Journal of Medical Systems (2019) 43: 33
https://doi.org/10.1007/s10916-018-1149-5

SYSTEMS-LEVEL QUALITY IMPROVEMENT

Sensor-Based mHealth Authentication for Real-Time Remote Healthcare Monitoring System: A Multilayer Systematic Review

Moceheb Lazam Shuwandy[1] · B. B. Zaidan[1] · A. A. Zaidan[1] · A. S. Albahri[1]

Received: 22 September 2018 / Accepted: 20 December 2018 / Published online: 6 January 2019

Abstract

The new and groundbreaking real-time remote healthcare monitoring system on sensor-based mobile health (mHealth) authentication in telemedicine has considerably bounded and dispersed communication components. mHealth, an attractive part in telemedicine architecture, plays an imperative role in patient security and privacy and adapts different sensing technologies through many built-in sensors. This study aims to improve sensor-based defence and attack mechanisms to ensure patient privacy in client side when using mHealth. Thus, a multilayer taxonomy was conducted to attain the goal of this study. Within the first layer, real-time remote monitoring studies based on sensor technology for telemedicine application were reviewed and analysed to examine these technologies and provide researchers with a clear vision of security- and privacy-based sensors in the telemedicine area. An extensive search was conducted to find articles about security and privacy issues, review related applications comprehensively and establish the coherent taxonomy of these articles. ScienceDirect, IEEE Xplore and Web of Science databases were investigated for articles on mHealth in telemedicine-based sensor. A total of 3064 papers were collected from 2007 to 2017. The retrieved articles were filtered according to the security and privacy of sensor-based telemedicine applications. A total of 19 articles were selected and classified into two categories. The first category, 57.89% ($n = 11/19$), included survey on telemedicine articles and their applications. The second category, 42.1% ($n = 8/19$), included articles contributed to the three-tiered architecture of telemedicine. The collected studies improved the essential need to add another taxonomy layer and review the sensor-based smartphone authentication studies. This map matching for both taxonomies was developed for this study to investigate sensor field comprehensively and gain access to novel risks and benefits of the mHealth security in telemedicine application. The literature on sensor-based smartphones in the second layer of our taxonomy was analysed and reviewed. A total of 599 papers were collected from 2007 to 2017. In this layer, we obtained a final set of 81 articles classified into three categories. The first category of the articles [86.41% ($n = 70/81$)], where sensor-based smartphones were examined by utilising orientation sensors for user authentication, was used. The second category [7.40% ($n = 6/81$)] included attack articles, which were not intensively included in our literature analysis. The third category [8.64% ($n = 7/81$)] included ‘other’ articles. Factors were considered to understand fully the various contextual aspects of the field in published studies. The characteristics included the motivation and challenges related to sensor-based authentication of smartphones encountered by researchers and the recommendations to strengthen this critical area of research. Finally, many studies on the sensor-based smartphone in the second layer have focused on enhancing accurate authentication because sensor-based smartphones require sensors that could authentically secure mHealth.

Keywords Real-time remote healthcare monitoring system · mHealth · Security and privacy · Sensor · Smartphone

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ A. A. Zaidan
aws.alaa@gmail.com; aws.alaa@fskik.upsi.edu.my

Moceheb Lazam Shuwandy
moceeb@yahoo.com

B. B. Zaidan
bilalbaha@fskik.upsi.edu.my

A. S. Albahri
ahmed.bahri78@gmail.com

[1] Department of Computing, Universiti Pendidikan Sultan Idris, Tanjong Malim, Perak, Malaysia

Introduction

Authentication is a necessary security service to prevent false data injection and is also required to verify a user's identity before data access [1–13]. Authentication, security, user's privacy protection and data confidentiality are important for patient or doctor accessing to remote health monitoring system (RHMS) and Electronic Medical Records (EMR) [14, 15]. RHMS needs secure authentication when using health applications [16–23]. A secure authentication scheme will be required to achieve these goals [24–29].

Telemedicine is an emerging technology that largely benefits patient healthcare areas. It is a medical application of information technology that enables patients to have medical consultations outside hospitals by using video conferencing or digital imaging systems [30, 31]. Telemedicine is a remote medical practice that allows coordination amongst different individuals and facilitates their collaboration efforts in diagnosing or treating a disease through information technologies and telecommunication [32–34]. Thus, this domain requires multidisciplinary advancements, particularly in the use of telecommunication, computer science and instrumentation, for the exchange and administration of medical data [35, 36]. Currently, telemedicine has attracted considerable attention in research due to the development of new technologies [32, 37] and has appeared many tools to support it [38–41]. Telemedicine is a proficient tool that allows coordinated efforts amongst doctors and offers numerous benefits, such as enhanced care, cost investment funds, improved arrival and real-time responses. Similar to medicinal training, telemedicine is used for diagnosis; the conduct of preventive or post-curative medicinal checking and monitoring and therapeutic procedures; and the prescription of medications and provision of services [32]. Authors in [42, 43] reported that a general three-tier pervasive telemedicine system based on a wireless body area network (WBAN) enables real-time and continuous healthcare monitoring. In Tier 1, users can obtain their vital signals through small intelligent wireless sensors and send them to Tier 2, which is the personal gateway (e.g. smartphones), through small-area network protocols (e.g. Bluetooth and Zigbee) and the WBAN. Medical data are sent from Tier 2 to Tier 3, which is the healthcare provider in medical institutes (MIs), through wide-area wireless communication protocols or Internet services. Healthcare providers in Tier 3 apply certain processes and generate services that are sent back to users as responses. Tiers 1 and 2 represent the client side, which can serve patients through mobile health (mHealth), whereas Tier 3 represents the server side. This process is shown in Fig. 1 [35].

With the recent progress of electronics and information technology, telemedicine is currently not only a technology that facilitates remote medical conversations but also utilises various biomedical sensors to capture several critical vital signs [44–46]. Vital signs of patients must be sent to doctors in securely through the Internet (e.g. using IPSec [47–50]). Unfortunately, despite these benefits, telemedicine still suffers from several problems associated with security issues [47–49, 51–55]. Patients have long been plagued by problems, such as security and privacy on authentication for sensor-based mHealth [56–59], there are many techniques can be used to face the security issues related m-health [60–72]. As well as, the sensor-based defence and attack mechanisms can be easily improved to ensure the privacy of patients in the client side when using a smartphone. When using health applications, patients also need access to mHealth via secure authentication to ensure secure transmission of their vital signs/data [47–49, 73–80]. In this context, factors on smartphones are considered to understand fully the various contextual aspects of the field in published studies. The characteristics include the motivation and challenges faced by researchers and the recommendations to strengthen this critical area of research to adopt within mHealth fully. This study aims to analyse and review the literature on sensor-based smartphones. Exploring the literature reveals numerous research articles on authentication for sensor-based smartphones. Many methods and technologies have been previously developed for accessing smartphones, user recognition and data security [81–91]. In this study, the use of smartphone sensors, particularly orientation (e.g. accelerometer, gyroscope and magnetic sensors), finger, camera and touchscreen sensors, is discussed. The main focus of this discussion is on usability and security [92]. Authentication solutions based on biometrics are a promising technique to replace traditional authentication mechanisms [93, 94]; such traditional techniques rely on personal identification numbers (PINs) or passwords, which are often perceived as inconvenient by patients [95–106]. Biometrics is more reliable and capable of distinguishing between the authorised user and a fraud than the traditional means of identity verification, which merely confirms the knowledge of users. The biometric approach has two types, namely, behavioural and physiological. The biometric approach can effectively prevent access to unauthorised mobile resources and avoid identity theft [81–91, 95, 107–110]. Ling (2016) stated that oily or thermal residues remain on the touchscreen, thereby leaving a visible effect that can be detected by the naked eye; thus, the movement of the finger on the screen can be analysed as the starting point of the attack depending on the motion sensor [111]. The use of sensors is varied, and new methods to protect smartphones have been developed. User recognition methods do not require identification through fingertip [112], gesture [108, 113, 114] or gait [115, 116] of users. Some studies are based on the behaviour of patients; therefore, the authentication process has been divided into the following four sections: continuous authentication (CA) [117, 118],

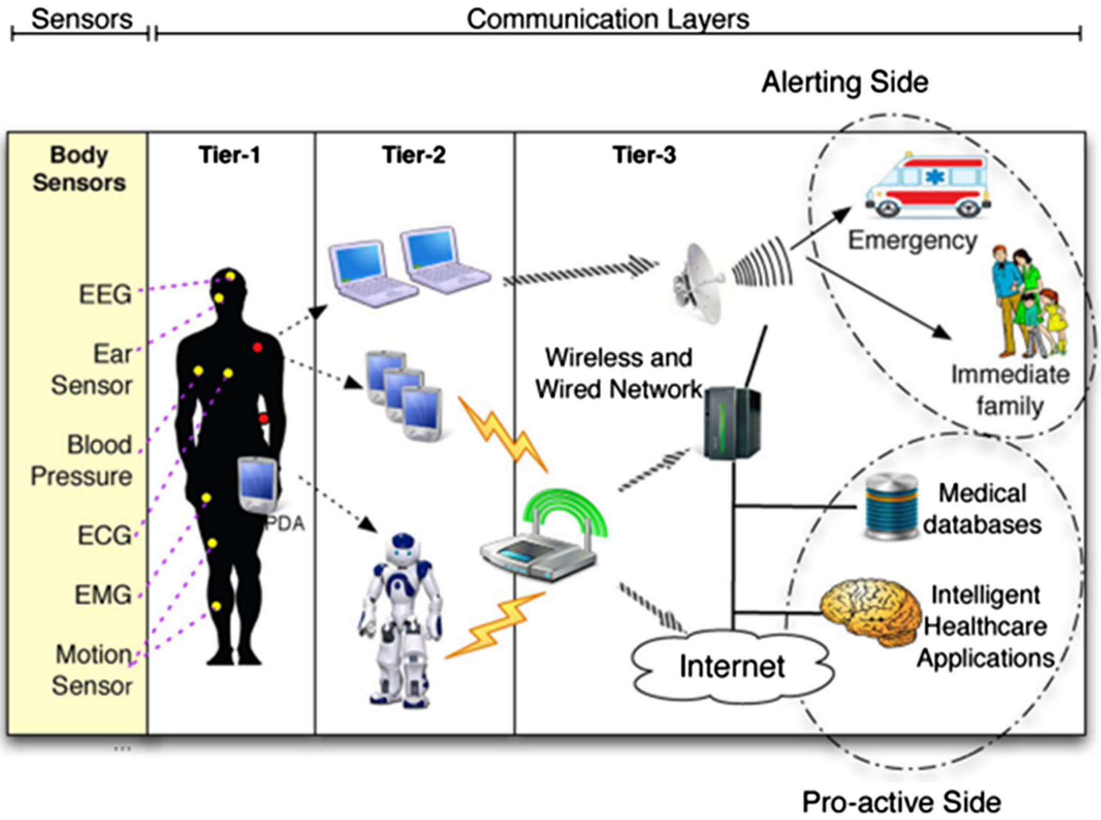


Fig. 1 Three-tiered architecture of a WBAN telemedicine system for healthcare monitoring

implicit authentication (IA) [119, 120], mechanism authentication [121, 122] and hybrid tracking [120]. Researchers have developed methods to obtain the latest impenetrable and easy-to-use sensor to improve the defence and attack mechanisms of sensor-based mHealth [123–125]. Rybnicek (2014) found that no databases are available because user samples contain stored data from accelerometer, gyroscope, touchscreen, keyboard and magnetic terrestrial sensors. Therefore, researchers are required to acquire data prior to exploring a new authentication technique [126]. Nevertheless, many researchers have used ready-made datasets [127]. This systematic review of the present study comprises two layers of review; the first layer aims to survey the academic literature related to the security and privacy of sensor-based telemedicine applications, whereas the second layer aims to survey the relevant studies on security and privacy of sensor-based smartphone authentication. Figure 2 shows a framework of multilayer systematic review protocols. The remainder of this paper is organised as follows. Sections 2 and 3 provide an overview of the first and second layers of our systematic review protocol, respectively. Section 4 illustrates the challenges, motivations, recommendations and methodological aspects indicated in the literature review, which is collected from diverse studies on security and privacy of sensor-based smartphone authentication. Finally, conclusions are drawn in Section 5.

First Layer: systematic review for security and privacy of sensor-based telemedicine applications

Method

Telemedicine applications are widely presented in the academic literature and have recently acquired considerable popularity [128]. The keywords used in the first layer of this study were ‘telemedicine’, ‘sensor’, ‘triage’ and ‘priority’. Only English-language literature is surveyed in this layer. Therefore, all telemedicine-related areas, including the general category of health domains, were considered. The following three digital databases [129, 130] were used to conduct the search for target articles:

1. ScienceDirect database, which offers access to science and technical journal articles;
2. IEEE Xplore library of technical literature in engineering and technology; and
3. Web of Science (WoS) service, an indexing database that covers different academic disciplines.

The sources of this layer were carefully screened from the literature sources. The study period of this layer was 10 years, from 2007 to 2017. The study selection of this layer

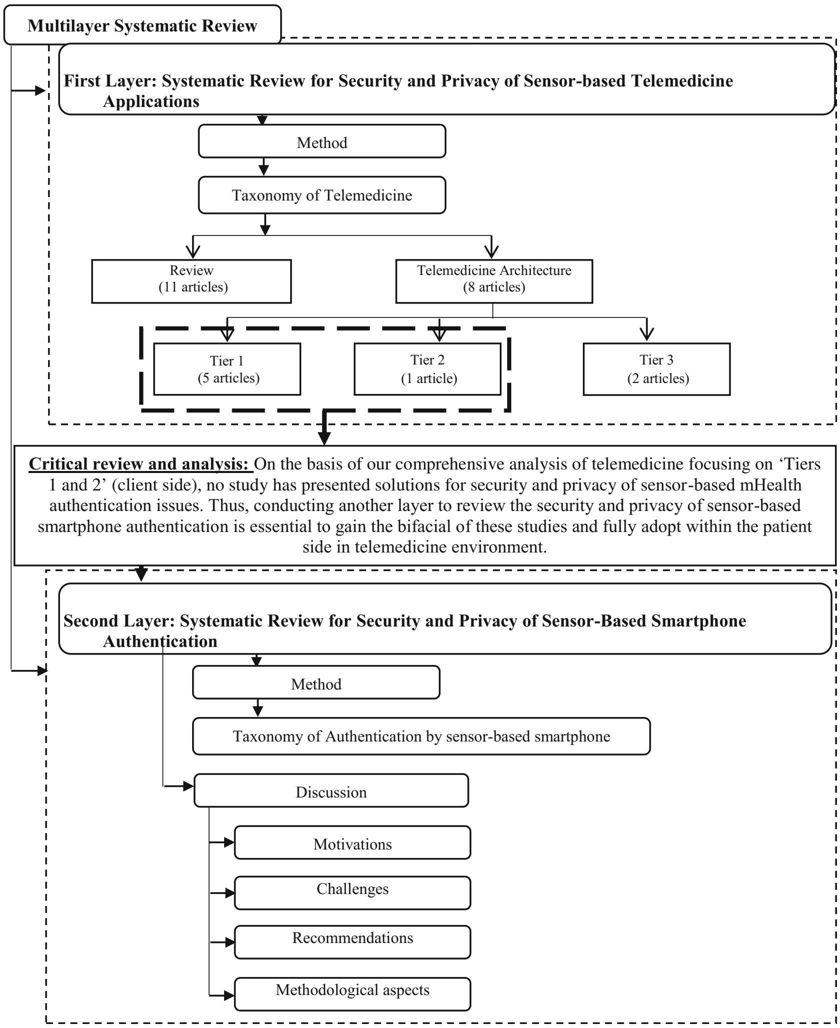

Multilayer Systematic Review
First Layer: Systematic Review for Security and Privacy of Sensor-based Telemedicine Applications
Method
Taxonomy of Telemedicine
Review (11 articles)
Telemedicine Architecture (8 articles)
Tier 1 (5 articles)
Tier 2 (1 article)
Tier 3 (2 articles)
Critical review and analysis: On the basis of our comprehensive analysis of telemedicine focusing on 'Tiers 1 and 2' (client side), no study has presented solutions for security and privacy of sensor-based mHealth authentication issues. Thus, conducting another layer to review the security and privacy of sensor-based smartphone authentication is essential to gain the bifacial of these studies and fully adopt within the patient side in telemedicine environment.
Second Layer: Systematic Review for Security and Privacy of Sensor-Based Smartphone Authentication
Method
Taxonomy of Authentication by sensor-based smartphone
Discussion
Motivations
Challenges
Recommendations
Methodological aspects

Fig. 2 Framework of multilayer systematic review protocols

comprised searching the academic literature sources and was classified based on two stages. **In the first stage**, filtering and screening were accomplished to exclude duplicates and unrelated studies to the remote health monitoring systems based on sensor information [131–133]. **In the second stage**, the authors executed filtering on the basis of the security and privacy of telemedicine applications for articles collected from the first stage. Consequently, the final encompassed set was correlated to the security and privacy of sensor-based telemedicine applications through diverse topics, as shown in Fig. 3. The search was conducted on April 2017 via the search boxes of the ScienceDirect, WoS and IEEE Xplore databases. We used a combination of groups of keywords. The first group included 'medical system', 'telemonitoring', 'e-health', 'telemedicine', 'telehealth', 'healthcare services', 'mHealth', 'remote monitoring' and 'mobile doctor'; these keywords were combined by the 'OR' operator. The second group included 'triage' and 'priority', which were combined by the 'OR' operator. The third group included only one keyword, that is, 'sensor'. The three groups were combined by the 'AND' operator. Figure 3 shows the query. The options provided by each database were considered. Books, reports and contents that appeared in the search results were excluded. However, the latest journal articles and conferences were adopted, and the most relevant were considered for this layer of our study [128, 134–136]. The criteria described in Fig. 3 were followed and applied to each article. Every article that satisfied the criteria listed in Fig. 3 was included. A plan was devised to cover the research using two categories related to the privacy and security of telemedicine literature. Duplicates were initially removed, and the articles that did not satisfy the criteria of eligibility within the stages of screening and filtering were then excluded. All involved criteria used in this layer in the two stages of our filtering are listed in Fig. 3.

