Journal of Engineering Research 13 (2025) 741–750

Contents lists available at ScienceDirect

Journal of Engineering Research

journal homepage: www.journals.elsevier.com/journal-of-engineering-research

Sensor-based authentication in smartphone: A systematic review

Moceheb Lazam Shuwandy [a,*], A.S. Jouda [b], M.A. Ahmed [a], Mahmood M. Salih [a], Z.T. Al-qaysi [a], A.H. Alamoodi [c,e,h], Salem Garfan [d,*], O.S. Albahri [f,g], B.B. Zaidan [i,j], A.S. Albahri [k,l]

[a] Computer Science Department, College of Computer Science and Mathematics, Tikrit University (TU), Tikrit, Iraq
[b] Salahaddin Health Office, Ministry of Health, Tikrit, Iraq
[c] MEU Research Unit, Middle East University, Amman, Jordan
[d] Faculty of Computing and Meta-Technology (FKMT), Universiti Pendidikan Sultan Idris (UPSI), Perak, Malaysia
[e] Hourani Center for Applied Scientific Research, Al-Ahliyya Amman University, Amman, Jordan
[f] Victorian Institute of Technology, Australia
[g] Computer Techniques Engineering Department, Mazaya University College, Nasiriyah, Iraq
[h] Applied Science Research Center, Applied Science Private University, Amman, Jordan
[i] SP Jain School of Global Management, Lidcombe, Sydney, NSW 2141, Australia
[j] International Graduate School of Artificial Intelligence, National Yunlin University of Science and Technology, Douliu, Taiwan, ROC
[k] Technical College, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq
[l] Iraqi Commission for Computers and Informatics (ICCI), Baghdad, Iraq

ARTICLE INFO

Keywords:
Password
Authentication
Privacy
MHealth
Touch Sensor
Microphone Sensor

ABSTRACT

With the widespread usage of smartphones, users not just using their smartphone for calls and messaging only, but they are using it for a variety of purposes such as banking transactions, e-mailing, chatting, online shopping, video conferencing, health monitoring, and many more. Most of these activities store personal and sensitive data of the user on the device, reaching this confidential information by unauthorized person may cause huge losses and bad consequences. Therefore, securing the smartphone's accessibility from unauthorized people became an extremely essential. With the advanced development in the area of sensor-based smartphone authentication methods, different methods were developed to be easily used by users through specific criteria. However, many aspects haven't been discovered yet in the area of sensor-based smartphone authentication methods. On the basis of that, this study aims to review the area of sensor-based smartphone authentication methods systematically to provide a comprehensive understanding of this new area and to discuss the current challenges and issues. To conduct this systematic review, four scientific digital databases were utilized; ScienceDirect, IEEE Xplore, Web of Science, and Scopus. The total number of studies found was $n = 256$ articles, only $n = 46$ articles were included based on our inclusion criteria. To provide a comprehensive understanding of the included studies, taxonomy was drawn. Also, this study provides a discussion on the current motivations, challenges and issues, and recommendations in sensor-based smartphone authentication methods. This review enlightens, encourage, and direct researchers to develop authentication solutions and reduce the current gaps in this area.

1. Introduction

In previous years, the area of sensors-based smartphones authentication has been getting a huge intention by researchers and developers [1]. With the widespread usage of smartphones, users not just using their smartphone for calls and messaging only, but they are using it for a variety of purposes such as banking transactions, e-mailing, chatting, online shopping, video conferencing, health monitoring, and many more [2]. Most of these activities store personal and sensitive data of the user on the device, reaching these confidential information by unauthorized person may cause huge loses and bad consequences [2,3]. Therefore, securing the smartphone's accessibility from unauthorized people became an extremely essential [4]. The potential risk of data being vulnerable to cyberattacks is a major challenge. This may occur due to software infection or lack of user diligence. Therefore, it is important to improve smartphone access policy. Authentication mechanism secures that the user is the legitimate one. Traditionally, users attempt to secure their phones using PINs, passwords, or patterns [5,6]. With the

* Corresponding authors.
E-mail addresses: moceheb@tu.edu.iq, moceheb@yahoo.com (M.L. Shuwandy), salem.g@meta.upsi.edu.my, salem.garfan@gmail.com (S. Garfan).

https://doi.org/10.1016/j.jer.2024.02.003
Received 11 August 2023; Received in revised form 29 January 2024; Accepted 7 February 2024
Available online 9 February 2024

