015. Doi: 10.1007/s10916-015-0235-1

A7: Pendergrass, J. C., Heart, K., Ranganathan, C., and Venkatakrishnan, V. N., *A Threat Table Based Approach to Telemedicine Security*, Transactions of the International Conference on Health Information Technology Advancement, 2013.

A8: Lupu, C., and Cosmin-Constantin, M., *Actual portable devices as base for telemedicine and e-health: research and case study application*, E-Health and Bioengineering Conference (EHB), 2013. Doi: 10.1109/EHB.2013.6707257

A9: Hossain, M., Islam, S. R., Ali, F., Kwak, K. S., and Hasan, R., *An Internet of Things-based health prescription assistant and its security system design*, Future Generation Computer Systems, 2018. Doi: 10.1016/j.future.2017.11.020

A10: M. Johnstone, *Cloud security: A case study in Telemedicine*, ECU Publications, 2012.

A11: Lee, G. S., and Thuraisingham, B., *Cyberphysical systems security applied to telesurgical robotics*, Computer Standards & Interfaces, 2012. Doi: 10.1016/j.csi.2011.09.001

A12: Giakoumaki, A., Perakis, K., Tagaris, A., and Koutsouris, D., *Digital Watermarking in Telemedicine Applications - Towards Enhanced Data Security and Accessibility*, International Conference of the IEEE Engineering in Medicine and Biology Society, 2006. Doi: 10.1109/IEMBS.2006.260283

A13: Gai, K., Qiu, M., Chen, L. C., and Liu, M., *Electronic Health Record Error Prevention Approach Using Ontology in Big Data*, International Conference on High Performance Computing and Communications (HPCC), International Symposium on Cyberspace Safety and Security (CSS), and International Conf on Embedded Software and Systems (ICESS), 2015. Doi: 10.1109/HPCC-CSS-ICESS.2015.168

A14: Xiong, H., Tao, J., and Yuan, C., *Enabling Telecare Medical Information Systems With Strong Authentication and Anonymity*, IEEE Access, 2017. Doi: 10.1109/ACCESS.2017.2678104

A15: Mansouri, S., and Raggad, B. G., *Evidential Modeling for Telemedicine Continual Security*, International Journal of Computer Science and Network (IJCSN), 2017.

A16: Bonaci, T., Yan, J., Herron, J., Kohno, T., and Chizeck, H. J., *Experimental Analysis of Denial-of-Service Attacks on Teleoperated Robotic Systems*, International Conference on Cyber-Physical Systems (ICCPS), 2015. Doi: 10.1145/2735960.2735980

A17: Pirbhulal, S., Shang, P., Wu, W., Sangaiah, A. K., Samuel, O. W., and Li, G., *Fuzzy vault-based biometric security method for tele-health monitoring systems*, Computers and Electrical Engineering, 2018. Doi: 10.1016/j.compeleceng.2018.08.004

A18: Huerta, M., Clotet, R., Alvizu, R., Rivas, D., Lara, F., Escalante, R., and Gonzalez, R.., *Implementation of a Open Source Security Software Platform in a Telemedicine Network*, Advances in E-Activities, Information Security and Privacy, 2010.

A19: Vivas, T., Zambrano, A., and Huerta, M., *Mechanisms of Security Based on Digital Certificates Applied in a Telemedicine Network*, Annual International IEEE EMBS Conference, 2008. Doi: 10.1109/IEMBS.2008.4649532

A20: Maskani, I., Boutahar, J., and El Houssaïni, S. E. G., *Modeling telemedicine security requirements using a SysML security extension*, International Conference on Multimedia Computing and Systems (ICMCS), 2018. Doi: 10.1109/ICMCS.2018.8525939

A21: Li, T., Liu, Y., Xiong, N. N., Liu, A., Cai, Z., and Song, H., *Privacy-Preserving Protocol for Sink Node Location in Telemedicine Networks*, IEEE Access, 2018. Doi: 10.1109/ACCESS.2018.2858274