Results

In this layer, the first result from the query search showed $n =$ 3064 articles published in 2007–2017; particularly, 657, 911 and 1496 articles were from WoS, Science Direct and IEEE Xplore, respectively. A total of 1612 out of 3064 studies published from 2012 to 2017 were collected in the first stage of

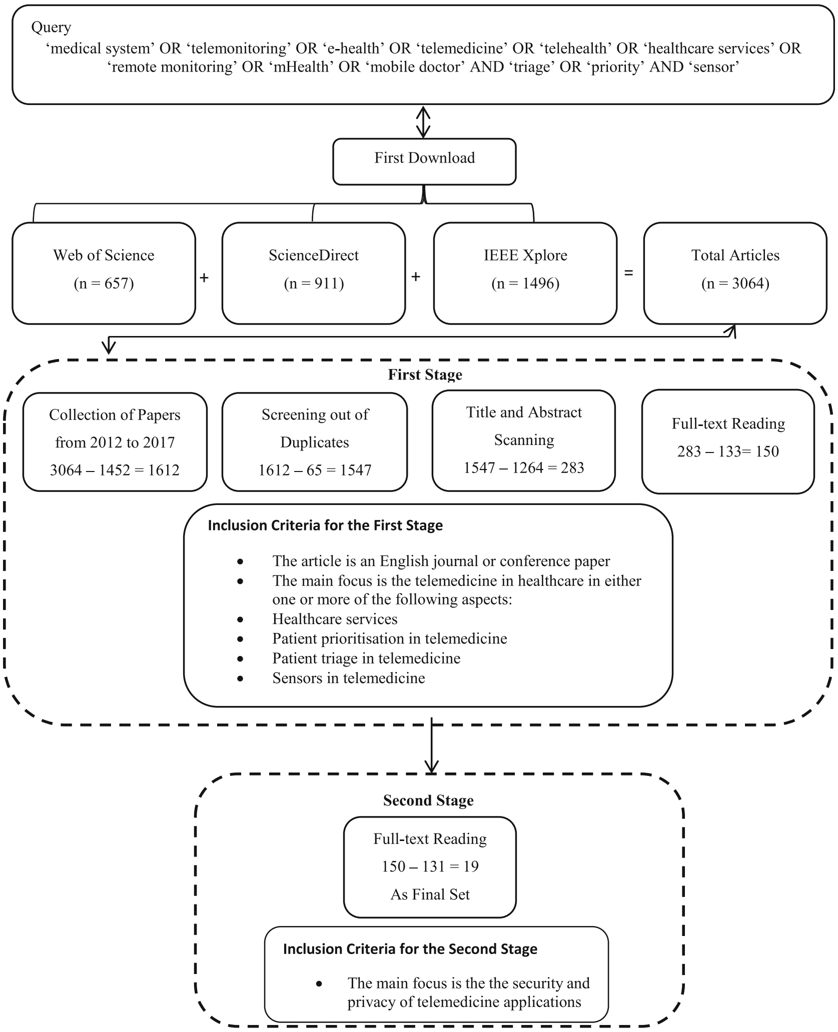

Query
'medical system' OR 'telemonitoring' OR 'e-health' OR 'telemedicine' OR 'telehealth' OR 'healthcare services' OR 'remote monitoring' OR 'mHealth' OR 'mobile doctor' AND 'triage' OR 'priority' AND 'sensor'
First Download
Web of Science (n = 657)
+
ScienceDirect (n = 911)
+
IEEE Xplore (n = 1496)
=
Total Articles (n = 3064)
First Stage
Collection of Papers from 2012 to 2017 3064 – 1452 = 1612
Screening out of Duplicates 1612 – 65 = 1547
Title and Abstract Scanning 1547 – 1264 = 283
Full-text Reading 283 – 133= 150
Inclusion Criteria for the First Stage
• The article is an English journal or conference paper
• The main focus is the telemedicine in healthcare in either one or more of the following aspects:
• Healthcare services
• Patient prioritisation in telemedicine
• Patient triage in telemedicine
• Sensors in telemedicine
Second Stage
Full-text Reading 150 – 131 = 19 As Final Set
Inclusion Criteria for the Second Stage
• The main focus is the the security and privacy of telemedicine applications

Fig. 3 First-layer flowchart of study selection, including search query and inclusion criteria

filtering. Then, the collected studies (n = 65/1612) of duplicated articles were found in the three libraries. This stage also excluded n = 1264/1547 of the articles after filtering the titles and abstracts, and 283 articles were obtained. Reading the entire text resulted in the exclusion of n = 133/283 of the articles, thereby obtaining 150 articles. In the second stage of filtering, the articles were filtered and those obtained from the previous stage according to the security and privacy of telemedicine applications resulted in the exclusion of n = 131/150 of the articles after filtering the full text. Only 19 articles related to the security and privacy of telemedicine applications were obtained. Then, resulting articles from this layer were carefully read and divided into two major categories to present a general research map of the security and privacy of telemedicine applications. Amongst the 19 articles, 57.89% (n = 11/19) indicated the review articles, which aim to examine telemedicine articles and their applications to present the current direction to researchers and identify the need for future research direction on unknown telemedicine topics. A total of 42.1% (n = 8/19) articles involving three tiers (Tiers 1–3) contributed to security and privacy within the telemedicine architecture. Tiers 1 and 2 represented the client side, which comprised medical sensors (i.e. ECG, BP and SpO2) connected with mHealth (i.e. smartphones and taps) that facilitate the transfer of vital signs of patients to the medical centre side (Tier 3). The articles in this category were classified into three subsections as follows: (1) Tier 1 (n = 5/8 articles), Tier 2 (n = 1/8 articles) and Tier 3 (n = 2/8 articles). This systematic review classified all related articles within the mentioned category into a literature taxonomy, as shown in Fig. 4.

Review

The primary goal of survey and review articles on telemedicine is to understand current thinking and justify the need for future research on related topics that have been overlooked or understudied. This category contained 11 articles. A review of the penetration of mobile technology in Asia considered the integration with diagnoses and treatments of mental disorders and highlighted the limitations and potential barriers of mHealth for mental health, including data security and privacy, language and literacy barriers and power supply issues

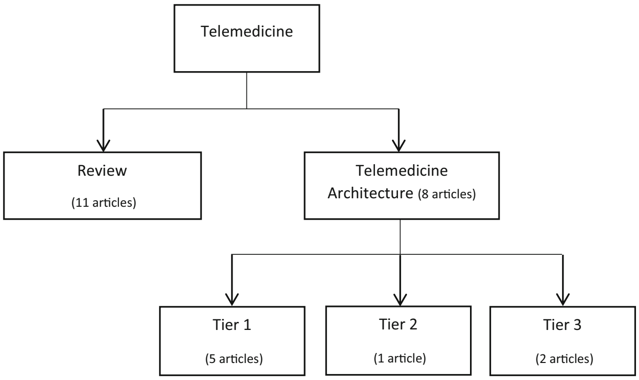


Fig. 4 First-layer taxonomy of research literature on the security and privacy of telemedicine applications

[137]. The study in [35] focused on the field of patient telemonitoring conducted in European projects to present the requirements and components common of telemonitoring system in the context of technical issues, services, tools and functionalities and distinguish projects related to comfort and security. A comprehensive survey of mHealth research initiatives in Brazil included 42 projects. This analysis considered issues, such as health condition, security features, development and deployment of involved main providers, types of devices used and target users, where each project was tested and/or deployed amongst others [138]. The study in [43] reviewed WBAN applications and highlighted their QoS requirements. The goal was to provide appropriate wireless technologies for WBAN by studying various technologies and attempting to associate the WBAN applications with the suitable technologies for maximum QoS. The study in [139] explored the effective measures and strategies for the promotion of ICT-enabled innovations for people with special needs and the elderly. The study reviewed and evaluated the current government initiatives in the field of e-health and accessibility, which address the challenges faced by the rapidly ageing society of Japan. A review of mHealth technologies for military mental health was presented in [140] to identify two categories of high-priority mHealth technology development considerations, namely, priority considerations to mental health care provision and broad applicability to mHealth. This review also included military programmes, such as the Telemedicine and Advanced Technology Research Center, the Military Operational Medicine Research Program, United States Army Medical Research and Material Command and the National Center for Telehealth and Technology. A review in the study of [141] provided an overview on the state of mHealth in a wide array of biomarkers in the context of psychiatric functioning (e.g. anxiety, substance use, autism and psychological stress); this study also identified several specific opportunities for expanding this promising methodology and advantages and special considerations for incorporating mHealth tools. A comprehensive review of the state of the art on mHealth applications and services was presented in [142]. This review surveyed the most important studies and presented a comprehensive analysis of the top and novel applications and services in the industry considering the approaches of the United States and European Union. A study on national domain and quality was conducted and provided an overview of the US population health, access to care, status of healthcare quality and disparities in care experienced by different socioeconomic, racial and ethnic groups [143]. The author in [144] reviewed different technologies and technological advances applicable to oncology care through websites, books, magazine articles, online product-specific information and peer-reviewed guidelines and studies. The authors in [145] provided a systematic review for health smart homes and home-based consumer health literature from indexed repositories for healthcare and technology disciplines and categorized the included articles according to an evidence-based public health typology.

Telemedicine architecture

This category contained eight articles within three subsections of Tiers 1–3) as explained as follows.

Tier 3 A healthcare provider in MIs generally allows medical professionals to monitor and analyse vital signs in real time and provide patients with appropriate healthcare services. It can also manage, organise and support professionals in telemedicine. Generally, a healthcare provider comprises a medical institution’s server, patient history and database and service generation [146]. This subsection contains two articles. An innovative architecture for collecting and accessing large amount of data generated by medical sensor networks was proposed in [147]. This architecture overcomes all the aforementioned challenges and facilitates easy information sharing between healthcare professionals in normal and emergency situations. Furthermore, this study proposed an effective and flexible security mechanism that guarantees confidentiality, integrity and fine-grained access control to outsourced medical data. This mechanism relies on Ciphertext-Policy Attribute-based Encryption to achieve high flexibility and performance. A machine-to-machine low-cost and secure communication system for e-Healthcare society was proposed in [148]. The system was designed to consider the psychological issues related to all actors in the e-Healthcare society, such as stress, anxiety and loneliness. To ensure data privacy, this mechanism involves intelligent authentication based on random distributive key management, electronic certificate distribution and modified Kerberos realm.

Tier 2 In Tier 1, patients can acquire their vital signs and send them to Tier 2 through small-area network protocols (e.g. Zigbee and Bluetooth) and WBAN [149]. The Tier 2 in telemedicine architecture is used to bridge sensor-based vital signs to remote stations by using interfaces, such as LAN, 3G, 4G or u-health [150]. This subsection contains only one article. A priority-based health data aggregation (PHDA) scheme was proposed in [151] with privacy preservation for cloud-assisted WBANs to improve the aggregation efficiency amongst various types of health data. The study explored social spots to aid forward health data and enable patients to select the optimal relay according to their social ties. The security analysis in this study demonstrated that the PHDA could achieve identity and data privacy preservation while resisting forgery attacks.

Tier 1 The first tier in telemedicine architecture is represented by Tier 1, which comprises tiny intelligent wireless sensors responsible for gathering the vital signs of patients and transmitting vital information to Tier 2 through WBANs [152]. This subsection contained five articles. The authors in [153] implemented TinyECC, which is a public key algorithm with optimisations for resource-constrained hardware platforms, to secure the wireless communication between sensor nodes and investigate the feasibility of using TinyECC in a real-time sensor network. A system for secure logging of events in sensor networks was introduced in [154] by gathering all information at one central point in a secure and reliable manner. The system guarantees the chronological order of logged events sent by the different sensors. It also permits one to detect the modification, deletion and addition of logged data and design a prototype of the gateway sensor on an FPGA platform. In [155], a security protocol for ultra-wideband impulse radios was proposed based on distance bounding; this protocol provides multiple levels of security, including encryption and a distance bounding test, to prevent long-distance attacks used in WBANs for medical devices where security is imperative. The authors in [156] proposed a priority-based compressed data aggregation scheme with integrity preservation to improve the aggregation efficiency of different types of health data in medical wireless sensor networks. This study used compressed sensing to reduce the communication overhead and minimise power consumption. Then, the compressed data were encrypted, and integrity was protected by a cryptographic hash algorithm to preserve data integrity. A comparative performance analysis between the IEEE 802.15.6-based communication system using UP and the IEEE 802.15.4-based communication system was conducted in [157] to show the effectiveness of the IEEE 802.15.6 in home monitoring of an individual cardiac patient in WBANs.

Critical review and analysis

Overall, the aforementioned studies within Tiers 1 and 2 (client side) have not presented solutions for the security and privacy of sensor-based mHealth related with authentication issues. Thus, adding another layer to review the security and privacy of sensor-based smartphone authentication to gain the bifacial of these studies and fully adopt them within the client side in telemedicine environment is necessary. The new mapping of a multilayer systematic review allows interring additional knowledge of sensor-based smartphone authentication within the second-layer studies, which include a wide area of authentication contributions. This study aims to highlight completed research, such as the aforementioned articles that were conducted to address new and authentication technologies, delineate research scene from the literature to a coherent taxonomy and discover the key aspects that describe this developing research direction, which will be proposed and described in detail.

Second Layer: systematic review for security and privacy of sensor-based smartphone authentication

In this layer, sensor-based authentication techniques are newly introduced in the academic literature. The keyword used in this layer is ‘sensor-based mobile’, which excludes any other type of non-smartphone devices. The English-language literature is a limitation of this scope. Therefore, all authentication-related areas, including the general category of password and sensor types, were considered. In addition, colour and colour gradients were used as keywords to secure information related to sensor-based mobile phones. The following three digital databases were used to conduct the search for target articles:

1. ScienceDirect database, which offers access to science and technical journal articles;
2. IEEE Xplore library of technical literature in engineering and technology;
3. WoS service, an indexing database that covers different academic disciplines; and
4. SciVerse Scopus, an indexing database that covers different academic disciplines.

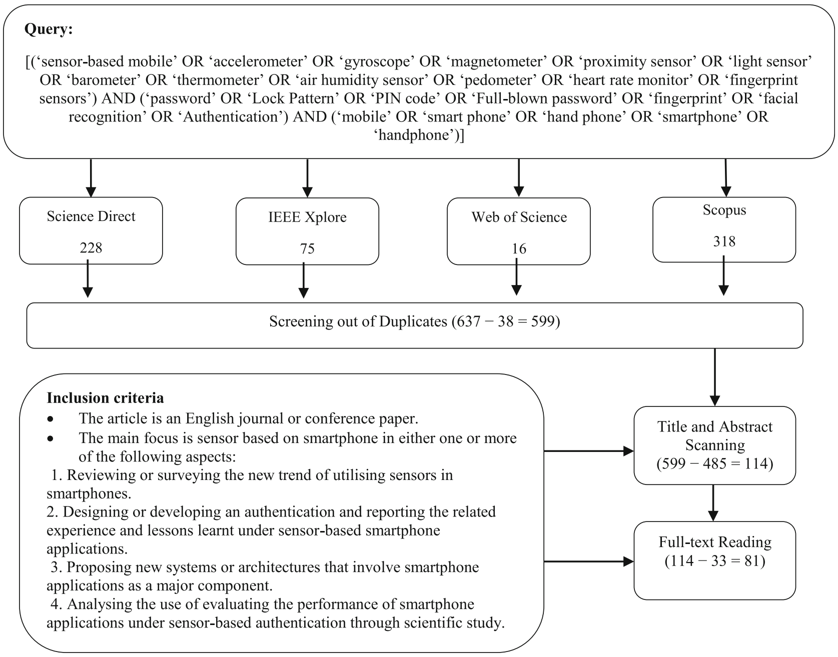
The sources of this layer were carefully screened from the literature sources. The study period was 10 years, from 2007 to 2017. The articles were screened and filtered to exclude duplicates and those unrelated to this layer. Then, full-text reading was performed. The search was conducted on August 2017 via the search boxes of the ScienceDirect and IEEE Xplore databases.

We used a combination of groups of keywords. The first group included ‘sensor-based mobile’, ‘accelerometer’, ‘gyroscope’, ‘magnetometer’, ‘proximity sensor’, ‘light sensor’, ‘barometer’, ‘thermometer’, ‘air humidity sensor’, ‘pedometer’, ‘heart rate monitor’ and ‘fingerprint sensors’; these keywords were combined by the ‘OR’ operator. The second group included ‘password’, ‘lock pattern’, ‘PIN code’, ‘full-blown password’, ‘fingerprint’, ‘facial recognition’ and ‘authentication’; these keywords were combined by the ‘OR’ operator. The third group included ‘mobile’, ‘smartphone’, ‘hand phone’, ‘smart phone’ and ‘handphone’; these keywords were combined by the ‘OR’ operator. The three groups were combined by the ‘AND’ operator. Figure 5 shows the query. The options provided by each database were considered. Books, reports and contents that appeared in the search results were excluded [158]. However, the latest journal articles and conferences were adopted, and the most relevant were considered for our study. The criteria described in Fig. 5 were followed and applied to each article. Every article that satisfied the criteria listed in Fig. 5 was included. A plan was devised to cover the research in four categories to protect the privacy of smartphones that operate on sensors. Google Scholar was used to obtain the views and trends in the literature entitled ‘ACCessory: Password Inference using Accelerometers on Smartphones’. Duplicates were initially removed, and the articles that did not satisfy the criteria of eligibility within the stages of screening and filtering were then excluded. The exclusion criteria included non-English articles and articles that focused on a specific aspect of smartphones that do not use any type of sensor in authorisation. All included articles from different sources were used to further improve our investigation. A few full-content readings led to a substantial gathering of features and remarks on these works and resulted in a refined scientific categorisation of articles. All remarks were excluded from the text (contingent upon each writer’s favoured style, either in hard or delicate duplicate renditions). The principal discoveries were compressed, organised and presented. The sets of relevant information (including a full list of articles, their respective source databases, summary and description tables, categorisation tables, purposes, review sources, target platforms, audience and various related figures) were saved in Word and Excel formats. These datasets are shown in the Supplementary Material section. Figure 6 presents the number of articles according to index source and type in the second layer.

Result

The first result from the query search showed $n = 637$ articles published in 2007–2017; particularly, 228, 75, 16 and 318 articles were from Science Direct, IEEE Xplore, WoS and Scopus. A total of 5.96% ($n =$ 38/637) of duplicated articles were found in the four libraries. In the second set of results, 80.96% ($n =$ 485/599) of the articles were excluded after filtering the titles and abstracts, obtaining only 19.03% ($n = 114/599$) of the articles. Reading the entire text resulted in the exclusion of 28.94% ($n = 33/114$) of the articles, and only 71.05% ($n = 81/114$) articles were obtained. Then, the articles were carefully read in the final set of a general research map conducted on this subject. The number of articles is shown according to index source and article type. Most of the selected articles (27) were from the United States, whereas the other articles were from 18 different countries, as shown in Fig. 8. Our analysis results show the three main research categories, namely, defence, attack and others. The ‘defence’ group included research articles that focus on defending smartphones from attackers, whereas the ‘attack’ group included those that utilise smartphone sensors to attack the phone. The ‘others’ group included articles that discuss the development of defence. However, the type of sensors used in the development is unclear.