development of different smartphone sensors (e.g. orientation sensors, camera sensors, finger sensors, microphone sensors, touchscreen sensors and 3D touchscreen sensors) [7], researchers have attempted to utilize these sensors in developing new ways for authentication mechanisms to improve the usability and security [2,8-11]. Currently, biometric based authentication solutions are promising techniques to replace traditional authentication mechanisms due to the traditional methods are based on personal identification passwords, which are usually considered inconvenient by users. Biometric techniques compared to traditional methods considered more reliable and capable in recognizing an authorized person and imposter by verifying the identity of the owner rather than just confirming the knowledge of the user's password [12,3,13,14]. Utilizing biometric methods can efficiently prevent unauthorized access to smartphone internal resources and identity theft [15-18]. With the variety usage of sensors, new ways of protecting smartphone devices were developed. User recognition methods were developed by researchers without requiring identification made by the detection of the user's gesture [19], gait [20], or fingertip [14]. Further, some researchers developed authentication methods based on the behavior of the user. Authentication includes four sections; mechanism authentication [8,21], implicit authentication [22,23], continuous authentication [11,24], and hybrid tracking [25,26]. With the advanced development in the area of sensor-based smartphone authentication methods, different methods were developed to be easily used by users through specific criteria [22,24,27,28]. However, many aspects haven't been discovered yet in the area of sensor-based smartphone authentication methods. On the basis of that, this study aims to review the area of sensor-based smartphone authentication methods systematically to provide a comprehensive understanding of this new area and to discuss the current challenges and issues. This review may enlighten other researchers to develop solutions and reduce the current gaps. Also, this study presents recommended solutions to direct researchers on the right way to fill the different gaps in this field of interest. This research presents various noteworthy contributions. In the first place, it carries out a methodical examination, providing comprehensive insights into diverse sensor-driven techniques for authenticating smartphones. Secondly, it devises a classification system that organizes the existing body of literature in this domain, furnishing a structured framework for comprehending the differing approaches. Thirdly, it identifies the present motivations, challenges, and issues linked to sensor-driven authentication, which can serve as a roadmap for future research endeavors. Lastly, the investigation puts forth potential remedies to bridge the gaps in the field of sensor-driven smartphone authentication. Collectively, these contributions serve to advance knowledge and comprehension in this specific area.

2. Systematic review

This research is based on systematic literature review protocol. This type of review promotes a comprehensive and detailed understanding about a certain topic of discussion in order to facilitate deep understanding [29]. Systematic review not only is known for its methodological robustness but also its capability to be adopted in different research domains and areas [30], including sensor based authentication which is the mains scope of this research. Accordingly, this research presents published academic research focused on sensors in smartphones used for authentication. It is carried out as a follow-up to Shuwandy's 2019 systematic review [4]. This systematic review aims to establish a categorization of academic literature to identify research needs in this area. In addition, the challenges, motivations, and recommendations are included. Sensor-based authentication is a trending academic topic. The keyword for this research is "***sensor-based smartphone***," which excludes all non-smartphone devices. The English-language literature constraints this range. Consequently, all authentication-related areas, including the broad category of passwords and sensor types, are evaluated and used as keywords to protect information related to sensor-based smartphones.

2.1. Information sources

The target article search was carried out using four digital databases; (1) ScienceDirect database, which contains articles from scientific and technical journals; (2) IEEE Xplore library of engineering and technology technical papers; (3) Web of Science (WoS) service, an indexing database that covers a wide range of academic disciplines; and (4) SciVerse Scopus, an indexing database that covers a variety of academic disciplines. These databases were chosen based on their academic robustness and accommodation of different research works which correlated with the scope of this research.

2.2. Study selection

The sources for this research were carefully screened from the literature. The research was conducted on six years period between 2017 to 2023. Articles were checked and filtered to exclude duplicates and those unrelated to this research. Following that, full-text reading was performed.

2.3. Search scenario

The search was carried out in May 2017 using the search boxes of the databases ScienceDirect, IEEE Xplore, Web of Science, and Scopus. Keyword combinations were utilized in groups. The first set contains the terms: "*sensor-based mobile*", "*accelerometer*", "*gyroscope*", "*magnetometer*", "*proximity sensor*", "*light sensor*", "*barometer*", "*thermometer*", "*air humidity sensor*", "*pedometer*", "*heart rate monitor*", and "*fingerprint sensors*"; which are merged by the "OR" operator. The second set contains the terms: "*password*", "*lock pattern*", "*PIN code*", "*full-blown password*", "*fingerprint*", "*facial recognition*", and "*authentication*"; which are merged using the "OR" operator. The third group contains the terms: "mobile", "smartphone", "hand phone", "smart phone", and "handphone"; the "OR" operator is used to join these keywords. The "AND" operator joins the three groups.