A22: Simplicio, M. A., Iwaya, L. H., Barros, B. M., Carvalho, T. C., and Näslund, M., *SecourHealth: A Delay-Tolerant Security Framework for Mobile Health Data Collection*, Journal of Biomedical and Health Informatics, 2015. Doi: 10.1109/JBHI.2014.2320444

A23: Nguyen, H. H., Mehaoua, A., and Hong, J. W. K., *Secure Medical Tele-consultation based on Voice Authentication and Realtime Audio/Video Encryption*, International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), 2013. Doi: 10.1109/Ubi-HealthTech.2013.6708066

A24: Liu, Q., Lu, S., Hong, Y., Wang, L., and Dssouli, R., *Securing Telehealth Applications in a Web-Based e-Health Portal*, International Conference on Availability, Reliability and Security IEEE, 2008. Doi: 10.1109/ARES.2008.9

A25: Maji, A. K., Mukhoty, A., Majumdar, A. K., Mukhopadhyay, J., Sural, S., Paul, S., and Majumdar, B., *Security Analysis and Implementation of Web-based Telemedicine Services with a Four-tier Architecture*, International Conference on Pervasive Computing Technologies for Healthcare, 2006. Doi: 10.1109/PCTHEALTH.2008.4571024

A26: Barnickel, J., Karahan, H., and Meyer, U., *Security and Privacy for Mobile Electronic Health Monitoring and Recording Systems*, International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 2010. Doi: 10.1109/PCTHEALTH.2008.4571024

A27: Xiao, Y., Shen, X., Sun, B. O., and Cai, L., *Security and Privacy in RFID and Applications in Telemedicine*, IEEE Communications Magazine, 2006. Doi: 10.1109/MCOM.2006.1632651

A28: Chryssanthou, A., Varlamis, I., and Latsiou, C., *Security and trust in virtual healthcare communities*, International Conference on PErvasive Technologies Related to Assistive Environments (PETRA), 2009. Doi: 10.1145/1579114.1579186

A29: Zain, J., and Clarke, M., *Security In Telemedicine: Issues In Watermarking Medical Images*, International Conference: Sciences of Electronic,Technologies of Information and Telecommunications (SETIT), 2005.

A30: Chang, M. J., Jung, J. K., Park, M. W., and Chung, T. M., *Strategy to Reinforce Security in Telemedicine Services*, International Conference on Advanced Communication Technology (ICACT), 2015. Doi: 10.1109/ICACT.2015.7224778

A31: Kovacevic, S., Kovac, M., and Knezovic, J., *System for Secure Data Exchange in Telemedicine*, International Conference on Telecommunications - ConTEL, 2007. Doi: 10.1109/CONTEL.2007.381881

A32: Qu, H., Cheng, J., Cheng, Q., and Wang, L. Y., *WiFi-Based Telemedicine System: Signal Accuracy and Security*, International Conference on Computational Science and Engineering, 2009. Doi: 10.1109/CSE.2009.60

A33: Hussain, M., Zaidan, A. A., Zidan, B. B., Iqbal, S., Ahmed, M. M., Albahri, O. S., and Albahri, A. S., *Conceptual framework for the security of mobile health applications on Android platform*, Telematics and Informatics, 2018. Doi: 10.1016/j.tele.2018.03.005

A34: Subramanian, M. S., and Anand, S., *End-to-End Security for At-Home Medical Monitoring*, International Conference on Network Security and Applications, 2011. Doi: 10.1007/978-3-642-22540-6_46

A35: Barua, M., Alam, M. S., Liang, X., and Shen, X., *Secure and quality of service assurance scheduling scheme for wban with application to ehealth*, Wireless Communications and Networking Conference 2011. Doi: 10.1109/WCNC.2011.5779285