Amongst the 81 articles, 86.41% ($n = 70/81$) represents the defence area, where sensor-based smartphones were used via an orientation sensor to authenticate the user; this authentication technique is called behaviour or gait authentication, as

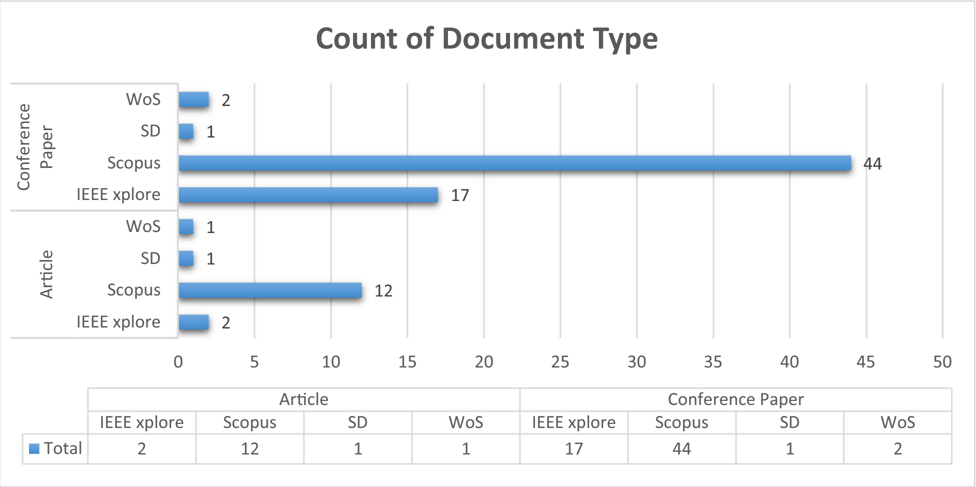

Query:
Science Direct
228
IEEE Xplore
75
Web of Science
16
Scopus
318
Screening out of Duplicates (637 − 38 = 599)
Title and Abstract Scanning (599 − 485 = 114)
Full-text Reading (114 − 33 = 81)
Inclusion criteria

[(‘sensor-based mobile’ OR ‘accelerometer’ OR ‘gyroscope’ OR ‘magnetometer’ OR ‘proximity sensor’ OR ‘light sensor’ OR ‘barometer’ OR ‘thermometer’ OR ‘air humidity sensor’ OR ‘pedometer’ OR ‘heart rate monitor’ OR ‘fingerprint sensors’) AND (‘password’ OR ‘Lock Pattern’ OR ‘PIN code’ OR ‘Full-blown password’ OR ‘fingerprint’ OR ‘facial recognition’ OR ‘Authentication’) AND (‘mobile’ OR ‘smart phone’ OR ‘hand phone’ OR ‘smartphone’ OR ‘handphone’)]

- The article is an English journal or conference paper.
- The main focus is sensor based on smartphone in either one or more of the following aspects:

1. Reviewing or surveying the new trend of utilising sensors in smartphones.
2. Designing or developing an authentication and reporting the related experience and lessons learnt under sensor-based smartphone applications.
3. Proposing new systems or architectures that involve smartphone applications as a major component.
4. Analysing the use of evaluating the performance of smartphone applications under sensor-based authentication through scientific study.

Fig. 5 Second-layer flowchart of study selection, including search query and inclusion criteria



	Article				Conference Paper			
	IEEE xplore	Scopus	SD	WoS	IEEE xplore	Scopus	SD	WoS
■ Total	2	12	1	1	17	44	1	2

Fig. 6 Number of articles according to index source and type in the second layer

shown in Figs. 7 and 8. A total of 7.40% ($n = 6/81$) articles were attack articles, which were not intensively included in our literature analysis. The category 'others' was represented by 8.64% ($n = 7/81$) of the articles. Figure 9 presents the literature taxonomy.

Figure 10 shows the relationship between the years of publication and the number of articles obtained during our study. The chart of the studies and the preparation within our research area are contrasting and thus should be explained. The observations related to this objective should be considered and expounded.

The IEEE, Science Direct, WoS and Scopus search engines were targeted because they were the most reliable sources. The second layer is based on 81 articles from the following sources: IEEE (9 articles), WoS (3 articles), Science Direct (2 articles) and Scopus (56 articles). Many studies, which include all the documentation related to the sensors in the smartphone, were provided through these sources by international journals to aid users maintain safe and convenient devices.

Defence

We found the articles on smartphone protection by authentication using the sensors in those devices. The largest component includes using the orientation sensor, which comprises many sensors, such as the accelerometer and gyroscope. The other component is the fingerprint sensor, in which related articles suggest using a fingerprint to obtain smartphone authorisation. The third set of articles discusses the use of a touchscreen sensor. These articles indicate the pattern for obtaining authentication when using a password to access mobile data. The last set of articles in the defence group presents the camera sensor.

The articles were divided into four groups according to the type of sensor used. The orientation sensor accounts for the largest number of articles. A total of 35.71% ($n = 25/70$) articles on the orientation sensor developed based on gait authentication were obtained and divided into the following research strategies: cryptosystem with a fuzzy scheme that used

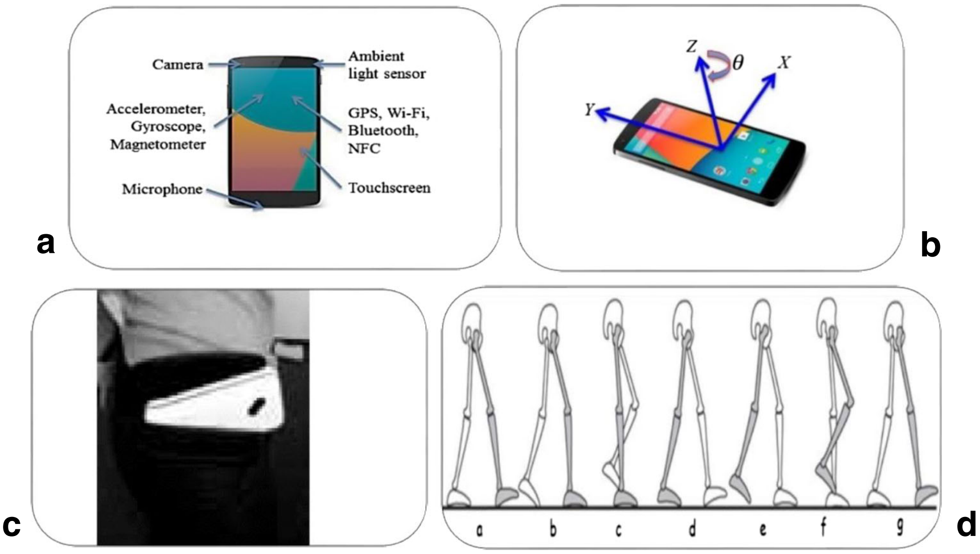

Camera
Ambient light sensor
Accelerometer, Gyroscope, Magnetometer
GPS, Wi-Fi, Bluetooth, NFC
Microphone
Touchscreen
a
Z
θ
X
Y
b
c
a
b
c
d
e
f
g
d

Fig. 7 (**a**) Sensors, (**b**) axes, (**c**) position of phone during gait recognition and (**d**) gait cycle [116, 118, 123]

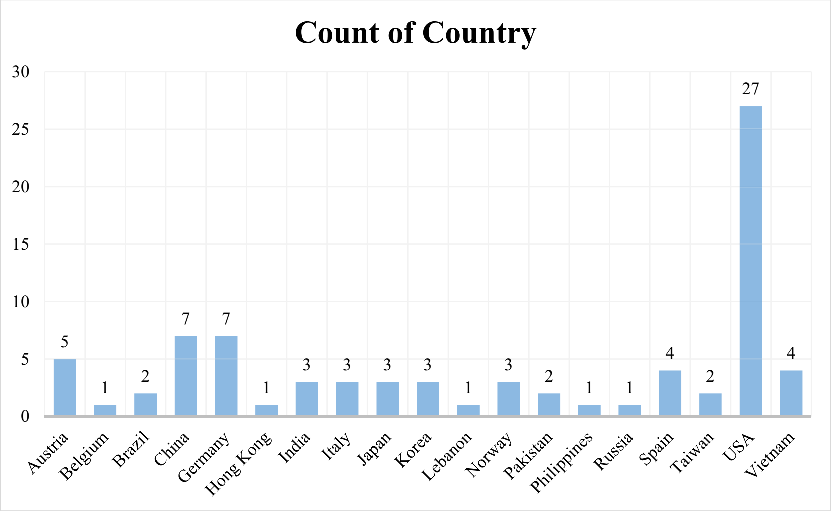


Fig. 8 Total number of articles according to country in the second layer

cryptography and fuzzy logic to produce authentication for users. This strategy utilises human walking style, which is used as an authentication pattern to recognise whether the person is the authorised user. In this case, the developers use accelerometer data in the classification and/or recognition process.

The defence group was further classified into fingerprint sensor content with 5.71% (*n* = 4/70) of the articles [125], [159–161]. The touchscreen sensor has 5.71% (*n* = *4/70*) articles. Half of these articles [50% (*n* = 2/4)] use hybrid authentication [162, 163], whereas the other half [50% (*n* = 2/4)] use

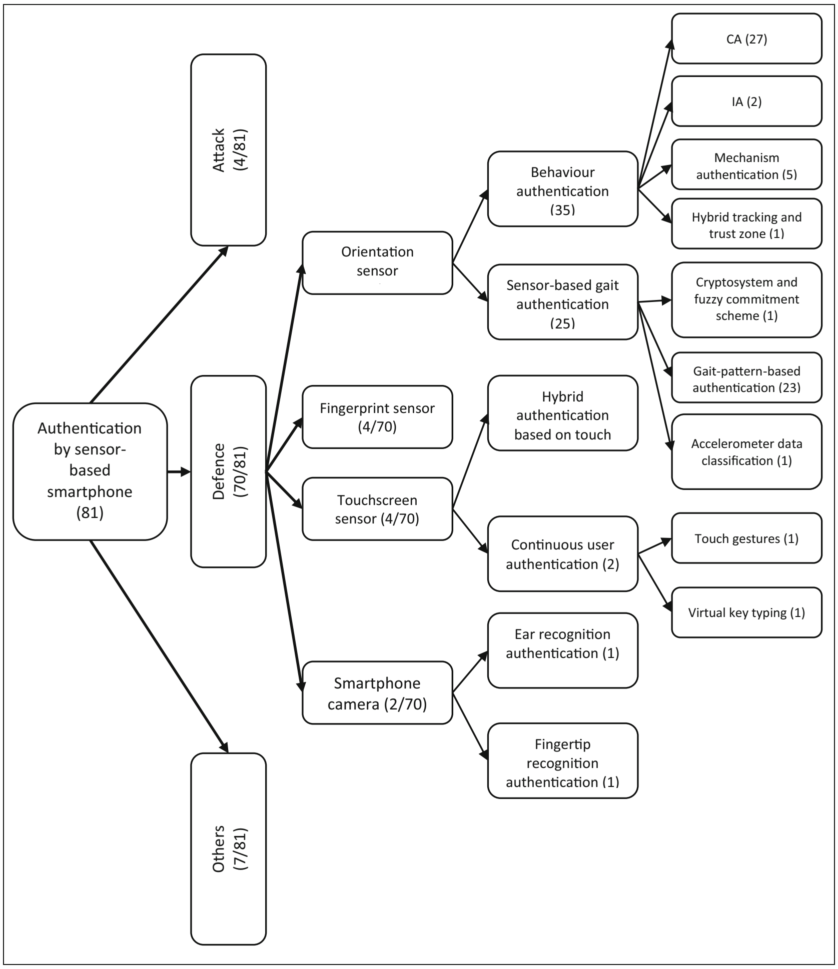

Authentication by sensor-based smartphone (81)
Attack (4/81)
Defence (70/81)
Others (7/81)
Orientation sensor
Fingerprint sensor (4/70)
Touchscreen sensor (4/70)
Smartphone camera (2/70)
Behaviour authentication (35)
Sensor-based gait authentication (25)
Hybrid authentication based on touch
Continuous user authentication (2)
Ear recognition authentication (1)
Fingertip recognition authentication (1)
CA (27)
IA (2)
Mechanism authentication (5)
Hybrid tracking and trust zone (1)
Cryptosystem and fuzzy commitment scheme (1)
Gait-pattern-based authentication (23)
Accelerometer data classification (1)
Touch gestures (1)
Virtual key typing (1)

Fig. 9 Second-layer taxonomy of research literature on sensor-based smartphone authentication

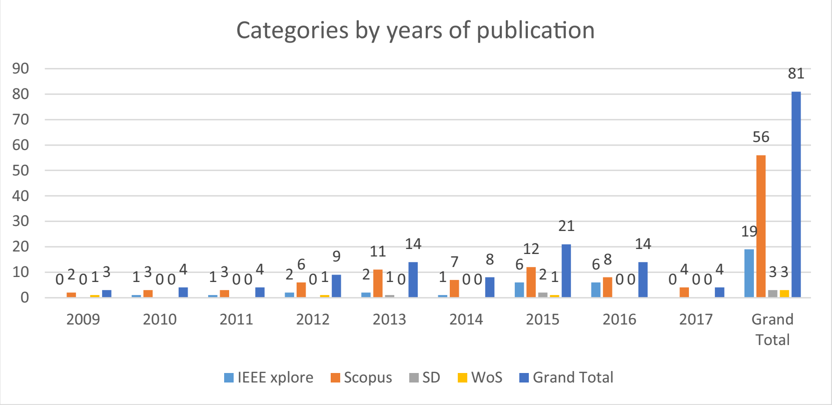


Fig. 10 Number of included articles in different categories by year of publication in the second layer

CA [164, 165]. CA contains two articles; the first article uses touch gestures and virtual key typing. In addition, the defence group has 2.85% ($n = 2/70$) of the articles with two different methods, namely, ear and fingertip recognition authentication.

Orientation Sensor The largest number of articles is about the use of orientation sensor, which includes many sensors, such as the accelerometer and gyroscope. In this category, 50% ($n = 35/70$) of the articles account for behaviour authentication, and the sensor-based gait authentication accounts for 35.71% ($n = 25/70$) of the articles. The details of each category are presented as follows.

Behaviour Authentication Behavioural biometrics is defined by the measure of distinctive and commensurable patterns of human actions. The term appears differently in relation to physical biometrics, which includes intrinsic human qualities, such as patterns of fingers or iris. Biometric confirmation techniques of behaviour include pressure dynamics, analysis of gait and signature, voice ID, mouse use features and cognitive biometrics. Biometrics is used for safe authentication in government facilities, corporations, financial institutions, retail points of sale and in many other environments.

The articles in the behaviour authentication group were divided into the following four parts: CA with 77.14% ($n = 27/35$) of the articles, IA with 5.71% ($n = 2/35$) of the articles, mechanism authentication with 14.28% ($n = 5/35$) of the articles and hybrid tracking and trust zone with 2.85% ($n = 1/35$) of the articles. Some studies focus on hand gestures for signature [108]. Figure 11 presents the behavioural authentication [113, 167], gait recognition of CA [115, 116] and behavioural biometrics [167].

Sensor-Based Gait Authentication Biometric authentication depends on a person's gait, which represents the person's motion when using a smartphone with accelerometer sensor to determine the authentication of this device. The sensor-based gait authentication includes 35.71% ($n = 25/70$) of the articles under the defence group; it was divided into cryptosystem and fuzzy commitment scheme with 4% ($n = 1/25$) of the articles, gait-pattern-based authentication with 92% ($n = 23/25$) and accelerometer data classification with 4% ($n = 1/25$) [168].

Fingerprint Sensor In this article category, the defence group accounts for 5.71% (*n = 4/70*) of the articles. Some articles focused on hazard-based verification systems in setting mobile phones. These systems failed to provide solid gadget-related data that could be utilised for the hazard examination process [125]. Another article proposed the use of finger gestures as a characteristic in a range of unique fingerprint sensors, which was limited, conservative and cost-effective; the effectiveness of a specialised feature set was analysed [159, 160]. Any threat that could occur was determined while identifying the necessary steps to address security vulnerability [161].

Touchscreen Sensor In this article category, the defence group accounts for 5.71% ($n = 4/70$) of the articles. The touchscreen sensor uses the touchscreen to obtain data for the authentication process, which was divided into two types, that is, CA

Fig. 11 Using a magnet to perform 3D magnetic signature on the space around a device [166]

with 50% (n = 2/4) of the articles and hybrid authentication with 50% (n = 2/4). The CA contents have two types, namely, touch gestures and virtual key typing. Some articles proposed the use of typing authentication and protection, which is a virtual key writing-based verification framework for mobile phones [165]. The proposed system considers miniaturised scale developments of a phone and that of the client's finger whilst signing or writing on the touchscreen [164]. Another article on hybrid authentication system included CA and IA based on touch gestures [162].

Camera Sensor In this article category, the defence group represents 2.85% (n = 2/70) of the articles. The camera sensor utilises the camera to obtain information with a specific goal for the verification procedure, which was divided into two types, that is, ear recognition authentication with 50% (n = 1/2) of the articles and fingertip recognition with 50% (n = 1/2). Some articles showed a picture of the ear using surface and shape data, which considered ear recognition [169]. Another article utilised a mobile phone's camera to detect the fingertip development, move the cursor on the screen and execute clicks by detecting click movements [111].

Attack

Articles regarding attack on a smartphone were obtained by using sensors or gaps in these devices. This category accounts for 4.93% (n = *4/81*) of the articles. In these articles, display TapLock was used as a mobile phone secret key framework that enables finger tapping on capacitive touchscreens for expansion whilst sustaining surfing assaults (the secret key contribution via a user can be effectively identified through an observer over the user's shoulder) [170]. An attack has other genuine ramifications. The touchscreen is not the only primary keystroke input gadget but is the principal input gadget for most client cooperation (a reasonable special case includes sound-perceiving applications), which can supplant the console and mouse [171]. The experimental results from user authentication utilised touch operational features, and some features were extracted from an accelerometer [172].

Others

This category accounts for 8.64% (n = 7/81) of the articles, which were beyond the scope or were not included in the previous categories, such as articles that only reviewed sensors.

Discussion

This study aims to update the substructure of smartphone sensors constantly on the basis of authentication techniques, as well as the focus of the research trends. The results of the applications during the comprehensive survey are ignored, and the authentication techniques are considered. In addition, we provide the taxonomy of the articles on this topic. The development of the taxonomy based on the literature can provide several benefits. The taxonomy of published works imposes organisation on a set of publications. Numerous publications on the topic may be dominated by a new researcher who is interested in the trend of authentication with the absence of an organisational structure and fails to gain an appropriate sense of the actual activities in this field.

Various articles consider the topic from an introductory perspective, whereas other articles examine a selected number of existing applications and some actual applications involved in the development. Taxonomy is provided to sort out the various activities and works into a meaningful, coherent and manageable framework that is collected from the literature. The taxonomy can also provide researchers with novel ideas on several aspects of the topic.

Motivations

Authentication used in smartphones is a promising research area. This section presents some of the characteristics of the literature, which we have grouped into categories according to specific benefits based on references for further discussion, as shown in Fig. 12.

Benefits related to usability of smartphones

Smartphones are in our work and home environments ubiquitously. Individuals generally store their delicate and private data on their phones. Thus, verifying the legitimate users of a phone and blocking impostors are crucial [173, 174]. Omnipresent mobile devices, such as smartphones and tablets, are frequently vulnerable to unauthorised access because users do not utilise passwords due to inconvenience [116, 175]. Mobile devices, such as smartphones, tablets and portable computers, have rapidly spread over the last decade. Given that smartphones store a large amount of important private information, user authentication is increasingly necessary to prevent attacks, such as motion-based inference attack, by illegal users [171, 172, 176, 177]. A mobile device is a dominant model that becomes interactive between a human and a computer.