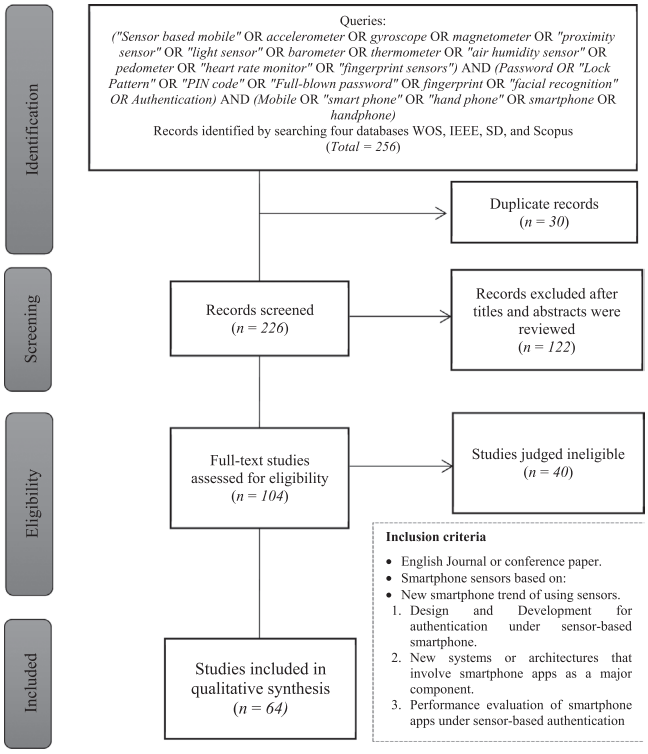

Fig. 1. SLR Protocol.

This query is shown in Fig. 1. Each database's choices are evaluated. Books, reports, and contents that appear in the search results are not included. However, the most recent journal papers and conferences are used, and only the most relevant are selected for this research.

2.4. Eligibility criteria

The criteria described in Fig. 1 were followed and applied to each article. Every article that satisfied the criteria was included. A plan was devised to reach a goal from which the research can be covered in four categories to protect the privacy of smartphones that operate on sensors. ScienceDirect database was used to obtain the views and trends in the literature entitled "*Sensor-based mHealth authentication for real-time remote healthcare monitoring system: A multilayer systematic review*". Initially, duplicates were removed, and then the articles that did not satisfy the criteria of eligibility within the stages of screening and filtering were excluded. The exclusion criteria included non-English articles and articles that focused on a specific aspect of smartphone that does not use any type of sensor in authorization.

2.5. Data collection process

All of the included articles from various sources were utilized to improve this research. A few full-content reads resulted in a large collection of features and comments on these works and a refined scientific classification of the papers. Finally, the most important findings have been summarized, organized, and presented. The essential data was recorded in Word and Excel formats and comprised a complete list of articles, their respective source databases, summary, and description tables, categorization tables, purposes, review sources, target platforms, audiences, and other statistics.

3. Taxonomy of research literature

In this research, the first result from the query search revealed ($n = 256$) articles published between 2017 and 2022; from Science Direct, 34.38% ($n = 88/256$) articles; from IEEE Xplore, 27.73% ($n = 71/256$) articles; from WoS, 1.95% ($n = 5/256$) articles; and from Scopus, 35.94% ($n = 92/256$) articles. Total of 11.72% ($n = 30/256$) duplicated articles were discovered from the four libraries. After screening the titles and abstracts, 53.98% ($n = 122/226$) were eliminated, leaving just 46.02% ($n = 104/226$) of the articles. Reading the full content resulted in removing 38.46% ($n = 40/104$) of the articles, leaving just 61.54% ($n = 64/104$) of the articles, see the Fig. 2 below.

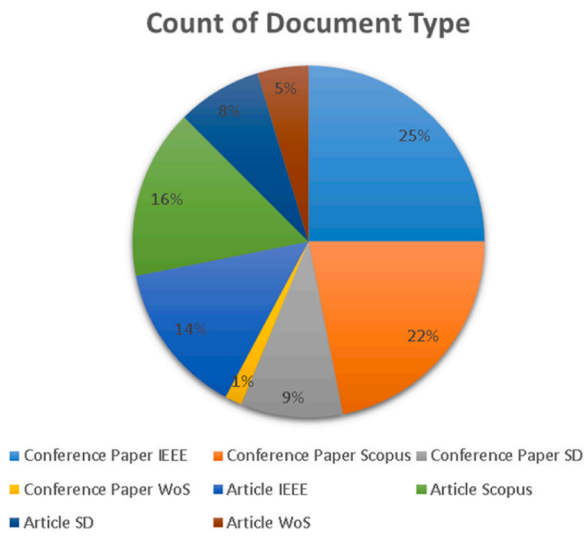

Fig. 2. Distribution of Articles by Database.

The findings of this analysis reveal the three primary research articles categories in term of taxonomy, as shown in Fig. 3, which are (1) defense, (2) attack, and (3) others. The "***defense***" category contains research papers that focus on defending the smartphone from attackers, whereas the "***attack***" category contains research articles that use smartphone sensors to attack the phone. Articles on the evolution of defense are included in the "***others***" category. The sort of sensors employed in the development, however, remains unknown.

3.1. Defense articles

The articles discussing smartphone protection by utilizing built-in sensors are the main aspect of discussion. The defense group is divided into seven groups according to the type of sensor used. Amongst the discussed sensors comes the (1) *Orientation sensor*, which contains many sensors such as the (i) *accelerometer*, (ii) *gyroscope*, and (iii) *magnetic*. Another type of discussed articles is those who utilize (2) *Fingerprint sensor* to acquire smartphone authorization. Furthermore, another group of papers is utilizing (3) *Camera sensor*. Moreover, the fourth series of papers focuses on the use of a (4) *Touchscreen sensor*. These articles discuss the pattern for obtaining authentication when using a password to access mobile data. The fifth set of articles is about utilizing a (5) *3D Touchscreen sensor*. Furthermore, the following group employs (6) Microphone sensors. Finally, the final set of articles in the defensive group is about the (7) *Light sensor*.