A36: Doh, I., Lim, J., and Chae, K., *Distributed authentication mechanism for secure channel establishment in ubiquitous medical sensor networks*, Mobile Information Systems, 2011. Doi: 10.3233/MIS-2011-0117

A37: Kamarudin, N. H., Yussoff, Y. M., and Hashim, H., *IBE_Trust Authentication for e-health mobile monitoring system*, Symposium on Computer Applications & Industrial Electronics (ISCAIE), 2015. Doi: 10.1109/ISCAIE.2015.7298348

A38: Arun, V., Shyam, V., and Padma, S. K., *Privacy of health information in telemedicine on private cloud*, Family Medicine & Medical Science Research, 2015. Doi: 10.4172/2327-4972.1000189

A39: Lubamba, C., and Bagula, A., *Cyber-healthcare cloud computing interoperability using the HL7-CDA standard*, Symposium on Computers and Communications (ISCC), 2017. Doi: 10.1109/ISCC.2017.8024513

A40: Sudha, G., and Ganesan, R., *Secure transmission medical data for pervasive healthcare system using android*, International Conference on Communication and Signal Processing, 2013. Doi: 10.1109/iccsp.2013.6577090

A41: Pirbhulal, S., Samuel, O. W., Wu, W., Sangaiah, A. K., and Li, G., *A joint resource-aware and medical data security framework for wearable healthcare systems*, Future Generation Computer Systems, 2019. Doi: 10.1016/j.future.2019.01.008

REFERENCES

[1] World Health Organization. *Telehealth*. Accessed: Sep. 9, 2019. [Online]. Available: https://www.who.int/sustainable-development/health-sector/strategies/telehealth/en/

[2] American Telemedicine Association. *Telemedicine Glossary*. Accessed: Feb. 3, 2019. [Online]. Available: https://thesource.americantelemed.org/resources/telemedicine-glossary

[3] A. Chryssanthou, I. Varlamis, and C. Latsiou, "Security and trust in virtual healthcare communities," in *Proc. 2nd Int. Conf. Pervasive Technol. Rel. Assistive Environ. (PETRA)*, 2009, p. 72, doi: 10.1145/1579114.1579186.

[4] G. S. Lee and B. Thuraisingham, "Cyberphysical systems security applied to telesurgical robotics," *Comput. Standards Interfaces*, vol. 34, no. 1, pp. 225–229, Jan. 2012, doi: 10.1016/j.csi.2011.09.001.

[5] M. Hussain, A. Al-Haiqi, A. Zaidan, B. Zaidan, M. Kiah, S. Iqbal, S. Iqbal, and M. Abdulnabi, "A security framework for mHealth apps on Android platform," *Comput. Secur.*, vol. 75, pp. 191–217, Jun. 2018, doi: 10.1016/j.cose.2018.02.003.

[6] M. Hossain, S. R. Islam, F. Ali, K.-S. Kwak, and R. Hasan, "An Internet of Things-based health prescription assistant and its security system design," *Future Gener. Comput. Syst.*, vol. 82, pp. 422–439, May 2018, doi: 10.1016/j.future.2017.11.020.

[7] M. Sajjad, A. A. Abbasi, A. Malik, A. B. Altamimi, and I. M. Alseadoon, "Classification and mapping of adaptive security for mobile computing," *IEEE Trans. Emerg. Topics Comput.*, to be published, doi: 10.1109/TETC.2018.2791459.

[8] F. Fatehi and R. Wootton, "Telemedicine, telehealth or e-health? A bibliometric analysis of the trends in the use of these terms," *J. Telemed. Telecare*, vol. 18, no. 8, pp. 460–464, Dec. 2012, doi: 10.1258/jtt.2012.gth108.