The theory of around-device interaction (ADI) in the field of human–computer interaction has recently gained attention. ADI covers beyond the peripheral area of a device and suggests a touchless user interface as an alternative to the classic data-entry methods [178]. Approximately more than five billion devices were used worldwide in 2015 [179]. Many people use smartphones to access their bank accounts and social networks and store their personal information. These devices, particularly their authentication mechanisms, may not be sufficiently safe [180]. The improvement of smartphones

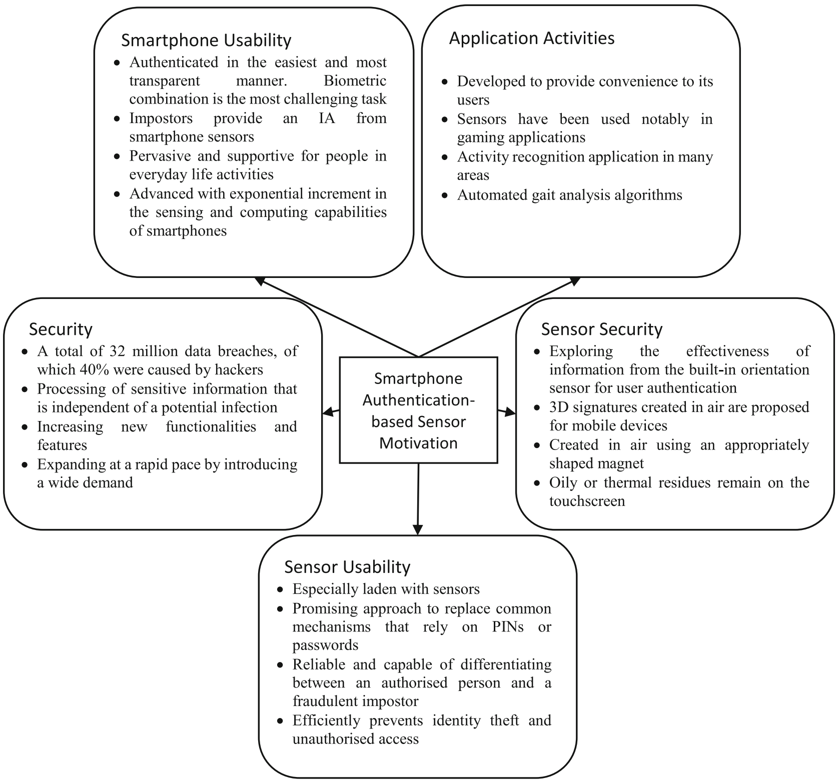

Smartphone Usability
• Authenticated in the easiest and most transparent manner. Biometric combination is the most challenging task
• Impostors provide an IA from smartphone sensors
• Pervasive and supportive for people in everyday life activities
• Advanced with exponential increment in the sensing and computing capabilities of smartphones
Application Activities
• Developed to provide convenience to its users
• Sensors have been used notably in gaming applications
• Activity recognition application in many areas
• Automated gait analysis algorithms
Security
• A total of 32 million data breaches, of which 40% were caused by hackers
• Processing of sensitive information that is independent of a potential infection
• Increasing new functionalities and features
• Expanding at a rapid pace by introducing a wide demand
Smartphone Authentication-based Sensor Motivation
Sensor Security
• Exploring the effectiveness of information from the built-in orientation sensor for user authentication
• 3D signatures created in air are proposed for mobile devices
• Created in air using an appropriately shaped magnet
• Oily or thermal residues remain on the touchscreen
Sensor Usability
• Especially laden with sensors
• Promising approach to replace common mechanisms that rely on PINs or passwords
• Reliable and capable of differentiating between an authorised person and a fraudulent impostor
• Efficiently prevents identity theft and unauthorised access

Fig. 12 Benefit categories for smartphone authentication based on sensor

continually advances, and new features are rapidly included in the device. These features include high-quality cameras, UMTS antennas and calendars, thereby simultaneously increasing the number of applications that can be executed on a smartphone and the stored amount of sensitive data [127]. The use of these devices has increased over the past years as evidenced by the growth in their sales. Currently, many services use these devices to access social networks and bank accounts and store personal information [127]. Mobile devices constantly enter the lives of people; everyone possesses one or more smartphones (e.g. iPhone, Android and tablet). Identity verification is required in many common activities, and most people want to be authenticated in the easiest and most transparent manner, without the need to remember a PIN [119, 181]. Mobile devices currently contain an assortment of personal or business-related information that is secured from unauthorised access. Smartphones are increasingly utilised similar to PC platforms to access personal information; thus, the request for secure and usable authentication techniques for continuous protection is emphasised [177]. The owners of such devices ought to utilise an unlock pattern or passcode to secure such important resources. However, given that these procedures are considered disturbing obstructions, locked devices are not standard [126].

Mobile devices are considered fundamental devices in our daily lives [182]. Smartphones are context-aware devices that supply a convincing platform for omnipresent computing and support users in fulfilling many of their routine tasks anytime and anywhere, such as receiving and sending emails. The nature of tasks relative to these devices has developed with an exponential increment in the sensing and computing smartphone capabilities [183]. Smartphones have become a part of modern life. Currently, approximately 46% of the adult population in the US have smartphones. Although no accurate statistics is available on blind or disabled individuals as smartphone users, the assumption that the number increases is reasonable. This technological revolution has attracted thousands of disabled users, including the visually impaired [184]. Mobile devices have become popular and support people in their daily activities. Smartphones are available in the market as a wide range of portable and wearable devices [185].

People can go anywhere at any time with their smartphones. The important features of mobile devices include their diversity in sizes, styles and input controls (i.e. displays) and capability to store a substantial volume of data, including sensitive personal information, such as bank accounts or emails [185]. Personal and sensitive data, such as project information, emails and business contacts, are often included in a smartphone business scenario. However, in a private environment, the amount of sensitive data is high. In a special environment, the sensitive data stored on smartphone devices are of high quantity; thus, the protection of those data becomes increasingly important [186]. Mobile devices that use the Android operating system are used as a platform for the WISDM project, which is simple, open and free. Thus, this operating system is expected to dominate the smartphone market [187]. These devices offer innovative interaction models due to their low price and simplicity of use [179]. The adoption of smartphones rapidly increases yearly worldwide. The smartphone sales in the first quarter of 2013 reached 225 million, surpassing all previous sales figures. Moreover, the number of smartphones sold exceeded one billion units in 2014. In addition to this sales increase, the number of services (i.e. personal and corporate) available from these devices also increase [127].

Benefits related to security impact on smartphones

Mobile phones have received extensive research attention; numerous attack vectors and countermeasure solutions have also been explored [171]. Feng (2014) stated that an increasing amount of sensitive information, such as transaction information for bank accounts, credit cards and trade secrets, passes through mobile digital devices. He also identified new privacy and security issues. In January 2012, 32 million data breaches were reported, of which 40% were caused by hackers [120]. In response to these astonishingly large numbers, sensitive information should be processed through an approach that is independent of a potentially infected operating system whilst monitoring physical events of the device to detect possible physical unauthorised use. Previous mobile user authentication technologies, such as passwords, only offer protections at the login point [120]. The widespread use of small mobile computing devices, such as smartphones, increases the need to protect these devices and the sensitive data they contain against unauthorised use [95, 188, 189]. New features and functionalities in smartphones have led to an increased need to raise the safety level of these devices [165, 182]. The world of smartphones has rapidly grown; consequently, the demand for Internet access, applications and services has shown a remarkable increase. Therefore, smartphones are exposed to many threats, which include the thief's ability to authenticate due to the easy identification of the PIN or password to access personal data [119, 164, 175]. In addition to privacy issues related to stolen or counterfeit biometrics, the burden of remembering passwords has led to a future idea of authentication systems. An attacker may be an unfamiliar person who steals or finds a mobile device. However, a family member, colleague or close friend may also be the attacker [171, 190]. New systems are expected to be transparent, and minimum user participation requires IA [112, 164, 169, 191, 192]. Biometrics is used in the authentication of smartphones to unlock the device at the start up, resulting in portable devices with only login authentication that are vulnerable to data theft [118, 183]. Display lock and release are the main features of modern phones to prevent unexpected operations and ensure security of personal data. Specific reaction, movement, security code or fingerprints must be provided when the mobile is locked [160, 193].

Benefits related to sensor authentication usability

Varied and powerful sensors exist during the period of rapid development of mobile devices. The latest generation of smartphones is particularly loaded with sensors, including GPS, vision cameras, microphones, light, smart thermometer, compasses and acceleration sensors [187]. Modern mobile devices are characterised by numerous sensors that enable a large area of interactions. However, some of these sensors have weaknesses that cause access to user input [194]. Many modern mobile sensors include the extraction of required parameters within the scope of their uses [195]. Authentication solutions based on biometrics are a promising approach to replace common mechanisms that rely on PINs or passwords, which are often perceived as inconvenient by users [95]. Biometrics is considered to be more reliable than non-biometric methods, which are used to prove the owner's identity by merely confirming his possession through a particular confidentiality or the user's knowledge. Biometrics has two types, namely, behavioural and physiological. These methods can effectively prevent identity theft and unauthorised access to any of the mobile terminal resources [95, 107, 108, 196]. Smartphone devices that support biometrics are available from many of the major service providers, thereby decreasing the price of biometrics sensors [108, 122, 196]. The considerable potential of non-obtrusive gait biometrics measurements is shown by the accelerometers directly embedded in the characteristic motion of users [197–199]. Smartphone users have appropriate authentication methods in addition to the accelerometer in these devices [185]. Accelerometers have become a highly important tool because of their effectiveness in activity recognition. They are inexpensive, small, efficient and only require minimal energy; they are also insensitive to environmental conditions [123, 180, 197, 200–203]. Although most smartphones are equipped with a front-facing camera, facial recognition, a popular biometric authentication technique, is rarely used in practice for device unlock or website/application login in smartphones [107, 173, 204]. In addition, Muaaz and Mayrhofer (2016) suggested that gait authentication using a mobile phone based on accelerometer sensor offers an unobtrusive, user friendly and periodic manner of authenticating individuals to their smartphones [205–207].

Benefits related to sensor security

The possibility of losing mobile phones leads to security threats on one's personal data [119]. Thus, the effectiveness of information from the built-in orientation sensor for user authentication has been explored [175]. The potential of smartphone sensors (e.g. accelerometers and gyroscopes) has been widely explored in gait-based authentication [208]. Ketabdar (2012) proposed a new authentication method based on 3D signature for mobile devices. The 3D signature is manually created in air using an appropriately shaped magnet (a rod or ring) [166]. This method is based on influencing the compass or accelerometer sensor embedded in the new generation of mobile devices [166, 201]. Each user of these smartphones has his own style when clicking the touchscreens [113]. Personal patterns are reflected on the intensity and difference in rhythm and the corner of the preferred applied force. User behaviour is effectively captured because smartphones are equipped with different sensors, such as gyroscopes, accelerometers and touchscreens [162, 163]. However, Ling (2016) suggested that oily or thermal residues remain on the touchscreen, thereby leaving a visible effect that can be detected by the naked eye. Thus, the movement of the finger can be analysed, which can lead to an attack depending on the motion sensor [111]. Biometric gait authentication using accelerometer sensors based on personal mobile device offers a user friendly, unobtrusive and periodic approach in authenticating individuals [115, 168, 209, 210]. Given that gait is biologically less biometric and unobtrusive, which are major advantages over other biometrics, gait considerably differs from other biometrics because it does not require any physical connection. Through a remote camera or some sensors, the moment can be easily captured as long as the device is connected to the person. Biometric gait can also be used for documentation purposes in mobile devices [196]. The system becomes multilayer for authentication and utilises the user gait pattern and location traceability for authentication without creating noise. The system also interacts with the user of the device when it provides the password, which comprises a series of emotions and cannot be used in the device if any defect exists in the location traces or gait pattern. If the user fails to provide an accurate behaviour, then the system asks the user regarding the description of the image context that has been previously stored for the user [211].

Many attempts have been made to use sensor noise in identifying and authenticating a device. Most of these developments have occurred in smartphone sensors, such as gyroscope and light sensors. The implication of sensor fingerprint isolation is that any third party using multiple sources may effectively track user movements without using cookies [161]. The accelerometer and gyro sensors record the displacement and rotation of the mobile device during the gesture. A sensor fingerprint is generated for the user when the two sensors are combined. Every time the user performs one of the unlocking gestures, the device is slightly displaced and rotated. The displacement and rotation of the device is evidently reflected in the accelerometer and gyro sensor data [92]. Wong suggested that the fingerprint sensor, which is installed in many electronic gadgets ranging from portable mobile devices to high-end PCs, has become increasingly popular [159]. Apple's touch ID sensor enables fingerprinting for iPhone 5 s or 6/6 Plus or other iOS devices; however, this fingerprint sensor is currently unavailable on most smartphones. Recent research reveals that conventional smartphone password systems are unsafe [170].

Benefits related to application activities

Mobile applications related to online financial transactions have been developed to provide convenience to users [107]. Smartphone motion sensors measure the movement and orientation of the phone in space, and sensors have been used in a wide variety of tasks, notably in gaming applications [194]. Activity recognition has become a key research field due to its application in many different areas, such as healthcare, fitness, industrial application, security and entertainment. [200]. Accelerometer data are applied to many types of automated gait analysis algorithms [191, 198]. Mobile phones have become immensely popular in recent years. Location-based services have attracted user interests with many popular applications on mobile phones. These applications provide access control, authentication, advertisements and other important functions based on the location of mobile users [212]. Mobile applications also effectively allow sensitive processes to be operated in this mode, such that they are secure from any malware that may be present in the normal world [120]. In the software-based authentication category, knowledge-based authentication systems often fulfil limited training, rapid process of authentication and global use. However, the effectiveness of the present authentication systems in removing forbidden access and reducing faulty access denial remains unclear. Smartphone devices can obtain a perfect reply to those questions posed by sensors built into those devices. Smartphones can also be used to gather different attributes of a person's behaviour or nature because they have many built-in sensors. Most people have habits that are influenced by their behaviour depending on the environment [211].

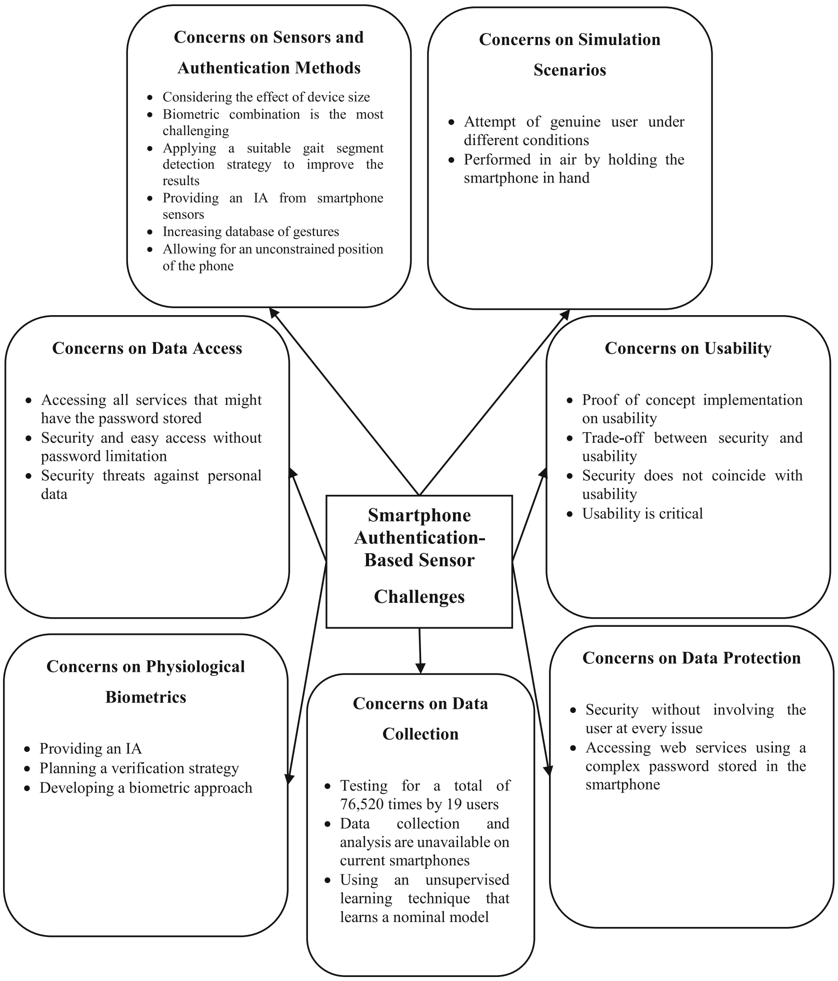
Challenges

Sensor-based smartphones that verify client access to the gadget do not effectively provide sufficient information guarantee. In the academic literature, researchers have reported numerous challenges related to sensors and their utilisation in security. The main challenges are categorised and reported in the following subsections alongside their references. Figure 13 depicts the main challenges reported in the academic literature related to the reviewed articles.

Concerns on data access

Data access is one of the main challenges in authentication. In 2013, explicit authentication was ineffective for devices that relied upon it. When a mobile phone is stolen, the thief gains access to important and personal information and can use services provided by the device based on the stored password.

Fig. 13 Challenges for sensor-based smartphone authentication


Concerns on Sensors and Authentication Methods
Considering the effect of device size
Biometric combination is the most challenging
Applying a suitable gait segment detection strategy to improve the results
Providing an IA from smartphone sensors
Increasing database of gestures
Allowing for an unconstrained position of the phone
Concerns on Simulation Scenarios
Attempt of genuine user under different conditions
Performed in air by holding the smartphone in hand
Concerns on Data Access
Accessing all services that might have the password stored
Security and easy access without password limitation
Security threats against personal data
Concerns on Usability
Proof of concept implementation on usability
Trade-off between security and usability
Security does not coincide with usability
Usability is critical
Smartphone Authentication-Based Sensor Challenges
Concerns on Physiological Biometrics
Providing an IA
Planning a verification strategy
Developing a biometric approach
Concerns on Data Collection
Testing for a total of 76,520 times by 19 users
Data collection and analysis are unavailable on current smartphones
Using an unsupervised learning technique that learns a nominal model
Concerns on Data Protection
Security without involving the user at every issue
Accessing web services using a complex password stored in the smartphone

In addition, the medical files of the elderly and the disabled can be easily accessed without the complexities of passwords; thus, the security of their devices should be ensured [119]. The coordinates of the position are used by dragging the image of the underlying context-aware system and excluding this information from a challenging classification scenario [213]. Personal data are subject to threats due to the possibility of theft or loss of a mobile device. More specifically, elderly and physically disabled users face difficulties in using screen patterns and entering PIN codes or cannot explicitly authenticate [119, 193]. They confirm that the data are secured and accessible on the smartphone by ensuring that the authorised user is the only person who can access the device [200].

Concerns on data protection

Security risks constantly emerge in relation to mobile devices, thereby posing a serious threat to the privacy of the users and the security of information when the device is lost or stolen [191]. Developing new authentication techniques require improved user friendly authentication process with less user involvement in addition to security and data protection [119].

In the web service module, complex passwords are stored in the smartphone with no requirement of repeated typing whenever needed [210]. However, in a trusted module, this particular device should be registered via a trusted module whenever a user attempts to access a web service [210]. The user authentication system allows the implicit identification module to retain the memory-based response and store it in a secure area; environmental and biometric measurements can also be used to verify security frequently [211]. This condition results in the following two potential issues. Firstly, passwords are the main sources of security sensitivity because they are overwhelmingly simple to reuse or guess and share with others and are susceptible to social engineering attacks. Secondly, the mobile system requires complete authentication to secure applications or data on a smartphone device, thereby resulting in serious usability issues [163]. Mobile applications should continue to operate and protect user privacy through a non-intrusive and easy Approac*h. mobile* computing platforms face these challenges that will extend to the next generation [214]. Manufacturers claim that the track pattern scheme may be unsafe. As the major drawback, the operation of a track pattern leaves an inerasable track on the screen. If the track is recovered, then the track pattern can be easily hacked [171, 195]. Another important aspect is payment processing, which faces new security challenges from these developments [120].