3.1.1. Orientation sensor

The largest number of articles is about using the orientation sensor 91.23% ($n = 52/57$) articles, which includes many sensors such as the *accelerometer*, *magnetic* and the *gyroscope*. In this category, 84.62% ($n = 44/52$) of the articles is about behavior authentication, and the sensor-based gait authentication accounts for 15.38% ($n = 8/52$) of the articles. The details of each category are presented as follows.

3.1.1.1. Behavior authentication. Behavioral biometrics measures distinct and comparable patterns of human behavior. Physical biometrics, such as finger or iris patterns, is referred to as biometrics slightly differently. Biometric confirmation techniques include pressure dynamics, gait and signature analysis, voice identification, mouse use features, and cognitive. Biometrics is used for secure authentication in government, corporations, financial institutions, retail, and other environments. The articles in the behavior authentication group are divided into the following five parts: (1) *continuous authentication* with 45.45% ($n = 20/44$) articles, (2) *implicit authentication* with 4.55% ($n = 2/44$) articles (3) *activity behavior recognition* with 40.91% ($n = 18/44$) articles (4) *hybrid authentication* with 4.55% ($n = 2/44$) articles and (5)

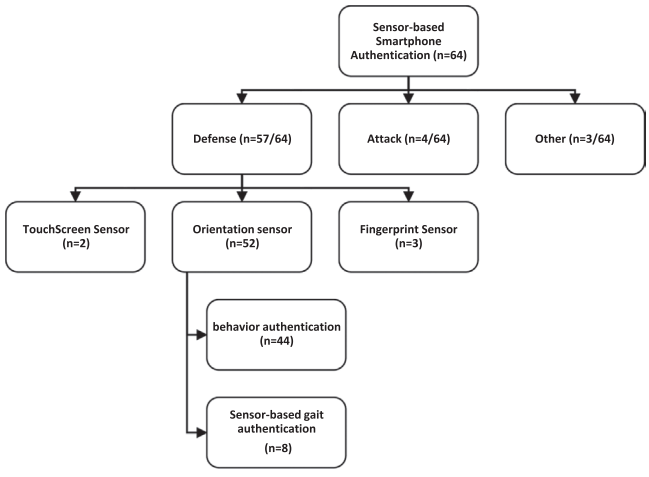

Fig. 3. Taxonomy of research literature.

Keystroke Dynamics with 4.55% ($n = 2/44$) articles Some studies focus on hand gestures for signature [14]. Fig. ↱4 and Fig. ↱5, shows behavioral authentication [22,31-36], Fig. ↱6, gait recognition of continuous authentication [26,37-39].

3.1.1.2. Sensor-based gait authentication. A person's gait represents their motion when using a smartphone with an accelerometer sensor to authenticate the device, such sensor type is used for biometric authentication. Articles in the defense category have sensor-based gait authentication covering 7.02% ($n = 4/57$); [27].

3.1.2. Fingerprint sensor

The defense group accounts for 5.26% ($n = 3/57$) of articles in this category. Others discuss hazard-based verification systems for mobile phones. These systems fail to provide reliable device-related data for testing [42]. This is a limited, conservative, and cost-effective feature set analyzed in another article [43]. On the one hand, any potential threat is identified. On the other hand, however, the steps required to address that security flaw are identified [44].

3.1.3. Touchscreen sensor

A total of 3.51% ($n = 2/57$) of articles in this category are from the defense group. Touch gestures and key typing are both types of user authentication contents. Dynamic finger-drawn signature verification model to enhance user authentication on touch devices [37]. The proposed system uses a phone and the client's finger-draw to sign or write on the touchscreen [31].

3.2. Attack articles

We found articles about smartphone attacks using sensors or gaps. 6.25% ($n = 4/64$) of articles fall into this category. These articles show to expand capacitive touchscreens while enduring surfing assaults, Analysis of the potential of fingerprints are used as attack a mobile phone fingerprint recognition and evolution the fingerprint detection [45]. Fingerprint attacks on iOS and Android (Google Pixel 2 and 3) devices using calibration result in an unchangeable device fingerprint that may be used in many places, such as in applications and websites [10]. The user authentication experiments use touch operational features and some accelerometer features [35].

3.2.1. Others research related to sensor

Reviews of sensors, for example, fall into this category. So, these articles weren't analyzed. Consider that these articles are not about sensor-based smartphone authentication. Identifying the purpose of seeking articles with sensor-based smartphones.

4. Discussion

The research aims to update the substructure of smartphone sensors based on authentication techniques and research advances. Amongst the most important elements come the motivations, challenges and recommendations encountered by researchers in this domain.