[9] Joint Action to Support the eHealth Network. (2017). *Report on EU State of Play on Telemedicine Services and Uptake Recommendations*. [Online]. Available: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20171128_co09_en.pdf

[10] *Telehealth*. Accessed: Apr. 10, 2019. [Online]. Available: https://www.who.int/sustainable-development/health-sector/strategies/telehealth/en/

[11] *Telemedicine: Opportunities and Developments in Member States*. Accessed: Apr. 10, 2019. [Online]. Available: https://www.who.int/goe/publications/goe_telemedicine_2010.pdf

[12] *Telecare, Telehealth and Assistive Technologies—Do We Know What We're Talking About?* Accessed: Apr. 10, 2019. [Online]. Available: http://telecareaware.com/wp-content/uploads/2008/12/jat1-2debate_article.pdf

[13] P. Bourque and R. E. Fairley, *Software Engineering Body of Knowledge*. Washington, DC, USA: IEEE Computer Society Press, 2014.

[14] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *Proc. Int. Conf. Eval. Assessment Softw. Eng. (EASE)*, Oct. 2019.

[15] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele Univ., Keele, U.K., Tech. Rep. 2007-001, 2007.

[16] V. J. Watzlaf, D. R. Dealmeida, L. Zhou, and L. M. Hartman, "Protocol for a systematic review of telehealth privacy and security research to identify best practices," *Int. J. Telerehabilitation*, vol. 7, no. 2, p. 15, 2015, doi: 10.5195/ijt.2015.6186.

[17] L. Makris, N. Argiriou, and M. G. Strintzis, "Network and data security design for telemedicine applications," *Med. Inform.*, vol. 22, no. 2, pp. 133–142, Jan. 1997, doi: 10.3109/14639239709010886.

[18] W. S. Richardson, M. C. Wilson, J. Nishikawa, and R. S. Hayward, "The well-built clinical question: A key to evidence-based decisions," *ACP J. Club*, vol. 123, no. 3, p. A12-3, 1995.

[19] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Inf. Softw. Technol.*, vol. 55, no. 12, pp. 2049–2075, 2013, doi: 10.1016/j.infsof.2013.07.010.

[20] M. S. Jalali, S. Razak, W. Gordon, E. Perakslis, and S. Madnick, "Health care and cybersecurity: Bibliometric analysis of the literature," *J. Med. Internet Res.*, vol. 21, no. 2, p. e12644, 2019, doi: 10.2196/12644.

[21] N. Brennan, R. Barnes, M. Calnan, O. Corrigan, P. Dieppe, and V. Entwistle, "Trust in the health-care provider-patient relationship: A systematic mapping review of the evidence base," *Int. J. Qual. Health Care*, vol. 25, no. 6, pp. 682–688, Dec. 2013, doi: 10.1093/intqhc/mzt063.

[22] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng.*, 2014, p. 38, doi: 10.1145/2601248.2601268.

[23] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Res. Psychol.*, vol. 3, no. 2, pp. 77–101, 2006, doi: 10.1191/1478088706qp063oa.

[24] *Common Vulnerabilities and Exposures*. Accessed: Jul. 12, 2019. [Online]. Available: https://cve.mitre.org

[25] *Common Weakness Enumeration*. Accessed: Jul. 12, 2019. [Online]. Available: https://cwe.mitre.org

[26] *Common Attack Enumeration and Classification*. Accessed: Jul. 12, 2019. [Online]. Available: https://capec.mitre.org

[27] *Vulnerability Notes Database*. Accessed: Jul. 12, 2019. [Online]. Available: https://www.kb.cert.org/vuls/

[28] *National Vulnerability Database*. Accessed: Jul. 12, 2019. [Online]. Available: https://nvd.nist.gov

[29] E. B. Fernandez, H. Astudillo, and G. Pedraza-García, "Revisiting architectural tactics for security," in *Proc. Eur. Conf. Softw. Archit.*, 2015, pp. 55–69, doi: 10.1007/978-3-319-23727-5_5.

[30] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: A proposal and a discussion," *Requirements Eng.*, vol. 11, no. 1, pp. 102–107, 2006, doi: 10.1007/s00766-005-0021-6.

[31] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén, *Experimentation in Software Engineering*. Heidelberg, Germany: Springer, 2012.