Concerns on usability of authentication

Conventional authentication mechanisms, including graphical or alphanumeric passwords, require the user to remember a unique combination of information [122, 215]; therefore, weak passcodes for ease of memorisation are selected [163, 191]. Consequently, evaluating a proof of concept implementation should be at an acceptable level of feasibility and usability in the direction of deploying such a system in real-world scenarios. A trade-off exists between usability and security [113, 125, 165]. The security measures required should be increased, thereby discovering novel safety methods [121, 180, 200]. Smartphones can contain large amounts of personal data but are often unsafe. Studies show that PIN locks are unsuitable for use and therefore experience low dependence (33% of users) [193]. Researchers have raised the challenge of implementing implicit documentation by building their own model, creating a user profile and ensuring that privacy is maintained for the purpose of data integrity, which is provided to the user at the same level of security for explicit authentication methods [119, 192]. Security is also one of the main research challenges in the production task.

Therefore, the developers of these programs must maintain the balance between ensuring the usability and all the security requirements of an organisation; the establishment of testing and environment is required to evaluate the performance of new safety mechanisms to improve the system usability [211]. A trade-off exists between the security and usability of smartphone devices. One-shot authentication solutions are defenceless against theft and loss [185], whereas spontaneous logouts or periodic authentication following intervals of idleness are likely to be counterproductive [165]. The created classifier is unsuitable, and the enrolment must be repeated, thereby resulting in low usability [206].

Behavioural studies have examined the biometrics of the mobile device motion to locate its possible authentication accuracy on an Android phone [167, 177] and the pressure cannot be easily imitated because it is equal to the tapping power divided by the touched area [163]. One of the challenges is that independent workers must be simultaneously adjusted. The main reason (in 74% of the cases) for this lack of security is a demand for fast access, that is, security does not coincide with usability in mobile devices [213]. An inconspicuous authentication system may supply a relatively high usability but has low security access control. For the smartphone device scope, usability is critical because users do not want to be cut off from their workflow to verify their identity [118, 165]; moreover, it covers various input situations with additional feature sets and increases the practice period [163]. Particularly, the gait, cannot be easily identified in different orientations, especially when this pattern is the most vulnerable to external conditions and influences [199]. Identification systems are applied in practical conditions but are considered to have unsteady quality or low smartphone gait verification accuracy rate [123, 196].

Concerns on data collection

One of the main challenges faced by developers in sensor-based authentication is data collection. As a result of the data collection, a dataset is developed to produce further testing and enhancements instead of spending a considerable amount of time, money and efforts for data collection. Such datasets can help improve the quality of a particular authentication technique. In a study by Sun and Wang [43], 19 users were tested in an authentication process for a total of 76.520 times. The devices required collection and data analysis on existing smartphones that were unavailable, thereby creating further burden on the developers [108]. Researchers that worked on orientation-based authentication have reported that the composite outputs of all three axes are more regular than those of individual axes [184]. They have also reported that the variance in gait period has slow and normal style of walking for 5 min [184, 206, 209]. Two issues raised by Shih and Shih [121] were as follows. The first issue pertains to the required investigation on the feasibility of using behavioural biometric accelerometer data collection and touchscreen fingertip on a smartphone (the data can help developers to design new smartphone authentication techniques); the second issue is related to the accuracy of the data during data acquisition (e.g. iris patterns or fingerprints) [112, 121, 162, 203]. The other issue is related to determining difficulties of the accurate dimension (e.g. walking towards high places). The errors in the division layer may spread to the next processing stages. Therefore, the system efficiency can be compromised. Finally, dissimilar gait signals extract reliable features that may result in problems [123].

Concerns on physiological biometrics

The challenges in authentication are related to behavioural biometrics for a number of reasons. Firstly, a person with complicated malicious intentions can easily capture a normal movement compared with a fingerprint or even a password [160]. Secondly, the CA also involves natural movements, such as walking with the device, holding it against the user's ear and carrying the device [167]. Thirdly, light sensors are used to defend against 2D virtual camera and media attacks without penalty speed authentication [204]. Using the authentication of physiological biometrics on the smartphone platform shows several disadvantages. Firstly, the person should provide certain measurements, such as face, voice, teeth and signature, which cause difficulty and discomfort in data collection. Secondly, these measurements are vulnerable to attacks by penetration, such as attacks using spoof and the suffering from repeated attacks [108, 173]. Dynamic biometrics face several challenges, including high intra-class variation and the imitation threat of skilled forgers of the dynamical movement [95].

Simple algorithms that can facilitate movement based on biometric authentication have been presented and demonstrated that smartphone motion sensors have sufficient quality for biometric applications. On the basis of an acceptable 10% false rejection rate (FRR), which is comparable to an alphanumeric password-based entry, the false acceptance rate (FAR) is 0.02% [95]. Although all other modalities of biometrics are similar, this behavioural method faces two fundamental challenges, namely, intra-class similarity and variability [164]. This threat excludes the potency of opening the smartphone and larceny of a genuine biometric template [164]. Thus, additional or highly demanding hardware is often needed [113].

Concerns on simulation scenarios

A simulation scenario is somehow related to data collection, where developers propose a scenario for data collection. This scenario includes the number of users and the steps in performing the experiment. Different conditions and scenarios have been designed and proposed by researchers to validate a newly developed approach. Researchers randomly suggest the number of participants, scenarios of data collection and testing environments [108].

The sensor-based signature technique uses either magnetic or orientation sensors to authenticate users. Different from the traditional handwritten signature, this technique must be performed in air by holding the smartphone [122] or using a magnet to perform a 3D magnetic signature in space around the device [166, 178]. In this case, the training data are cached from multiple sensor orientations via artificially rotating available training data [197]. However, the possibility of trusting gait signals is raised for effective IA. Thus, the viability of all the current solutions fails in reality because they rely on fixed sensors to a specific position and orientation [123]. The main challenge of modelling gait for authentication is using an unsupervised learning technique that learns a nominal model of the user's gait based on the training data, which is used to flag anomalous gait signatures of an adversary [216].

Concern on sensors and authentication methods

Different sensors can provide different authentication techniques, and replicating or simulating authentication techniques require different sensors with special aspects. Therefore, exploring new sensor-based authentication techniques requires a comprehensive understanding of the sensor behaviour, specification, output data and visible action provided by a particular sensor.

Therefore, if a researcher explores a handwaving action as a biometric, then he is initially required to elaborate on the uniqueness of the handwaving from one user to another. Then, he should identify the appropriate motion sensor to provide this motion [114]. Roshandel proposed that user movements of an appropriately shaped magnet around the device deform the original magnetic field [178]. In addition, the sensor must be economical, simple for wide deployment and energy-efficient. Therefore, Yang [217] proposed using a three-axis accelerometer to extract stable and individual characteristics from the gesture action of users. Lyu [212] used CLIP with accelerometer sensor; CLIP uses a low-power inertial accelerometer sensor with a lightweight entropy-based commitment mechanism that can authenticate the mobility trace of users without any cost of trusted hardware. In such a solution, user input, technique and interaction affect the result of authentication [165, 198]. Behavioural biometrics requires data collection from the accelerometer sensor to authenticate smartphone users [183]. Researchers in behavioural biometrics have attempted to test the accuracy of the authentication technique, the effective feature for the authentication technique and the difference between users in the authentication process [124, 175, 198]. Arm flexing when picking the mobile phone is another behavioural biometric proposed in the literature. This method is combined with the ear-shape approach to authenticate smartphone users [169].

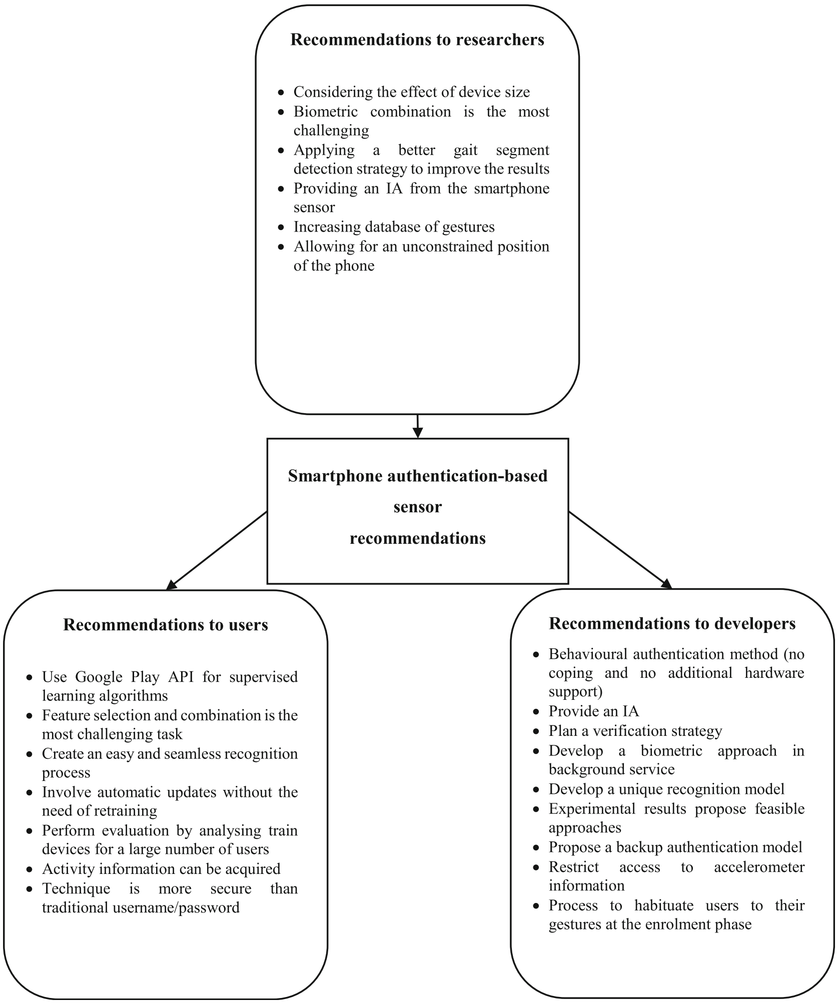
The traditional authentication methods, such as using PINs and passwords, require explicit interaction and are thus time-consuming and complicated [202]. In addition, classifier selection is reported to be a challenging task due to its complexity, execution time and classifier accuracy [162].

Recommendations

We provide several recommendations that aim to mitigate the challenges faced by developers, users and researchers in preventing smartphones from being utilised by unauthorised users. Figure 14 presents the recommendation categories for sensor-based smartphone authentication.

Recommendations related to users

Many smartphone users with highly sensitive data require substantial advice and recommendations to follow safe practices in their daily use. The users should be careful when using smartphones. The location of a smartphone user can be found using the sensors of the device, and his activity information can be obtained [183]. More secure techniques than the traditional username/password and similar methods are available; thus, users are required to use advanced authentication approaches [122]. Usability is one of the reasons why users do not use advanced authentication techniques. Lee [114] suggested a simple system using an accessory that users can carry



Recommendations to researchers

- Considering the effect of device size
- Biometric combination is the most challenging
- Applying a better gait segment detection strategy to improve the results
- Providing an IA from the smartphone sensor
- Increasing database of gestures
- Allowing for an unconstrained position of the phone

Smartphone authentication-based sensor recommendations

Recommendations to users

- Use Google Play API for supervised learning algorithms
- Feature selection and combination is the most challenging task
- Create an easy and seamless recognition process
- Involve automatic updates without the need of retraining
- Perform evaluation by analysing train devices for a large number of users
- Activity information can be acquired
- Technique is more secure than traditional username/password

Recommendations to developers

- Behavioural authentication method (no coping and no additional hardware support)
- Provide an IA
- Plan a verification strategy
- Develop a biometric approach in background service
- Develop a unique recognition model
- Experimental results propose feasible approaches
- Propose a backup authentication model
- Restrict access to accelerometer information
- Process to habituate users to their gestures at the enrolment phase

Fig. 14 Recommendation categories for sensor-based smartphone authentication

in public every day; the gestures of tapping and manipulating a mobile phone make the recognition process easy and seamless. Sufficient gait or location data are available, wherein some developers can detect an adversary in 50 s. Google Play API uses the inconspicuous label of data to obtain algorithms of supervised learning without clear user explanation [216]. However, CHAS involves automatic updating, in which the framework updates new data over time without the need for retraining [117].

Recommendations to developers

Developers or security providers have an important role in creating new authentication techniques. Several research recommendations are obtained from the studies of developers. Behavioural authentication that involves gestures is one of the sensor-based authentication methods. This type of authentication technique has good application prospect due to difficulties in replication or copying without the need for additional hardware support [179]. The data collected from these sensors can distinguish mobile users by analysing the user interaction

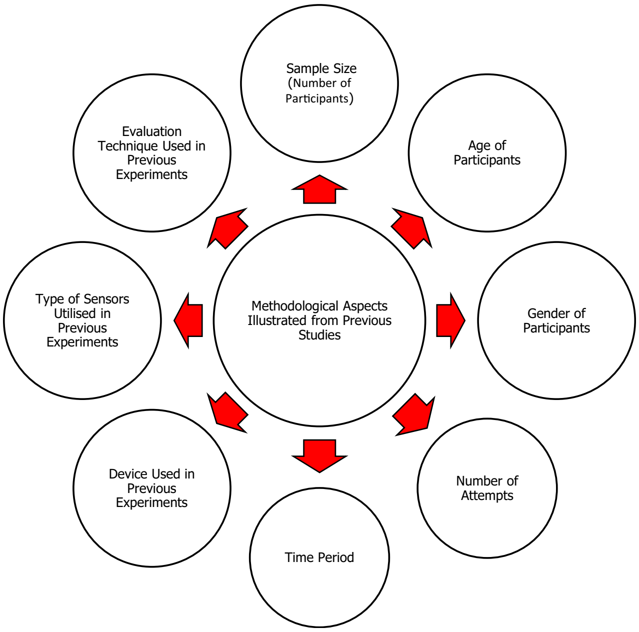
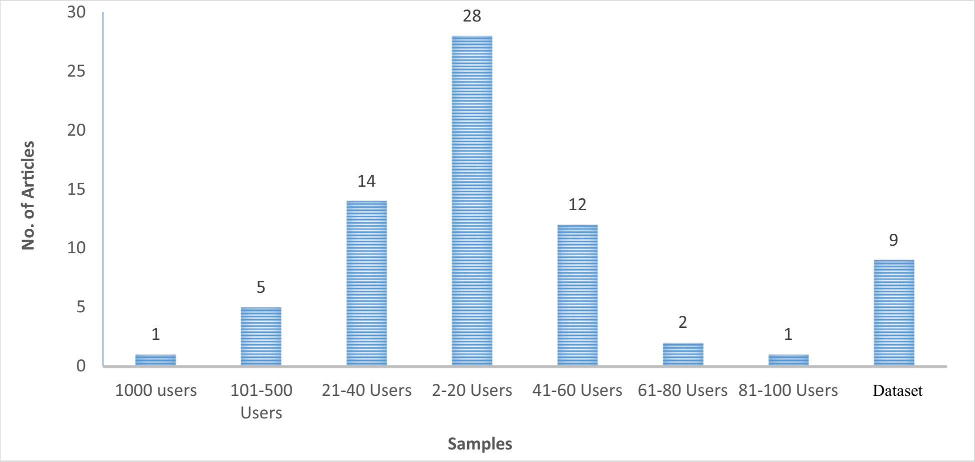

Sample Size (Number of Participants)
Age of Participants
Gender of Participants
Number of Attempts
Time Period
Device Used in Previous Experiments
Type of Sensors Utilised in Previous Experiments
Evaluation Technique Used in Previous Experiments
Methodological Aspects Illustrated from Previous Studies

Fig. 15 Methodological aspects illustrated from previous studies

Fig. 16 Number of samples according to academic articles in the second layer



with the device [179]. Smart sensors are suitable techniques to supply the IA [119]. This type of biometric approach can provide authentication in the background service. However, developers should be aware that not every feature is obtained as expected [121]. Orientation sensors can provide numerous features (e.g. in some experiments, 53 features were extracted from the orientation sensors alone), which lead to acceptable feasibility for such approach [124]. User behaviour models may contain multiple features of the user activity and the mobile device's response; a verification strategy should also be planned [121, 126]. A unique recognition model, where gait models are directly stored in the device that works effectively regardless of the position, is developed [123]. If this authentication fails, then an explicit authentication should provide a backup authentication model [119]. Authentication on the background service is required to verify the users. However, unconditional or unrestricted access to the sensors might enable attackers to track the smartphone [203].

In addition to a process that habituates users to their gestures at the enrolment phase, the optimal updating phase of the templates should be investigated to amend the deviation in the long term [189].

Recommendations to researchers

Five main directions found in the reviewed articles related to the present and future research were obtained. The first direction was the device size, wherein the literature reported that the newly developed authentication technique should be flexible with the device size or layout. Some researchers considered the effect of posture rather than that of device size. Liu et al. found a resilient authentication method against the device size [113]. The second direction was the recommendation related to feature selection. The most challenging tasks were biometric combination and feature selection [121]. Nguyen [123] proposed feature selection, which is an option to increase the usability of smartphones rather than providing a replacement for schemes of standard authentication on the smartphone due to the increase in privacy expectation. The result could be improved if the developers or researchers could apply improved gait segment detection strategy [123]. The third direction was related to the development of datasets by which researchers could test new techniques on the same data rather than collecting data with each experiment. Additional algorithms should also be proposed to compare the different performances of determining gestures [218]. The environment of the experiment was the fourth direction to produce feature research. The literature suggested that the new authentication techniques effectively performed in a controlled environment. Changing the position of the smartphone or other environment constraints, such as position of the phone, would affect the uncontrolled environment [206]. In addition, most of the experiments were performed in a single sitting; the researchers recommended collecting trials over multiple sessions to ensure verity in the environment [167]. Finally, in the evaluation process, one of the interesting questions related to scalability evaluation was how long users would need to train their devices and the response of real-time classification on smartphones for a large number of users [112].

Table 1 Age group distribution

Age group	18	24	28	16–56	16–60	18–30	18–35	18–40	19–36	19–60
Frequency	1	1	1	1	1	1	2	1	2	1
Age group	20–30	20–49	20–50	20–59	21–47	21–67	22–30	23–28	24–28	25–30
Frequency	2	1	1	2	1	1	2	1	1	1

Table 2 Gender distribution

Gender	References	Male	Female
3 m, 3 f	[112]	50%	50%
8 m, 1 f	[204]	88.9%	11.1%
All m	[183]	100.0%	0.0%
5 m, 1 f	[184]	83.3%	16.7%
10 m, 4 f	[198]	71.4%	28.6%
16 m, 4 f	[124]	80.0%	20.0%
29 m, 6 f	[209]	82.9%	17.1%
12 m, 8 f	[162]	60.0%	40.0%
6 m, 4 f	[121]	60.0%	40.0%
11 m, 8 f	[108]	57.9%	42.1%
10 m, 10 f	[170]	50.0%	50.0%
22 m, 8 f	[164]	73.3%	26.7%
15 m, 19 f	[201]	44.1%	55.9%
25 m, 15 f	[219]	62.5%	44.1%
15 m, 15 f	[218]	50.0%	50.0%
28 m, 10 f	[215]	73.7%	26.3%
29 m, 6 f	[205]	82.9%	15.8%
29 m, 6 f	[168]	82.9%	15.8%
29 m, 7 f	[206]	80.6%	19.4%
41 m, 10f	[182]	80.4%	19.6%
39 m, 12f	[115]	76.5%	23.5%
30 m, 14f	[186]	68.2%	31.8%
38 m, 12 f	[92]	76.0%	24.0%
30 m, 18 f	[202]	62.5%	37.5%
42 m, 31 f	[173]	57.5%	42.5%
62 m, 40 f	[177]	60.8%	39.2%
	Average	69.9%	30.3%

m = Male, f = Female

Methodological aspects of previous studies

Experimental research required references to justify the methodological aspects of previous research, particularly the number of samples, the type of device, the type of analysis, age and gender of participants, number of attempts, time period and evaluation technique. This information is important in the research methodology during exploration of a new authentication technique, as shown in Fig. 15.