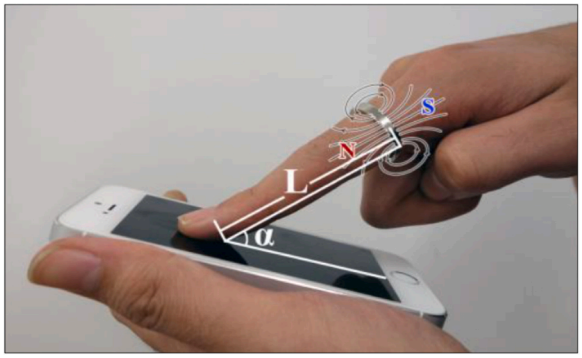

Fig. ↱4. Behavioral Authentication of Magnetic and touchscreen sensors [22].

4.1. Motivations

Research in smartphone authentication is exciting. It depicts some of the literature characteristics, which have groups base on advantages. The articles' motivations divide into five categories: (1) smartphone usability, (2) smartphone security, (3) sensor authentication usability, (4) sensor security, and (5) app activities. We elaborate on the advantages of article motivation in the following paragraphs, see Fig. 7 above.

4.1.1. Smartphones usability

Smartphones are omnipresent in both the workplace and the home. In addition, individuals typically keep sensitive and confidential information on their phones. As a result, authenticating phone users and preventing impostors is critical [21,46]. Ubiquitous mobile devices such as smartphones and tablets are often unprotected against unwanted access Because people avoid using passwords and PINs because they are inconvenient [21,42]. Smartphones, tablets, and portable computers have proliferated quickly during the past decade. Because smartphones contain a significant amount of sensitive private information, user authentication is becoming more vital to avoid attacks by unauthorized users, such as motion-based inference attacks [27,31,38,47]. A mobile device is a dominant model that enables a person to communicate with the outside world [23,48]. The theory of Around-Device Interaction (ADI) has recently gained much interest in human-computer interaction (HCI) because ADI goes beyond a device's peripheral area and provides a touchless user interface as an alternative to conventional data-entry methods [22,43,49,50]. Globally, about 4.78 billion mobile phone used in 2020 [51]. Many individuals use smartphones to access their bank accounts, social media, and personal data. However, it is possible not secure enough of these devices [23,45,48,52,53]. Smartphones are constantly improving and adding new features. These include high-quality cameras, boosting app runs, and the quantity of critical data saved [54]. In recent years, sales of these devices have risen as well. Many services now utilize these smartphones to access social media, shopping, banking, health, fitness monitoring, and personal data [47, 55-57]. For many tasks every day, identity verification is needed, and most individuals want to be verified without memorizing a PIN. Secured data on mobile devices nowadays includes personal and commercial data. The need for safe and accessible authentication methods for ongoing protection is emphasized as smartphones are increasingly used like PC platforms to access sensitive information [27,28,56]. An unlock pattern or passcode uses to safeguard these valuable assets. However, since these processes are deemed obstructive, locked devices; especially, when using a 3D Touchscreen when forgetting three levels of pattern locks consider a big challenge [8,9,21,27,35,40,56]. Mobile phones are considered essential in our everyday life [17], [27,40]. Smartphones are context-aware devices that enable users to do regular activities like receiving and sending emails anywhere and anytime. The task's nature has changed as smartphone sensing, and processing capabilities have increased exponentially [24]. Almost everyone has a mobile phone, which they use to socialize and do business utilizing the mobile applications (APP) installed on the phone [28]. The number of blind or disabled smartphone users is unclear but expected to rise. Many disabled users, especially the visually impaired, have flocked to this technological innovation. [14,58]. Mobile devices are becoming increasingly popular. Smartphones and other portable and wearable devices are available on the market [59]. Smartphones allow people to go virtually anywhere at any time. Mobile devices have many different sizes, designs, input controls (displays), and the capacity to store large amounts of data, including sensitive personal information such as bank accounts or emails [39]. Personal and sensitive data such as project details, emails, and business contacts are often incorporated in a smartphone business

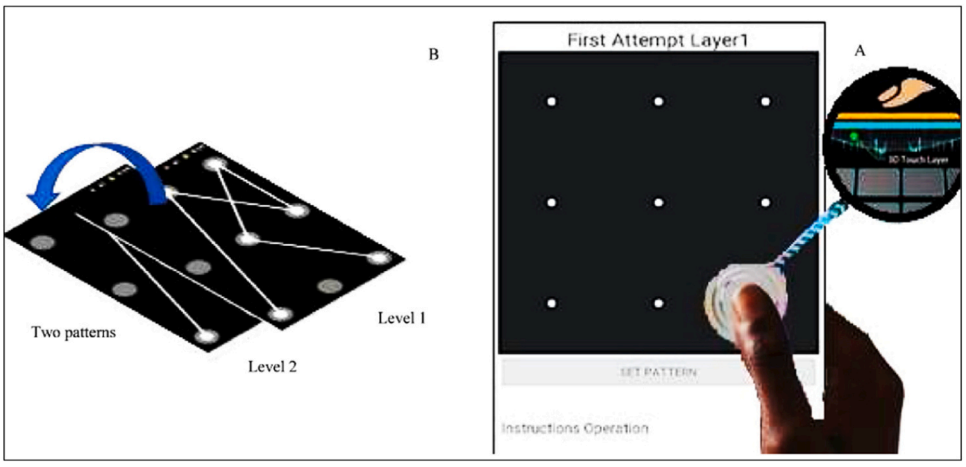

Fig. 5. The Behavior Authentication Pattern in (A) and (B) [40].