[32] L. Bass, P. Clements, and R. Kazman, *Software Architecture in Practice* (SEI Series in Software Engineering), 3rd ed. Reading, MA, USA: Addison-Wesley, 2013.

[33] F. T. Jaigirdar, C. Rudolph, and C. Bain, "Can i trust the data i see?: A physician's concern on medical data in IoT health architectures," in *Proc. Australas. Comput. Sci. Week Multiconf. (ACSW)*, 2019, p. 27, doi: 10.1145/3290688.3290731.

[34] W. Hasselbring, "Information system integration," *Commun. ACM*, vol. 43, no. 6, pp. 32–36, 2000, doi: 10.1145/336460.336472.

[35] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for information security management," *J. Inf. Secur.*, vol. 4, pp. 92–100, 2013.

[36] B. W. Boehm, "Software risk management: Principles and practices," *IEEE Softw.*, vol. 8, no. 1, pp. 32–41, Jan. 1991, doi: 10.1109/52.62930.

[37] TechTarget Search Security. *Privilege Escalation Attack*. Accessed: Aug. 26, 2019. [Online]. Available: https://searchsecurity.techtarget.com/definition/privilege-escalation-attack

[38] A. Al-Haiqi, M. Ismail, and R. Nordin, "A new sensors-based covert channel on android," *Sci. World J.*, 2014, doi: 10.1155/2014/969628.

[39] M. Naveed, X. Zhou, S. Demetriou, X. Wang, and C. A. Gunter, "Inside job: Understanding and mitigating the threat of external device mis-bonding on Android," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2014.

[40] D. Wang and P. Wang, "Offline dictionary attack on password authentication schemes using smart cards," in *Information Security*. Cham, Switzerland: Springer, 2015, pp. 221–237, doi: 10.1007/978-3-319-27659-5_16.

[41] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002, doi: 10.1109/MC.2002.1039518.

[42] OwnCloud. (2019). *Data Protection and Data Secrecy in Owncloud*. [Online]. Available: https://oc.owncloud.com
[43] TechTarget Search Security. *Identity Theft*. Accessed: Aug. 27, 2019. [Online]. Available: https://searchsecurity.techtarget.com/definition/identity-theft
[44] E. Fernandez-Buglioni, *Security Patterns in Practice: Designing Secure Architectures Using Software Patterns*. Hoboken, NJ, USA: Wiley, 2013.
[45] D. Mellado, C. Blanco, L. E. Sánchez, and E. Fernández-Medina, "A systematic review of security requirements engineering," *Comput. Standards Interfaces*, vol. 32, no. 4, pp. 153–165, 2010, doi: 10.1016/j.csi.2010.01.006.
[46] A. Winter, R. Haux, E. Ammenwerth, B. Brigl, N. Hellrung, and F. Jahn, "Health information systems," in *Health Information Systems*. London, U.K.: Springer, 2010, pp. 33–42, doi: 10.1007/978-1-84996-441-8_4.
[47] M. Whitman and H. Mattord, *Principles of Information Security*. Boston, MA, USA: Course Technology, 2011.
[48] I. Mistrík, R. Bahsoon, N. Ali, M. Heisel, and B. Maxim, *Software Architecture for Big Data and the Cloud*. San Mateo, CA, USA: Morgan Kaufmann, 2017.
[49] S. Newman, *Building Microservices: Designing Fine-Grained Systems*. Newton, MA, USA: O'Reilly Media, 2015.
[50] S. Zeadally, J. T. Isaac, and Z. Baig, "Security attacks and solutions in electronic health (e-health) systems," *J. Med. Syst.*, vol. 40, no. 12, p. 263, 2016, doi: 10.1007/s10916-016-0597-z.
[51] I. B. Ida, A. Jemai, and A. Loukil, "A survey on security of IoT in the context of ehealth and clouds," in *Proc. Design Test Symp. (IDT)*, 2016, pp. 25–30, doi: 10.1109/IDT.2016.7843009.
[52] V. Garg and J. Brewer, "Telemedicine security: A systematic review," *J. Diabetes Sci. Technol.*, vol. 5, no. 3, pp. 768–777, 2011, doi: 10.1177/193229681100500331.
[53] M. Kompara and M. Hölbl, "Survey on security in intra-body area network communication," *Ad Hoc Netw.*, vol. 70, pp. 23–43, Mar. 2018, doi: 10.1016/j.adhoc.2017.11.006.