Table 3 Frequency of iteration attempts

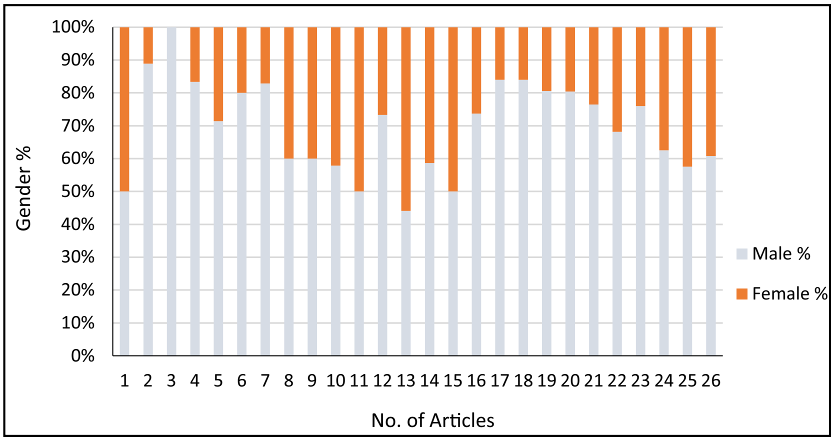
Group No.	Number of repetitions	Frequency of Appearance
1	100 t	1
2	10–40 t	1
3	10 t	4
4	12 t	2
5	15 t	2
6	20 t	3
7	2 t	1
8	30 t	1
9	35 t	1
10	36 t	1
11	3960 t	1
12	3 t	6
13	40 t	1
14	4 t	2
15	500 t	1
16	5 t	5
17	6 t	2
18	7 t	2
19	8 t	3

Sample size

In this section, we tabulate these aspects from the selected studies. The largest portion of research articles (28) suggested a sample size between 2 and 20 participants, whereas nine articles used a dataset from other research articles. Only eight articles did not mention the number of participants.

The literature stated that 60 articles were used and reported as the sample size in the development of their experiments.

Fig. 17 Visualisation of gender distribution



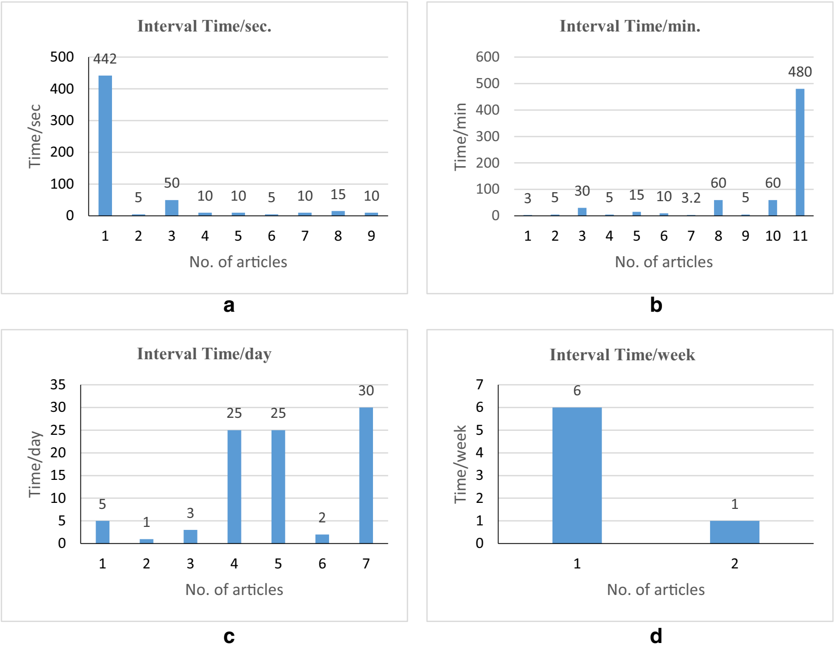


Fig. 18 Different time interval systems in (**a**) seconds, (**b**) minutes, (**c**) days and (**d**) weeks

Amongst these articles, 46% ($n = 28/60$) used 20 participants or less, whereas 23% ($n = 14/60$) of the 60 research articles used between 20 and 40 participants (23). In total, 70% ($n = 42/60$) of the articles used a sample size from 2 to 40 participants. Another 10 articles used datasets collected by other researchers; however, these articles did not report the number of participants. The last 11 articles discussed the frameworks with no data collection process, following the majority of the academic literature. Figure 16 presents a number of samples according to the academic articles in the second layer.

Age group

The age category varies in sample selection, as shown in Table 1. Most participants in different experiments are between the ages of 16 and 67 years.

On the basis of the literature, 20 different age groups were reported in 25 articles that reported the sample age in the development of their experiments. Only 5 age groups were presented in 2 different studies, whereas 20 studies introduced different age groups. The variety of age groups causes difficulty in selecting only one study from amongst a multitude.

Gender

The gender of the participants is important for the comparison of different gender groups. However, none of the studies analysed or compared gender groups. Therefore, only 26 research articles mentioned the gender of the participants, whereas the others (excluding the articles that used datasets) did not. Table 2 shows the details of gender distribution per article. The table includes the articles that mentioned the gender of the participants in the 26 studies out of the total number of screened articles.

Figure 17 presents the ratio of different genders per study. From the figure, the ratio of male participants is higher than that of females. A total of 26 articles mentioned gender. Gender distribution in the previous research articles was conducted without evident basis. The average of male participants from the total participants in the selected studies was 69.9%, whereas the female participants achieved a total average of 31.1% of the total participants. Two studies equally distributed the number of participants between the two genders. Only one study preferred female over male.

Table 4 Different time interval systems

No. of Time Interval	Interval Time (s)	Interval Time (min)	Interval Time (day)	Interval Time (week)
1	442	3	5	6
2	5	5	1	1
3	50	30	3	–
4	10	5	25	–
5	10	15	25	–
6	5	10	2	–
7	10	3.2	30	–
8	15	60	–	–
9	10	5	–	–
10	–	60	–	–
11	–	480	–	–

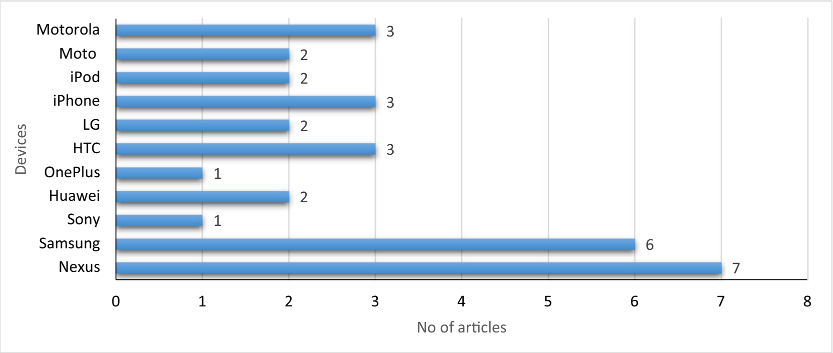


Fig. 19 Devices used in previous studies and frequency of usage

Frequency of attempts, iteration and time interval per experiment

In biometric research, use, repeat and remember are considered the most desired criteria for biometric performance measurement with respect to user experience, which is regarded as a part of the usability performance test. Table 3 shows the 19 articles that described the time interval for repetitions of the experiments per user.

The number of attempts per participant is not standardised. Different experiments proposed different attempts.

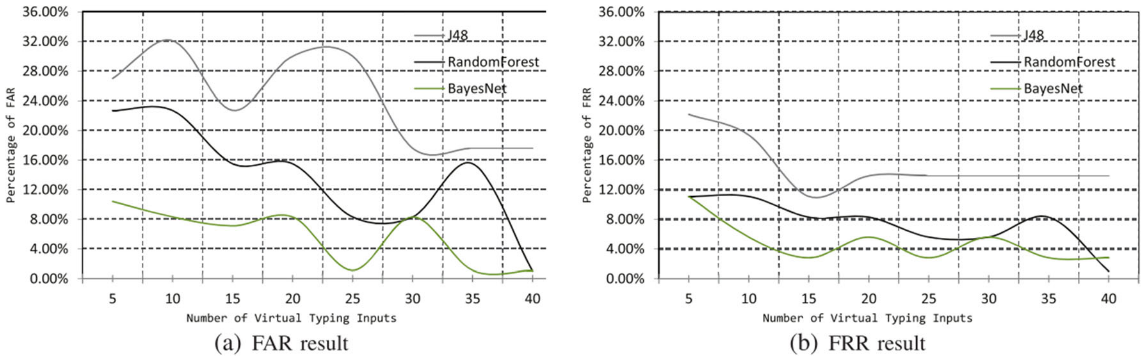
Time interval is another configuration illustrated from previous studies. Time interval represents the total period of the experiments. Researchers proposed four different time interval types. The first system used seconds as time interval, in which developers repeated the experiment with participants per second. The minimum time interval was 2 times every 5 s, whereas the maximum was repetition of experiment twice every 442 s. The second system used minutes as time interval, with minimum repetition of 10 times every 3 min and maximum of 2 times every 60 min. The third system used days as time interval, with minimum of 10–40 times in one day and maximum of 7 times in 30 days. The last system used week time interval, with minimum repetition of 2 times during the week and maximum of 16 times for 6 weeks. Figure 18 describes the four time interval systems used in the articles. Only 29 articles mentioned the time interval when they reported their experiment configuration.

Table lists the different time interval systems and time used in each system (Table 4).

Equipment

The selected studies utilised various types of smartphone devices. The first impression states no evident bases for device selection. However, sensor availability and ease of developments play important roles in selecting the device and operating system.

From our observation, the majority of the developments were conducted with devices that operate on Android rather than iOS; however, a number of iOS-related developments also exist. Figure 19 describes the devices utilised in the previous studies. Only 33 research articles mentioned the device type in their experiment configurations. A total of 12 devices were used in the previous experiments. The most frequently used devices were Nexus (seven times) and Samsung (six times). Other devices, such as Sony, Huawei, OnePlus, HTC, LG, iPhone, iPod, Moto and Motorola, were used only once, twice or thrice. Nexus is developed by different companies, such as Samsung, Motorola and Google. A total of 28 devices used in the previous experiments used the Android operating system whereas five devices used iOS. Android is more utilised than iOS due to its ease of development.



(a) FAR result

(b) FRR result

Fig. 20 High usability with high FAR and low FRR [165]

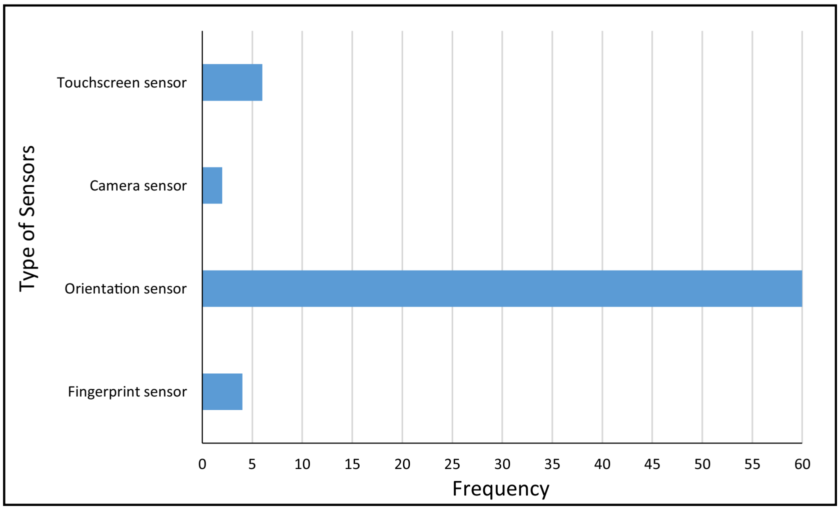


Fig. 21 Sensors utilised in academic literature

Performance analysis

The researchers adopted standard quality testing for evaluation techniques. Usability metrics are used to obtain results of the authentication technique. These metrics include FRR and FAR, which are the two measurements used for performance evaluation of the authentication technique. A total of 49.3% ($n = 40/81$) articles used the two measurements in their developed experiments. The two metrics were used to clarify the trade-off between ease of use and security achieved by the authentication solution. FAR is the decision percentage of authentication that allows access to an unauthorised user, whereas FRR is the decision percentage of authentication where an authorised user is denied access.

A solution that shows a decrease in FAR and an increase in FRR is secure but complicated whereas that which shows a low FRR and a high FAR is usable but less secure. Figure 20 depicts that FAR is high when the usability is high [113, 117, 165].

Sensors utilised in previous studies

A number of sensors were utilised to authenticate users with their smartphones. Our investigation of the academic literature identified that the orientation (e.g. accelerometer, gyroscope and magnetic sensors), finger, camera and touchscreen sensors were used. As reported in the literature, the usage frequency of these sensors is as follows: fingerprint sensor ($n = 4/72$), orientation sensor ($n = 60/72$), camera sensor ($n = 2/72$) and touchscreen sensor ($n = 6/72$). The microphone sensor was unexplored, whereas the touchscreen sensor was utilised six times. None of the articles mentioned the usage of 3D touch sensors (see Fig. 21).

Conclusion

This study aims to provide an updated substructure of authentication techniques for sensor-based mHealth. The research focuses on the directions that address this subject. The first layer of our taxonomy, that is, security and privacy of sensor-based telemedicine applications, is presented, and the studies related to the security issues are analysed and discussed in three tiers. In the second layer of our taxonomy, comprehensive survey focuses on previous articles on documentation techniques without applications. We also reviewed the new direction in using sensor-based smartphone authentication as innovative side channels to conclude taps on mHealth sensors in telemedicine application. This development resulted from the increasing popularity and wide deployment of sensor applications and patient privacy risks and low level of security awareness in telemedicine application. All recent and published works on sensor-based smartphone authentication were surveyed, and the findings and important contributions were highlighted. The first contribution is the provision of taxonomy in this research based on the literature. The second layer is divided into the following three main categories: defence, attack and others. The taxonomy can also provide the researchers with novel ideas in several related topics. In the second contribution, we covered the main highlights of the selected studies, including motivations, challenges and recommendations. We highlighted the motivation benefits related to smartphone usability, effect of security on smartphones, sensor authentication usability, sensor security and application activities. Our analysis raised several concerns reported by researchers. Therefore, we highlighted these challenges concerning protection, access and collection of data and all-inclusive understanding of the authentication method and usability, its sensors and biometrics. In addition, we emphasised the recommendations related to users, developers/providers and researchers. In the last contribution, we focused on the methodological aspects of the previous studies, which covered the sample size (number of participants); age and gender of participants; devices, type of sensors, evaluation techniques and operating systems in the previous experiments; and experimental configurations. To the best of our knowledge, our study is the first endeavour to provide a multilayer comprehensive overview of the sensor and security in telemedicine architecture and sensor-based smartphone authentication in the literature to match benefits to mHealth authentication security and privacy. We hope that other researchers will benefit from this study and use it as a starting point to expand the research further based on the challenges we discussed.

Compliance with Ethical Standards

Conflict of Interest The authors declare no conflict of interest.

Ethical Approval All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Declaration of Helsinki and its later amendments or comparable ethical standards.

Informed Consent Informed consent was obtained from all individual participants included in the study.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Hussain, M. et al., The rise of keyloggers on smartphones: A survey and insight into motion-based tap inference attacks. Pervasive Mob. Comput. 25:1–25, 2016.
2. Salem, Y. et al., A review on multimedia communications cryptography. Res. J. Inf. Technol. 3:146–152, 2011.
3. Elnajjar, M. et al.. Optimization digital image watermarking technique for patent protection. arXiv preprint arXiv:1002.4049. 2010.
4. Watari, M. A. et al., Securing m-government transmission based on symmetric and asymmetric algorithms: A review. Asian J. Sci. Res. 8:80–94, 2013.
5. Nabi, M. S. *et al.*. Suitability of adopting S/MIME and OpenPGP email messages protocol to secure electronic medical records. In Future Generation Communication Technology (FGCT), 2013 Second International Conference on (pp. 93–97). IEEE. 2013.
6. Naji, A. W. et al., Security improvement of credit card online purchasing system. Sci. Res. Essays 6(16):3357–3370, 2011.
7. Zaidan, A. A. et al., Spam influence on business and economy: Theoretical and experimental studies for textual anti-spam filtering using mature document processing and naive Bayesian classifier. Afr. J. Bus. Manag. 5(2):596–607, 2011.
8. Raad, M. et al., Impact of spam advertisement through e-mail: A study to assess the influence of the anti-spam on the e-mail marketing. Afr. J. Bus. Manag. 4(11):2362–2367, 2010.
9. Alanazi, H. *et al.*. Intrusion detection system: overview. arXiv preprint arXiv:1002.4047. 2010.
10. Aos, A. Z. *et al.*. Approved undetectable-antivirus steganography for multimedia information in PE-file. In Computer Science and Information Technology-Spring Conference, 2009. IACSITSC'09. International Association of(pp. 437–441). IEEE. 2009.
11. Eltahir, M. E. *et al.*. High rate video streaming steganography. In Information Management and Engineering, 2009. ICIME'09. International Conference on (pp. 550–553). IEEE. 2009.
12. Talib, Y. Y. A. *et al.*. 3 "Optimizing Security and Flexibility by Designing a High Security System for E-Government Servers". ICOCI09, University Utara Malaysia. 2009.
13. Zaidan, B. B. *et al.*. An empirical study for impact of the increment the size of hidden data on the image texture. *ICFCC09*. 2009.
14. Zaidan, A. A. *et al.*. Securing cover-file of hidden data using statistical technique and AES encryption algorithm. ICSAP09. 2009.
15. Ali, A. H. *et al.*. High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. Multimedia Tools and Applications, 1–30. 2018.
16. Zaidan, B. B. et al., Software and hardware FPGA-based digital watermarking and steganography approaches: Toward new methodology for evaluation and benchmarking using multi-criteria decision-making techniques. J. Circ. Syst. Comput. 26(07):1750116, 2017.
17. Zaidan, B. B. et al., A new digital watermarking evaluation and benchmarking methodology using an external group of evaluators and multi-criteria analysis based on 'large-scale data'. Softw. Pract. Exp. 47(10):1365–1392, 2017.
18. Zaidan, B. B. et al., Comparative study on the evaluation and benchmarking information hiding approaches based multi-measurement analysis using TOPSIS method with different normalisation, separation and context techniques. Measurement 117: 277–294, 2018.
19. Naji, A. W. et al., New approach of hidden data in the portable executable file without change the size of carrier file using distortion techniques. Proc. World Acad. Sci. Eng. Technol. (WASET) 56:493–497, 2009.
20. Zaidan, A. et al., New comprehensive study to assess comparatively the QKD, XKMS, KDM in the PKI encryption algorithms. Int. J. Comput. Sci. Eng. 1, 2009.
21. Aos, A. Z. *et al.*. Approved undetectable-antivirus steganography for multimedia information in PE-file. In Computer Science and Information Technology-Spring Conference, 2009. IACSITSC'09. International Association of(pp. 437–441). IEEE. 2009.
22. Zaidan, B. B. et al., Stego-image vs stego-analysis system. Int. J. Comput. Elect. Eng. 1(5):572, 2009.
23. Abomhara, Mohamed *et al.*, (2010). Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard. International Journal of Computer Theory and Engineering. 2. 223–229. https://doi.org/10.7763/IJCEE.2010.V2.141.
24. Alanazi, H *et al.*. New comparative study between DES, 3DES and AES within nine factors. arXiv preprint arXiv:1003.4085. 2010.
25. Zaidan, B. B. et al., Towards corrosion detection system. Int. J. Comput. Sci. Issues (IJCSI) 7(3):46, 2010.
26. Nidhal, S. et al., Computerized algorithm for fetal heart rate baseline and baseline variability estimation based on distance between signal average and alpha value. Int. J. Pharmacol. 7(2):228–237, 2011.
27. Jawad, M. M. et al., An overview of laser principle, laser-tissue interaction mechanisms and laser safety precautions for medical laser users. Int. J. Pharmacol. 7(2):149–160, 2011.
28. Abomhara, M. et al., An experiment of scalable video security solution using H. 264/AVC and advanced encryption standard (AES): Selective cryptography. Int. J. Phys. Sci. 6(16):4053–4063, 2011.
29. Zaidan, A. A. et al., Commercialization strategy and implementation plans for the proposed Vitual anti-spam system based on feasibility study. Asian J. Sci. Res. 8(3):403–412, 2015.
30. Kiah, M. L. M. et al., Open source EMR software: Profiling, insights and hands-on analysis. Comput. Methods Prog. Biomed. 117(2):360–382, 2014.
31. Kiah, M. M. et al., Design and develop a video conferencing framework for real-time telemedicine applications using secure group-based communication architecture. J. Med. Syst. 38(10):133, 2014.
32. Doumbouya, M. B., Kamsu-Foguem, B., Kenfack, H., and Foguem, C., A framework for decision making on teleexpertise with traceability of the reasoning. IRBM 36(1):40–51, 2015.
33. Kalid, N. et al., Based real time remote health monitoring systems: A review on patients prioritization and related" big data" using body sensors information and communication technology. J. Med. Syst. 42(2):30, 2018.
34. Salman, O. H. et al., Novel methodology for triage and prioritizing using "big data" patients with chronic heart diseases through

telemedicine environmental. Int. J. Inf. Technol. Decis. Mak. 16(05):1211–1245, 2017.