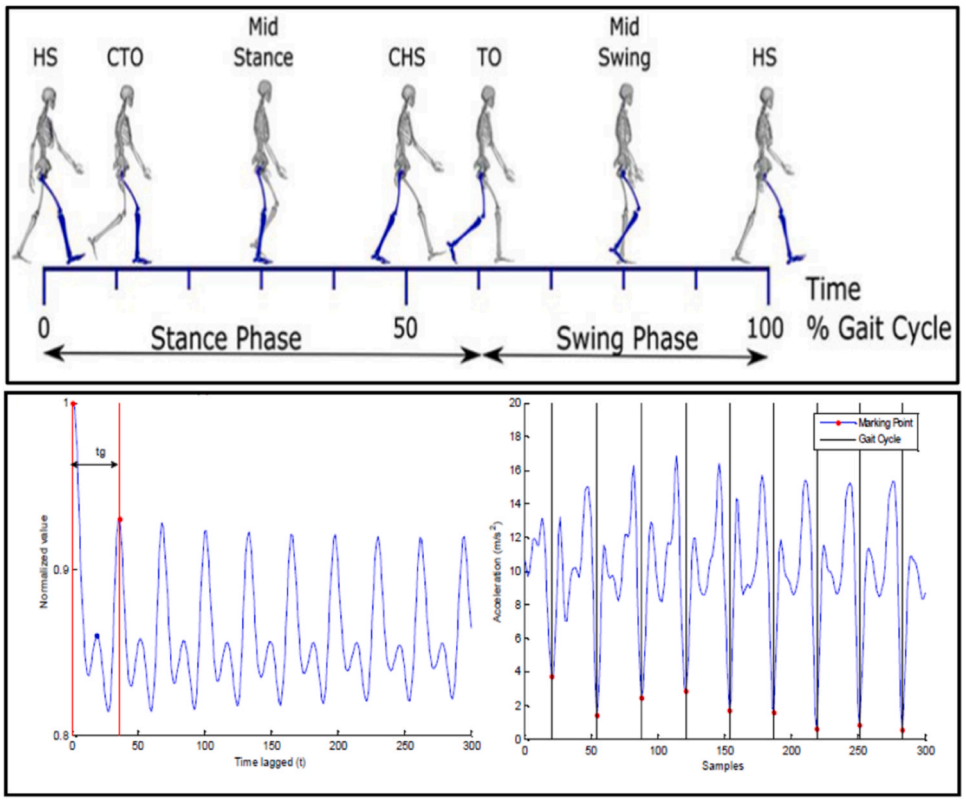

Fig. 6. Gait Recognition by Gait Cycle [41].

situation. However, private environments have a lot of sensitive data. The volume of sensitive data saved on smartphones increases in a specific context, making their security-critical [56]. Due to their cheap cost and ease of use, these devices provide novel interaction model [52]. Every year, the global smartphone adoption rate accelerates. The first quarter of 2019 saw record sales of 225 million smartphones, breaking all prior records. Moreover, sales of smartphones surpassed 1.93 billion in 2019. In addition to increased sales, these devices' services (personal and business) have increased [53].

4.1.2. Security impact on smartphones

Numerous attack routes and countermeasure methods have been investigated for mobile phones in recent years [60]. A growing quantity of sensitive information is being sent through mobile digital devices, according to Rayani 2020 [39]. He found additional privacy and security concerns. Hackers committed 40% of data breaches recorded in January 2020 [61]. As a result of these alarming figures, sensitive data should be handled independently of a possibly compromised operating system while monitoring physical device events for suspected illegal usage. Passwords, for example, only secure the login point [62]. Since smartphones are so widely used, they must be protected against illegal usage [51,63]. Mobile phone safety has been raised due to new features and functions. Increasingly, people want Internet access, apps, and services. In this way, the smartphone is vulnerable to numerous dangers, including the capacity to authenticate through a PIN or password [39, 64,65]. Remembering passwords and dealing with privacy problems arising from stolen or counterfeit biometrics has spawned a new concept for future authentication systems. Someone who takes or discovers a