GASTÓN MÁRQUEZ is currently pursuing the Ph.D. degree in informatics engineering with Federico Santa María Technical University, Chile. He is also working in the research fields of architectural tactics, patterns, microservice architectures, technical debt, and security in telehealth systems. He has published in several international conferences and has participated in international software architecture schools. He has participated as a Research Visitor with the Rochester Institute of Technology (RIT), Rochester, NY, USA, and the Université de Technologie de Compiègne (UTC), Compiègne, France. Before becoming a Ph.D. student, he worked in financial companies for five years.

HERNÁN ASTUDILLO received the Ph.D. degree in information and computer science from Georgia Tech, in 1995. He is currently a Professor of informatics with the Universidad Técnica Federico Santa María (UTFSM), the highest ranked Chilean University by Times Higher Education. He has been an Informatics Engineer with UTFSM, since 1988. He worked several years as lead or senior applications architect for consulting companies in USA and Chile, before joining Universidade de São Paulo, Brazil, and finally UTFSM, in 2003, where he is currently an Elected Trustee on behalf of professors. His main Research and Development interest is identification, recovery, and reuse of architectural decisions and architectural knowledge (especially architectural tactics). He is also the Principal Investigator of the Toeska Research and Development Team, which conducts teaching, research, and technology transfer in software architecture, semantic software systems and software process improvement, and their application in e-governance and heritage computing. He is also responsible for UTFSM's Software Architecture academic activities. He has published over 100 peer-reviewed articles in international journals and conferences, supervised tens of graduate theses, organized several national and international conferences and workshops, and lead numerous Research and Development projects and international collaboration ventures. He is a member of the IFIP TC2 (Software Engineering) and the Chile Mirror Committee for ISO TC3 (Intelligent Transportation Systems, ITS). He was the founding President of ArquiTIC (the Chilean association of IT architects, and until recently represented Chile in CLEI (the Association of Latin American informatics departments) and chaired the Chilean Scholarships Commission for Computing and Informatics. He is also the Chair of the UTFSM's Doctorate in informatics engineering and the Co-Chair of the UTFSM's BPM Center.

CARLA TARAMASCO received the B.Eng. degree in computer engineering from the Universidad de Valparaíso, Chile, in 2001, the M.Sc. degree in cognitive science from the Ècole Normale Supérieure, in 2006, and the Ph.D. degree *(summa cum laude)* from Ècole Polytechnique, France, in 2011. Her Ph.D. thesis was on Obesity and Social Structures. She was a Postdoctoral Fellow with CNRS, from 2011 to 2013. She is currently a Researcher and also a Professor with the Computer Science Department, Universidad de Valparaíso. She has scientific publications in books, journals, and conference proceedings. She has organized over ten international workshops/sessions and has acted as a Coordinator for over 20 national and international projects. She was involved in the development of networks for scientific collaboration between Africa, South America, and Europe. She was a Coordinator of the Latino America Committee of Complex Systems Society for five years. She has been involved in the investigation and development of technological solutions for health-monitoring software and hardware. She currently teaches both at the undergraduate and graduate levels, along with scientific divulging. Her main academic interests are health, which includes m-health, ambient assisted living for elderly persons, e-health, telemedicine and telerehabilitation, and supervision of chronic diseases and complex social systems, including dynamic networks, socio-semantic networks, and analysis of trajectories both individual and collective and among others.