35. Hamdi, O., Chalouf, M. A., Ouattara, D., and Krief, F., eHealth: Survey on research projects, comparative study of telemonitoring architectures and main issues. J. Netw. Comput. Appl. 46:100–112, 2014.

36. Kiah, M. L. M. et al., MIRASS: Medical informatics research activity support system using information mashup network. J. Med. Syst. 38(4):37, 2014.

37. Zaidan, B. B. et al., Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns. Int. J. Pharmacol. 7(3):382–387, 2011.

38. Zaidan, A. A. et al., Evaluation and selection of open-source EMR software packages based on integrated AHP and TOPSIS. J. Biomed. Inform. 53:390–404, 2015.

39. Zaidan, A. A. et al., Multi-criteria analysis for OS-EMR software selection problem: A comparative study. Decis. Support. Syst. 78: 15–27, 2015.

40. Hussain, M. et al., The landscape of research on smartphone medical apps: Coherent taxonomy, motivations, open challenges and recommendations. Comput. Methods Prog. Biomed. 122(3):393–408, 2015.

41. Al-Haiqi, M. et al., A distributed framework for health information exchange using smartphone technologies. J. Biomed. Inform. 69: 230–250, 2017.

42. Rajan, S. P., Review and investigations on future research directions of mobile based telecare system for cardiac surveillance. J. Appl. Res. Technol. 13(4):454–460, 2015 Universidad Nacional Autónoma de México, Centro de Ciencias Aplicadas y Desarrollo Tecnológico.

43. Negra, R., Jemili, I., and Belghith, A., Wireless body area networks: Applications and technologies. Procedia Comput. Sci. 83:1274–1281, 2016.

44. Alanazi, H. O. et al., Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. J. Med. Plants Res. 4(19):2059–2074, 2010.

45. Nabi, M. S. A. et al., Suitability of using SOAP protocol to secure electronic medical record databases transmission. Int. J. Pharmacol. 6(6):959–964, 2010.

46. Al-Bakri, S. H. et al., Securing peer-to-peer mobile communications using public key cryptography: New security strategy. Int. J. Phys. Sci. 6(4):930–938, 2011.

47. Hu, F., Celentano, L., and Xiao, Y., Mobile telemedicine: a computing and networking perspective.Mobile, Secure Tele-Cardiology Based on Wireless and Sensor Networks, 2008.

48. Ellouze, N., Rekhis, S., Boudriga, N., and Allouche, M., Powerless security for cardiac implantable medical devices: Use of wireless identification and sensing platform. J. Netw. Comput. Appl. 107:1–21, 2018.

49. Andriole, K. P., Security of electronic medical information and patient privacy: What you need to know. J. Am. Coll. Radiol. 11(12):1212–1216, 2014.

50. Kiah, M. M. et al., An enhanced security solution for electronic medical records based on AES hybrid technique with SOAP/XML and SHA-1. J. Med. Syst. 37(5):9971, 2013.

51. Alanazi, H. O. et al., Secure topology for electronic medical record transmissions. Int. J. Pharmacol. 6(6):954–958, 2010.

52. Alanazi, H. O. et al., Meeting the security requirements of electronic medical records in the ERA of high-speed computing. J. Med. Syst. 39(1):165, 2015.

53. Zaidan, B. B. et al., A security framework for nationwide health information exchange based on telehealth strategy. J. Med. Syst. 39(5):51, 2015.

54. Zaidan, A. A. et al., Challenges, alternatives, and paths to sustainability: Better public health promotion using social networking pages as key tools. J. Med. Syst. 39(2):7, 2015.

55. Medani, A. et al., Review of mobile short message service security issues and techniques towards the solution. Sci. Res. Essays 6(6): 1147–1165, 2011.

56. Hussain, M. et al., Conceptual framework for the security of mobile health applications on android platform. Telematics Inform. 35(5):1335–1354, 2018.

57. Iqbal, S. et al., Real-time-based E-health systems: Design and implementation of a lightweight key management protocol for securing sensitive information of patients. Heal. Technol.:1–19, 2018.

58. Enaizan, O. et al., Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. Heal. Technol.:1–28, 2018.

59. Hussain, M. et al., A security framework for mHealth apps on android platform. Comput. Sec. 75:191–217, 2018.

60. Zaidan, B. B. et al., A new approach based on multi-dimensional evaluation and benchmarking for data hiding techniques. Int. J. Inf. Technol. Decis. Mak.:1–42, 2017.

61. Zaidan, A. A. et al., Novel approach for high (secure and rate) data hidden within triplex space for executable file. Sci. Res. Essays 5(15):1965–1977, 2010.

62. Alam, G. M. et al., Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study. Sci. Res. Essays 5(21):3254–3260, 2010.

63. Naji, A. W. et al., Novel approach for cover file of hidden data in the unused area two within EXE file using distortion techniques and advance encryption standard. Proc. World Acad. Sci. Eng. Technol. (WASET) 56(5):498–502, 2010.

64. Naji, A. W. *et al.*. Novel framework for hidden data in the image page within executable file using computation between advanced encryption standard and distortion techniques. arXiv preprint arXiv:0908.0216. 2009.

65. Zaidan, B. B. et al., On the differences between hiding information and cryptography techniques: An overview. J. Appl. Sci. (Faisalabad) 10(15):1650–1655, 2010.

66. Hmood, A. K. et al., An overview on hiding information technique in images. J. Appl. Sci. (Faisalabad) 10(18):2094–2100, 2010.

67. Hamdan, A. et al., New frame work of hidden data with in non multimedia file. Int. J. Comput. Netw. Secur. 2(1):46–54, 2010.

68. Jalab, H. A. et al., New design for information hiding with in steganography using distortion techniques. Int. J. Eng. Technol. 2(1):72, 2010.

69. Zaidan, A. A. *et al.*. Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 1–7). 2009.

70. Zaidan, B. et al., Quality of image vs. quantity of data hidden in the image. IPCV 6:343–350, 2009.

71. Othman, F. *et al.*. An extensive empirical study for the impact of increasing data hidden on the images texture. In Future Computer and Communication, 2009. ICFCC 2009. International Conference on (pp. 477–481). IEEE. 2009.

72. Islam, R. *et al.*. New system for secure cover file of hidden data in the image page within executable file using statistical steganography techniques. arXiv preprint arXiv:1002.2416. 2010.

73. Zaidan, B. B. Et al.. Enhancement of the amount of hidden data and the quality of image. Faculty of Computer Science and Information Technology, *University of Malaya*, Kuala Lumpur, Malaysia. 2008.

74. Zaidan, A. A. et al., Novel approach for high secure data hidden in MPEG video using public key infrastructure. Int. J. Comput. Netw. Secur. 1(1):1985–1553, 2009.

75. Naji, A. W. et al., Challenges of hidden data in the unused area two within executable files. J. Comput. Sci. 5(11):890, 2009.

76. Naji, A. W. et al., New approach of hidden data in the portable executable file without change the size of carrier file using statistical technique. Int. J. Comput. Sci. Netw. Sec. (IJCSNS) 9(7): 218–224, 2009.

77. Majeed, A. et al., Novel approach for high secure and high rate data hidden in the image using image texture analysis. Int. J. Eng. Technol. 1(2):63–69, 2009.

78. Zaidan, A. A. *et al.*. Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography. *International Association of Computer Science and Information Technology (IACSIT)*, indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, 20. 2009.

79. Talib, *et al.*. 3 "Optimizing Security and Flexibility by Designing a High Security System for E-Government Servers". ICOCI09, *University Utara Malaysia*. 2009.

80. Naji, A. W. *et al.*. " Stego-Analysis Chain, Session One" Investigations on Steganography Weakness vs Stego-Analysis System for Multimedia File. In Computer Science and Information Technology-Spring Conference, 2009. IACSITSC'09. International Association of (pp. 405–409). *IEEE*. 2009.

81. Khalifa, O. O. et al., Novel approach of hidden data in the (unused area 2 within EXE file) using computation between cryptography and steganography. Int. J. Comput. Sci. Netw. Sec. (IJCSNS) 9(5): 294–300, 2010.

82. Zaidan, A. A. *et al.*. Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 1–7). 2009.

83. Naji, A. W. et al., Novel approach for secure cover file of hidden data in the unused area within exe file using computation between cryptography and steganography. Int. J. Comput. Sci. Netw. Sec. [On-line] 9(5):294–300, 2009.

84. Othman, F. *et al.*. An extensive empirical study for the impact of increasing data hidden on the images texture. In Future Computer and Communication, 2009. ICFCC 2009. International Conference on (pp. 477–481). IEEE. 2009.

85. Naji, A. W. *et al.*. " Stego-Analysis Chain, Session Two" Novel Approach of Stego-Analysis System for Image File. In Computer Science and Information Technology-Spring Conference, 2009. IACSITSC'09. International Association of (pp. 410–413). IEEE. 2009.

86. Zaidan, A. A. et al., High securing cover-file of hidden data using statistical technique and AES encryption algorithm. World Acad. Sci. Eng. Technol. (WASET) 54:468–479, 2009.

87. Taqa, A. et al., New framework for high secure data hidden in the MPEG using AES encryption algorithm. In. J. Comput. Elect. Eng. (IJCEE) 1(5):566–571, 2009.

88. Zaidan, A. A. et al., New technique of hidden data in pe-file with in unused area one. In. J. Comput. Elect. Eng. (IJCEE) 1(5):669–678, 2009.

89. Jalab, H. *et al.*, (2009). Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation. arXiv preprint arXiv:0912.3986.

90. Ahmed, M. A. et al., A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J. Appl. Sci. 10(1):59–64, 2010.

91. Al-Frajat, A. K. et al., Hiding data in video file: An overview. J. Appl. Sci. (Faisalabad) 10(15):1644–1649, 2010.

92. Wang H, Lymberopoulos D, Liu J. Sensor-Based User Authentication 168–185. 2015.

93. Mohsin, A. H. et al., Real-time medical systems based on human biometric steganography: A systematic review. J. Med. Syst. 42(12):245, 2018.

94. Mohsin, A. H. et al., Real-time remote health monitoring systems using body sensor information and finger vein biometric verification: A multi-layer systematic review. J. Med. Syst. 42(12):238, 2018.

95. Fantana, A. L., Ramachandran, S., Schunck, C. H., and Talamo, M., Movement based biometric authentication with smartphones. Proc. - Int. Carnahan Conf. Secur. Technol. 2015(18):235–239, 2016.

96. Al-Ani, Z. K. *et al.*. Overview: Main fundamentals for steganography. arXiv preprint arXiv:1003.4086. 2010.

97. Alanazi, H. *et al.*. New Classification Methods for Hiding Information into Two Parts: Multimedia Files and Non Multimedia Files. arXiv preprint arXiv:1003.4084. 2010.

98. Zaidan, A. A. et al., A new system for hiding data within (unused area two+ image page) of portable executable file using statistical technique and advance encryption Standared. Int. J. Comput. Theory Eng.\ 2(2):218, 2010.

99. Yahya, A. N. *et al.*. A new system for hidden data within header space for EXE-File using object oriented technique. In Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Vol. 7, pp. 9–13). IEEE. 2010.

100. Hmood, A. K. et al., On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. Int. J. Phys. Sci. 5(7):1054–1062, 2010.

101. Abomhara, M. et al., Suitability of using symmetric key to secure multimedia data: An overview. J. Appl. Sci. (Faisalabad) 10(15): 1656–1661, 2010.

102. Hmood, A. K., Jalab, H. A., Kasirun, Z. M., Zaidan, B. B., and Zaidan, A. A., On the capacity and security of steganography approaches: An overview. J. Appl. Sci. (Faisalabad) 10(16): 1825–1833, 2010.

103. Zaidan, A. A. et al., Investigate the capability of applying hidden data in text file: An overview. J. Appl. Sci. (Faisalabad) 10(17): 1916–1922, 2010.

104. Zaidan, A. A. et al., Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. Int. J. Phys. Sci. 5(11):1776–1786, 2010.

105. Zaidan, B. B. et al., StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem. Int. J. Phys. Sci. 5(11):1796–1806, 2010.

106. Mat Kiah, M. L. et al., A review of audio based steganography and digital watermarking. Int. J. Phys. Sci. 6(16):3837–3850, 2011.

107. Corpus, K. R., Gonzales, R. J. D., Morada, A. S., and Vea, L. A., Mobile user identification through authentication using keystroke dynamics and accelerometer biometrics. Proc. Int. Work. Mob. Softw. Eng. Syst. - MOBILESoft ' 16:11–12, 2016.

108. Sun Z, Wang Y. A 3-D Hand Gesture Signature Based Biometric Authentication System for Smartphones, no. 2. 2015.

109. Hameed, S. A. et al., Novel simulation framework of three-dimensional skull bio-metric measurement. Shibab a. Hameed et al/*International Journal on Computer Science and*. Engineering 1(3):269–274, 2009.

110. Hameed et al., An accurate method to obtain bio-metric measurements for three dimensional skull. J. Appl. Sci. 10(2):145–150, 2010.

111. Ling Z et al.. Secure fingertip mouse for mobile devices. Proc. - IEEE INFOCOM 2016 (16). 2016.

112. Ali, Z., Payton, J., and Sritapan, V., At your fingertips: Considering finger distinctness in continuous touch-based authentication for Mobile devices. Proc. - 2016 IEEE Symp. Secur. Priv. Work. SPW 2016:272–275, 2016.

113. Liu Q, Wang M, Zhao P, Yan C, Ding Z. A Behavioral Authentication Method for Mobile Gesture Against Resilient User Posture, 21016 3rd Int. Conf. Syst. Informatics, ICSAI 2016, no. Icsai. 324–331. 2016.

114. Lee S, Song K, Choi J. Access to an automated security system using gesture-based passwords, Proc 2012 15th Int Conf Network-Based Inf Syst NBIS 2012 (25): 760–765. 2012.

115. Muaaz M, Mayrhofer R. An Analysis of Different Approaches to Gait Recognition Using Cell Phone Based Accelerometers. Proc Int Conf Adv Mob Comput Multimed - MoMM '13. 293–300. 2013.

116. Nickel C, Brandt H, Busch C. Classification of Acceleration Data for Biometric Gait Recognition on Mobile Devices. Biosig 57–66. 2011.

117. Roy A, Halevi T, Memon N. An HMM-based multi-sensor approach for continuous mobile authentication. Proc - IEEE Mil Commun Conf MILCOM vol. 2015–Decem. 1311–1316. 2015.

118. Crouse D, Chandra D, Barbello B. Continuous Authentication of Mobile User: Fusion of Face Image and Inertial Measurement Unit Data. 135–142. 2013.

119. Dandachi, G, El Hassan B, El Husseini A. A Novel Identification/Verification Model Using Smartphone's Sensors and User Behavior. (1): 235–238. 2013.

120. Feng, T., DeSalvo, N., Xu, L., Zhao, X., Wang, X., and Shi, W., Secure session on Mobile: An exploration on combining biometric, TrustZone, and user behavior. Proc. 6th Int. Conf. Mob. Comput. Appl. Serv. 1(4):206–215, 2014.

121. Shih D-H, Lu C-M, Shih M-H. A flick biometric authentication mechanism on mobile devices. Int Conf Inf Cybern Comput Soc Syst 31–33. 2015.

122. Laghari A, Memon ZA. Biometric Authentication Technique Using Smartphone Sensor. 2016 13th Int. Bhurban Conf. 2016 Jan 12 IEEE (20):381–384. 2016.

123. Nguyen H, Nguyen HH, Hoang T, Choi D, Nguyen TD. A Generalized Authentication Scheme For Mobile Phones Using Gait Signals 386–407. 2016.

124. Lin CC, Chang CC, Liang D, Yang CH. A new non-intrusive authentication method based on the orientation sensor for smartphone users. Proc 2012 IEEE 6th Int Conf Softw Secur Reliab SERE 2012 (24):245–252. 2012.

125. T. Van Goethem (B), W. Scheepers, D. Preuveneers, and W. Joosen, "Accelerometer-Based Device Fingerprinting for Multi-factor Mobile Authentication," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9639, pp. 106–121, 2016.

126. Rybnicek M, Lang-Muhr C, Haslinger D. A roadmap to continuous biometric authentication on mobile devices. 2014 Int Wirel Commun Mob Comput Conf. 122–127. 2014.

127. Pisani, P. H., Lorena, A. C., and De Carvalho, A. C. P. L. F., Adaptive algorithms applied to accelerometer biometrics in a data stream context. Intell. Data Anal. 21(2):353–370, 2017.

128. Kalid, N. et al., Based on real time remote health monitoring systems: A new approach for prioritization "large scales data" patients with chronic heart diseases using body sensors and communication technology. J. Med. Syst. 42(4):69, 2018.

129. Yas, Q. M. et al., A systematic review on smartphone skin cancer apps: Coherent taxonomy, motivations, open challenges and recommendations, and new research direction. J. Circ. Syst. Comput. 27(05):1830003, 2018.

130. Zaidan, A. A. et al., A survey on communication components for IoT-based technologies in smart homes. Telecommun. Syst.:1–25, 2018.

131. Alsalem, M. A. et al., Systematic review of an automated multiclass detection and classification system for acute Leukaemia in terms of evaluation and benchmarking, open challenges, issues and methodological aspects. J. Med. Syst. 42(11):204, 2018.