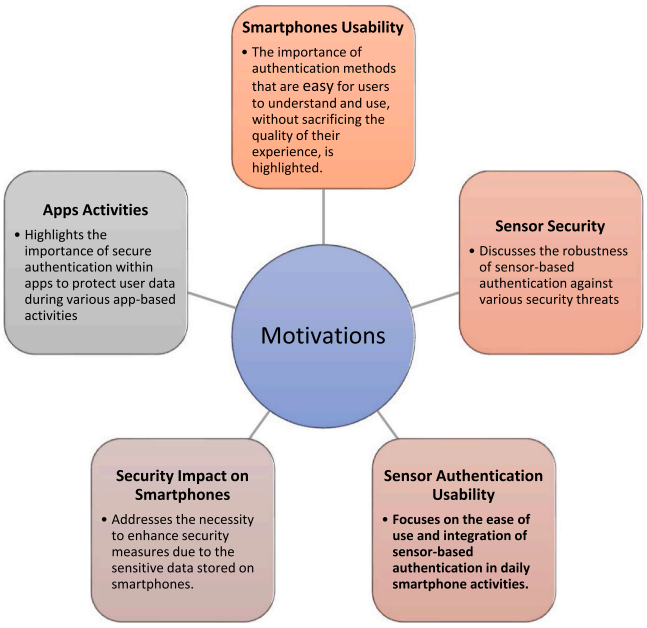

Fig. ꝑ7. Shows a Summary of Motives.

phone may be an attacker. It may be a family member, coworker, or acquaintance. Transparency is required in new systems, and implicit authentication is required [24,66]. To prevent data theft, biometrics is used to unlock cellphones upon startup. Modern phones include display lock and unlock capabilities to prevent accidental operations and protect personal data from being accessed. In order to unlock the smartphone, certain actions, movements, or fingerprints must be shown.

4.1.3. *Sensor authentication usability*

Sensors are becoming more sophisticated as mobile devices evolve rapidly. The newest smartphone models include GPS, vision cameras, microphones, light, 3D Touchscreen and acceleration sensors, among others [37,40]. Numerous sensors allow a wide range of interactions on modern smartphones. However, several of these sensors lack human input access [8]. These characteristics are extracted by several contemporary mobile sensors [15]. For individuals who dislike using PINs or passwords, biometric authentication may be a viable alternative [44]. Contrast this with non-biometric techniques that depend on the owner's knowledge or secrecy to establish his identity. Behavioral and physiological biometrics are both kinds. These techniques may successfully prevent ID theft and illegal access to mobile terminal resources [39]. Biometrics-enabled smartphones are widely accessible, lowering the cost of biometric sensors [14,46]. The accelerometers integrated directly in the user's typical motion demonstrate the tremendous potential of non-invasive gait biometrics assessments [26,38,41,67]. Aside from the accelerometer, cellphones users have other options for establishing authentication [54]. For detecting activity, accelerometers have become a vital instrument.

4.1.4. *Sensor security*

The risk of losing a phone compromises personal data security. Thus, the built-in orientation sensor usage for user authentication was investigated. Gait-based authentication has extensively used smartphone sensors (e.g., accelerometers and gyroscopes) [26]. In 2020, Shuwandy developed a 3D Touchscreen-based mobile device authentication technique. The 3D Touchscreen is generated manually on the touchscreen using a finger press pressure [40]. Each smartphone user has a unique way of clicking the touch displays [13]. The intensity, rhythm, and corner of the desired applied force represent personal tendencies. Smartphones featuring gyroscopes, accelerometers, and touchscreens efficiently record user activity [63]. Depending on the motion sensor, the movement of the finger may be evaluated [18]. The technology authenticates by tracking the user's stride pattern and location. The system interacts with the device's user by providing a password of emotions that cannot be utilized if the device's location traces or gait pattern are flawed. If the user fails to give correct behavior, the system asks about the previously recorded picture context description [55]. Sensor noise has been used to identify and authenticate devices. They mostly happened in smartphone sensors like gyroscopes and light sensors. Utilizing numerous sources, a third party may efficiently monitor user movements without cookies [68]. The mobile device's accelerometer and gyro sensors capture the gesture's displacement and rotation. This creates a sensor fingerprint for the user. The device is rotated and moved every time one of the 46 unlocking gestures is used. Apple's Touch ID sensor allows fingerprinting on iPhone 5 s, 6 Plus, and other iOS devices, although it is accessible on most smartphones. Unsafe Smartphone Password Systems: New Research [69].

4.1.5. *Apps activities*

These smartphone applications were made to help users [46]. Smartphone motion sensors monitor the phone's location in space in gaming applications [70]. Activity recognition is a hot research subject with healthcare, fitness, industrial, security, and entertainment [9,53,67]. Automatic gait analysis often uses accelerometry. Many popular smartphone applications utilize location-based features to entice users. Access management, authentication, and advertising are examples of location-based mobile apps [71]. Thus, these applications effectively safeguard key processes from real-world infection [72]. They are commonly employed in software-based authentication systems since they need minimal training. This raises the question of how effectively existing authentication techniques prevent unauthorized access. Smartphone sensors can answer questions perfectly. Smartphones' numerous sensors may gather personality data. Most people's habits are influenced by their environment [73].