132. Zaidan, A. A. et al., A review on smartphone skin cancer diagnosis apps in evaluation and benchmarking: Coherent taxonomy, open issues and recommendation pathway solution. Heal. Technol.:1–16, 2018.

133. Alsalem, M. A. *et al.*. A review of the automated detection and classification of acute leukaemia: Coherent taxonomy, datasets, validation and performance measurements, motivation, open challenges and recommendations. Computer methods and programs in biomedicine. (2018).

134. Ahmed, M. A. et al., A review on systems-based sensory gloves for sign language recognition state of the art between 2007 and 2017. Sensors 18(7):2208, 2018.

135. Hamada, M. et al., A systematic review for human EEG brain signals based emotion classification, feature extraction, brain condition, group comparison. J. Med. Syst. 42(9):162, 2018.

136. Tareq, Z. *et al.*. A review of disability EEG based wheelchair control system: Coherent taxonomy, open challenges and recommendations. Computer methods and programs in biomedicine. 2018.

137. Brian RM, Ben-Zeev D. Mobile health (mHealth) for mental health in Asia: Objectives, strategies, and limitations, *Asian Journal of Psychiatry*, vol. 10, no. 2014. Elsevier B.V. 96–100. 2014.

138. Iwaya, L. H. et al., Mobile health in emerging countries: A survey of research initiatives in Brazil. Int. J. Med. Inform. 82(5):283–298, 2013.

139. Obi, T., Ishmatova, D., and Iwasaki, N., Promoting ICT innovations for the ageing population in Japan. Int. J. Med. Inform. 82(4): e47–e62, 2013.

140. Shore, J. H., Aldag, M., McVeigh, F. L., Hoover, R. L., Ciulla, R., and Fisher, A., Review of Mobile health Technology for Military Mental Health. Mil. Med. 179(8):865–878, 2014.

141. Adams, Z. W., McClure, E. A., Gray, K. M., Danielson, C. K., Treiber, F. A., and Ruggiero, K. J., Mobile devices for the remote acquisition of physiological and behavioral biomarkers in psychiatric clinical research. J. Psychiatr. Res. 85:1–14, 2017.

142. Silva, B. M. C., Rodrigues, J. J. P. C., de la Torre Díez, I., López-Coronado, M., and Saleem, K., Mobile-health: A review of current state in 2015. J. Biomed. Inform. 56:265–272, 2015.

143. Point, C., Accreditation, E., and Benton, D., Health care delivery. J. Nurs. Regul. 7(4):S12–S16, 2017.

144. Schulmeister, L., Technology and the transformation of oncology care. Semin. Oncol. Nurs. 32(2):99–109, 2016.

145. Reeder, B., Meyer, E., Lazar, A., Chaudhuri, S., Thompson, H. J., and Demiris, G., Framing the evidence for health smart homes and home-based consumer health technologies as a public health intervention for independent aging : A systematic review. Int. J. Med. Inform. 82(7):565–579, 2013.

146. Albahri, O. S. et al., Systematic review of real-time remote health monitoring system in triage and priority-based sensor technology: Taxonomy, open challenges, motivation and recommendations. J. Med. Syst. 42(5):80, 2018.

147. Lounis, A., Hadjidj, A., Bouabdallah, A., and Challal, Y., Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. Futur. Gener. Comput. Syst. 55:266–277, 2016.

148. Saleem, K., Derhab, A., Al-Muhtadi, J., and Shahzad, B., Human-oriented design of secure machine-to-machine communication system for e-healthcare society. Comput. Hum. Behav. 51:977–985, 2015.

149. Albahri, A. S., Zaidan, A. A., Albahri, O. S., Zaidan, B. B., and Alsalem, M. A., Real-time fault-tolerant mHealth system: Comprehensive review of healthcare services, opens issues, challenges and methodological aspects. J. Med. Syst. 42(8):137, 2018.

150. Albahri, O. S., Zaidan, A. A., Zaidan, B. B., Hashim, M., Albahri, A. S., and Alsalem, M. A., Real-time remote health-monitoring Systems in a Medical Centre: A review of the provision of healthcare services-based body sensor information, open challenges and methodological aspects. J. Med. Syst. 42(9):164, 2018.

151. Zhang, K., Liang, X., Baura, M., Lu, R., and (Sherman) Shen, X., PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs. Inf. Sci. (Ny). 284:130–141, 2014.

152. Moreno, S., Quintero, A., Ochoa, C., Bonfante, M., Villareal, R., and Pestana, J., Remote monitoring system of vital signs for triage and detection of anomalous patient states in the emergency room, in *2016 XXI Symposium on Signal Processing, Images and Artificial Vision (STSIVA)*, pp. 1–5, 2016

153. Baehr, D., McKinney, S., Quirk, A., and Harfoush, K., On the practicality of elliptic curve cryptography for medical sensor networks, in *2014 11th Annual High Capacity Optical Networks and Emerging/Enabling Technologies (Photonics for Energy)*, pp. 41–45, 2014.

154. de la Piedra, A., Braeken, A., Touhafi, A., and Wouters, K., Secure event logging in sensor networks. Comput. Math. with Appl. 65(5):762–773, 2013.

155. Hedin, D. S., Kollmann, D. T., Gibson, P. L., Riehle, T. H., and Seifert, G. J., Distance bounded energy detecting ultra-wideband impulse radio secure protocol, in *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, vol. 2014, pp. 6619–6622, 2014.

156. Soufiene, B. O., Bahattab, A. A., Trad, A., and Youssef, H., Lightweight and confidential data aggregation in healthcare wireless sensor networks. Trans. Emerg. Telecommun. Technol. 27(4): 576–588, 2016.

157. Benmansour, T., Ahmed, T., and Moussaoui, S., Performance Evaluation of IEEE 802.15.6 MAC in Monitoring of a Cardiac Patient, in *2016 IEEE 41st Conference on Local Computer Networks Workshops (LCN Workshops)*, pp. 241–247, 2016.

158. Zughoul, O. *et al.*. Comprehensive Insights into the Criteria of Student Performance in Various Educational Domains. IEEE Access. 2018.

159. Yuen, P. C., Zou, W. W., Zhang, S. B., Wong, K. K. F., and Lam, H. H. S., Finger gesture recognition through sweep sensor, *Proc. 1st Int. Work. Interact. Multimed. Consum. Electron. - IMCE '09*, pp. 11–17, 2009.

160. Hupperich, T., Hosseini, H., and Holz, T., Leveraging sensor fingerprinting for mobile device authentication. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 9721:377–396, 2016.

161. Schwarting, M., Burton, T., and Yampolskiy, R., On the obfuscation of image sensor fingerprints. Proc. - 2015 Annu. Glob. Online Conf. Inf. Comput. Technol. GOCICT 2015:66–69, 2016.

162. Nader, J., Alsadoon, A., Prasad, P. W. C., Singh, A. K., and Elchouemi, A., Designing touch-based hybrid authentication method for smartphones. Procedia Comput. Sci. 70(28):198–204, 2015.

163. Zheng, N., Bai, K., Huang, H., and Wang, H., You are how you touch: User verification on smartphones via tapping behaviors, *Proc. - Int. Conf. Netw. Protoc. ICNP*, pp. 221–232, 2014.

164. Buriro, A., Crispo, B., DelFrari, F., and Wrona, K., Hold and sign: A novel behavioral biometrics for smartphone user authentication. Proc. - 2016 IEEE Symp. Secur. Priv. Work. SPW 2016:276–285, 2016.

165. Feng, T., Zhao, X., Carbunar, B., and Shi, W., Continuous mobile authentication using virtual key typing biometrics. Proc. - 12th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2013(21):1547–1552, 2013.

166. Ketabdar, H., Moghadam, P., Naderi, B., and Roshandel, M., Magnetic signatures in air for mobile devices, *Proc. 14th Int. Conf. Human-computer Interact. with Mob. devices Serv. companion - MobileHCI '12*, p. 185, 2012.

167. Maghsoudi, J., and Tappert, C. C., A behavioral biometrics user authentication study using motion data from android smartphones. Proc. - 2016 Eur. Intell. Secur. Inform. Conf. EISIC 2016:184–187, 2017.

168. Muaaz, M. and Mayrhofer, R., Orientation Independent Cell Phone Based Gait Authentication, *Proc. 12th Int. Conf. Adv. Mob. Comput. Multimed. - MoMM '14*, pp. 161–164, 2014.

169. Ali Fahmi, P. N., Kodirov, E., Choi, D. J., Lee, G. S., Mohd Fikri Azli A., and Sayeed, S., Implicit authentication based on ear shape biometrics using smartphone camera during a call, *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, no. 27, pp. 2272–2276, 2012.

170. Yang, H. et al., TapLock: Exploit finger tap events for enhancing attack resilience of smartphone passwords. IEEE Int. Conf. Commun. 2015(17):7139–7144, 2015.

171. Hussain, M. et al., The rise of keyloggers on smartphones: A survey and insight into motion-based tap inference attacks. Pervasive Mob. Comput. 25:1–25, 2016.

172. Watanabe, Y., and Houryu, T. F., Toward introduction of immunity-based model to continuous behavior-based user authentication on smart phone. Procedia Comput. Sci. 22(1):1319–1327, 2013.

173. Li, Y., Li, Y., Yan, Q., Kong, H., and Deng, R. H., Seeing Your Face Is Not Enough : An Inertial Sensor-Based Liveness Detection for Face Authentication, *ACM SIGSAC Conf. Comput. Commun. Secur.*, pp. 1558–1569, 2015.

174. Ahmad, M., Khan, A. M., Brown, J. A., Protasov, S., and Khattak, A. M., Gait fingerprinting-based user identification on smartphones. Proc. Int. Jt. Conf. Neural Netw. 2016:3060–3067, 2016.

175. Jain, A., and Kanhangad, V., Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touchscreen gestures. Pattern Recogn. Lett. 68:351–360, 2015.

176. Lee, W. and Lee, R. B., Multi-sensor Authentication to Improve Smartphone Security, *Conf. Inf. Syst. Secur. Privacy, IEEE,* pp. 1–11, 2015.

177. Shen, C., Li, Y., Chen, Y., Guan, X., and Maxion, R. A., Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication, *IEEE Trans. Inf. Forensics Secur.*, vol. 710049, 2017.

178. Roshandel, M., Haji-Abolhassani, A., and Ketabdar, H., MagiThings: Gestural interaction with mobile devices based on using embedded compass (magnetic field) sensor, *Emerg. Perspect. Des. Use, Eval. Mob. Handheld Devices*, 2015.

179. M. Wolff, Behavioral biometric identification on mobile devices, *2013 Int. Conf. Augment. Cogn.*, no. Icsai, pp. 783–791, 2013.

180. Pisani, P. H., Lorena, A. C., and De Carvalho, A. C. P. L. F., Adaptive algorithms in accelerometer biometrics. Proc. - 2014 Brazilian Conf. Intell. Syst. BRACIS 2014:336–341, 2014.

181. Abate, A. F., Nappi, M., and Ricciardi, S., I-Am: Implicitly Authenticate Me Person Authentication on Mobile Devices Through Ear Shape and Arm Gesture, *IEEE Trans. Syst. Man, Cybern. Syst.*, pp. 1–13, 2017.

182. Derawi, M. O., Nickely, C., Bours, P., and Busch, C., Unobtrusive user-authentication on mobile phones using biometric gait recognition, *Proc. - 2010 6th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIHMSP 2010*, pp. 306–311, 2010.

183. Islam, S., Naeem, U., and Amin, Y., Authentication of Smartphone Users Based on Activity Recognition and Mobile Sensing, *Sensors (Switzerland)*, 2017.

184. Haque, M. M., Zawoad, S., and Hasan, R., Secure techniques and methods for authenticating visually impaired mobile phone users. 2013 IEEE Int. Conf. Technol. Homel. Secur. HST 2013(14):735–740, 2013.

185. and T. M. P. Nguyen Ngoc Diep, Cuong Pham, "SigVer3D: Accelerometer based verification of 3-D signatures on mobile devices," vol. 326, pp. 353–365, 2015.

186. Nickel, C., Derawi, M. O., Bours, P., and Busch, C., Scenario test of accelerometer-based biometric gait recognition. Proc. 3rd Int. Work. Secur. Commun. Networks, IWSCN 2011:15–21, 2011.

187. J. R. Kwapisz, G. M. Weiss, and S. A. Moore, "Cell Phone-Based Biometric Identification," 2010.

188. Guerra-Casanova, J., Sánchez- Ávila, C., De Santos Sierra, A., and Del Pozo, G. B., Score optimization and template updating in a biometric technique for authentication in mobiles based on gestures. J. Syst. Softw. 84(11):2013–2021, 2011.

189. Guerra-Casanova, J., Sánchez-Ávila, C., Bailador, G., and de Santos Sierra, A., Authentication in mobile devices through hand gesture recognition. Int. J. Inf. Secur. 11(2):65–83, 2012.

190. Tamviruzzaman, M., Ahamed, S. I., Hasan, C. S., and O'brien, C., ePet: When cellular phone learns to recognize its owner. Proc. 2nd ACM Work. Assur. usable Secur. Config.:13–18, 2009.

191. M. O. Derawi, P. Bours, and K. Holien, "Improved cycle detection for accelerometer based gait authentication," *Proc.* - 2010 *6th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIHMSP* 2010, pp. 312–317, 2010.

192. W.-H. L. and R. B. Lee and Princeton, "Implicit Authentication for Smartphone Security," *Commun. Comput. Inf. Sci.*, vol. 576, pp. 160–176, 2015.

193. Dhanakoti, V., and Manju Priya, R., Mobile handswing pattern. Int. J. Control Theory Appl. 9(5):2497–2507, 2016.

194. A. J. Aviv, B. Sapp, M. Blaze, and J. M. Smith, "Practicality of accelerometer side channels on smartphones," *Proc. 28th Annu. Comput. Secur. Appl. Conf. - ACSAC '12*, p. 41, 2012.

195. Nixon, K. W., Chen, X., Mao, Z. H., Chen, Y., and Li, K., Mobile user classification and authorization based on gesture usage recognition. Proc. Asia South Pacific Des. Autom. Conf. ASP-DAC 11:384–389, 2013.

196. Sagar, M., and Kumar, S., Gait biometrics as an authentication in smartphones. Res. India Publ. J. 10(55):2954–2959, 2015.

197. Y. Zhong, Y. Deng, and G. Meltzner, "Pace independent mobile gait biometrics," *2015 IEEE 7th Int. Conf. Biometrics Theory, Appl. Syst. BTAS 2015*, 2015.

198. Hoang, T., Nguyen, T., Luong, C., Do, S., and Choi, D., Adaptive cross-device gait recognition using a mobile accelerometer. J. Inf. Process. Syst. 9(2):333–348, 2013.

199. Hoang, T., Choi, D., and Nguyen, T. D., On the instability of sensor orientation in gait verification on Mobile phone. Secrypt: 148–159, 2015.

200. G. Bajrami, M. O. Derawi, and P. Bours, "Towards an automatic gait recognition system using activity recognition (wearable based)," *2011 Third Int. Work. Secur. Commun. Networks*, pp. 23–30, 2011.

201. J. G. Casanova, C. S. Ávila, A. De Santos Sierra, G. B. Del Pozo, and V. J. Vera, "A real-time in-air signature biometric technique using a mobile device embedding an accelerometer," *Commun. Comput. Inf. Sci.*, vol. 87 CCIS, no. PART 1, pp. 497–503, 2010.

202. Nickel, C., and Busch, C., Classifying accelerometer data via hidden Markov models to authenticate people by the way they walk. IEEE Aerosp. Electron. Syst. Mag. 28(10):29–35, 2013.

203. E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang, "ACCessory: Password Inference Using Accelerometers on Smartphones," *Proc. Twelfth Work. Mob. Comput. Syst. Appl.*, p. 9:1–9:6, 2012.

204. P. Chen, Pande, A., and Mohapatra, "Sensor-Assisted Facial Recognition : An Enhanced Bio- metric Authentication System for Smartphones," *Proc. 12th Annu. Int. Conf. Mob. Syst. Appl. Serv. MobiSys '14*, pp. 109–122, 2014.

205. M. Muaaz and R. Mayrhofer, "Accelerometer based Gait Recognition using Adapted Gaussian Mixture Models," *Proc. 14th Int. Conf. Adv. Mob. Comput. Multi Media - MoMM '16*, pp. 288–291, 2016.

206. C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-NN algorithm," *Proc. 2012 8th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIH-MSP 2012*, pp. 16–20, 2012.

207. Watanabe, Y., Influence of holding smart phone for acceleration-based gait authentication. Proc. - 2014 Int. Conf. Emerg. Secur. Technol. EST 2014:30–33, 2014.

208. R. Kumar, V. V. Phoha, and A. Jain, "Treadmill attack on gait-based authentication systems," *2015 IEEE 7th Int. Conf. Biometrics Theory, Appl. Syst. BTAS 2015*, 2015.

209. Muaaz M.; Mayrhofer R., "Cross Pocket Gait Authentication Using Mobile Phone Based Accelerometer Sensor," *2015 Int. Conf. Comput. Aided Syst. Theory*, pp. 731–738, 2015.

210. Sanzziri, A., Nandugudi, A., Upadhyaya, S., and Qiao, C., SESAME: Smartphone enabled secure access to multiple entities. 2013 Int. Conf. Comput. Netw. Commun. ICNC 2013(7):879–883, 2013.

211. F. Rahman, M. O. Gani, G. M. T. Ahsan, and S. I. Ahamed, "Seeing Beyond Visibility: A Four Way Fusion of User Authentication for Efficient Usable Security on Mobile Devices, " *2014 IEEE Eighth International Conference on Software Security and Reliability-Companion* pp. 121–129, 2014.

212. C. Lyu, A. Pande, X. Wang, J. Zhu, D. Gu, and P. Mohapatra, "CLIP: Continuous location integrity and provenance for mobile phones," *Proc. - 2015 IEEE 12th Int. Conf. Mob. Ad Hoc Sens. Syst. MASS 2015*, pp. 172–180, 2015.

213. Witte, H., Rathgeb, C., and Busch, C., Context-aware Mobile biometric authentication based on support vector machines. 2013 Fourth Int. Conf. Emerg. Secur. Technol. 6:29–32, 2013.

214. Zhu, J., Wu, P., Wang, X., and Zhang, J., "SenSec: Mobile security through passive sensing," *2013*. Int. Conf. Comput. Netw. Commun. ICNC 2013(9):1128–1133, 2013.

215. Hoang, T., Choi, D., and Nguyen, T., Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. Int. J. Inf. Secur. 14(6):549–560, 2015.

216. Shila, D. M., Srivastava, K., O'Neill, P., Reddy, K., and Sritapan, V., A multi-faceted approach to user authentication for mobile devices — Using human movement, usage, and location patterns. 2016 IEEE Symp. Technol. Homel. Secur. 22:1–6, 2016.

217. Yang, L. et al., Unlocking smart phone through Handwaving biometrics. IEEE Trans. Mob. Comput. 14(5):1044–1055, 2015.

218. A. Guerra-Casanova, J., Sanchez-Avila, C., Bailador Del Pozo, G., & De Santos-Sierra, "A sequence alignment approach applied to a Mobile authentication technique based on gestures," Int. J. Pattern Recognit. Artif. Intell., vol. 27, no. 04, p. 1356006, 2013.

219. T. Feng, V. Prakash, and W. Shi, "touch panel with integrated fingerprint sensors based user identity management," *2013* IEEE Int. Conf. Technol. Homel. Secur. HST 2013, no. 12, pp. 154–160, 2013.