4.2. *Challenges*

Sensor-based smartphones that authenticate client access to the device do not provide adequate data security. Sensors and their use in security have been the subject of several academic studies. The main

Fig. ꝑ8. Shows a Summary of Challenges.

challenges are categorized and reported in the following subsections, see the Fig. 8 below.

4.2.1. Data access

Data access presents a significant obstacle in the realm of authentication. In 2019, the failure of devices employing explicit authentication mechanisms led to unauthorized access to sensitive data and services [25,66,71,74]. This issue disproportionately affects the elderly and disabled, who are at risk of having their medical records compromised due to the lack of password protection [9,21,52,55]. When mobile phones are stolen, the stored passwords enable perpetrators to misuse the device's services and access private information. The security of such devices is thus of paramount importance [25]. The context-aware system's image-dragging feature simplifies the authentication process by using positional coordinates, avoiding complex classification tasks [9]. The challenge lies in the inherent difficulty that elderly and physically disabled users face with conventional screen patterns and PIN codes, which makes explicit authentication methods impractical for them [21, 68]. Ensuring that data is protected and accessible only to legitimate users on their smartphones is a critical concern [75]. While an unobtrusive authentication system improves usability, it may compromise security access control. Nevertheless, usability remains a key factor for smartphone users who prefer not to disrupt their activities for identity verification [28,50,75,76]. It is essential to strike a balance between security and accessibility to ensure that data on smartphones is safeguarded and exclusively available to authorized individuals [50].

4.2.2. Data protection

Security risks in relation to mobile devices emerge on a regular basis, posing a serious threat to user privacy and information security when the device is lost or stolen [9,21,77]. In addition to security and data protection, developing new authentication techniques requires an improved user-friendly authentication process with less user involvement in the authentication process [11,55,75,76]. The user authentication system enables the implicit identification module to retain the memory-based response and store it in a secure area; most of the time, environmental and biometric measurements can also be relied on to verify security [14,17,28,50]. This condition can lead to the following two issues. For first off, passwords are the most common source of security sensitivity because they are so easy to reuse or guess, share with others, and are vulnerable to social engineering attacks. Second, in order to secure applications or data on a smartphone device, the mobile system requires full authentication, which causes serious usability issues [55]. Mobile applications should continue to operate while protecting users' privacy in a non-intrusive and simple manner. These are the challenges that mobile computing platforms will face in the future [37, 57,62,65].

4.2.3. Usability of authentication

Authentication using graphical or alphanumeric passwords requires the user to remember a unique combination of information, hence weak passcodes are chosen [48,72,76,78]. Consequently, evaluating a proof-of-concept implementation should be feasible and usable in real-world scenarios. Usability and security are tradeoffs [28,50,75,79]. The required security measures should be increased, requiring new safety solutions [37]. Smartphones save a lot of personal data, yet they are risky. The investigations found that PIN locks were inadequate for use, resulting in low dependency (33% of users) [9,53,55,60,74]. Implicit documentation for smartphone authentication creates a unique user profile from their device interactions, enabling continuous, user-transparent authentication. Therefore; the researchers addressed the problem of integrating implicit documentation by establishing their own model, generating a user profile, and providing privacy for data integrity [22,49,64,80,81]. Security is a major research challenge in production. To improve system usability, programmers must maintain a balance between usability and security [23,50,73]. Smartphone security and usability (i.e., trade-off) are mutually exclusive. One-time authentication is vulnerable to theft and loss [28,50,75]. When idleness occurs, it is counterproductive to spontaneous logouts or periodic authentication [46,51,74], Enrollment must be repeated, reducing usability [23, 50,73]. An unobtrusive authentication system may be more usable but has lower security access control. Usability is critical for smartphones because users do not want to interrupt their workflow to verify their identity [23,50,73].

4.2.4. Data collection

Data collection is one of the most difficult challenges that developers face when working with sensor-based authentication. Instead of spending a long time, money, and effort collecting data, a dataset is created as a result of the data collection to produce feather testing and enhancements. Such datasets can aid in the improvement of the quality of a specific authentication technique. Goicoechea-Telleria et al., in 2017, conducted a study in use each material at least 120 times on the smartphone sensor, making a total of 5841 attempts [45]. The devices necessitated collecting and analyzing data from existing smartphones that were not available, adding to the developers' workload [33,44,63]. Acien et al., 2020, raised two issues: the first is that it is necessary to investigate the feasibility of using behavioral biometric, touch dynamics (touch gestures and keystrokes), accelerometer, gyroscope, Wi-Fi, GPS location data collection and app usage on a smartphone (the data can help developers design new smartphone authentication techniques). The second is related to the accuracy of the data during data acquisition, for example, touch gestures patterns [22,31,32,34,43].

4.2.5. Behavioral biometrics

Biometric security technology depends on the input signal quality: if the received signal is weak or distorted noise, identification task becomes more difficult. The main challenge for modern biometric algorithms to create is to overcome these difficult conditions and to extract the maximum amount of reliable evidence to pinpoint accuracy to make personal status and identity recognition possible. Moreover, human gait is different from other human biometric such as fingerprint or voice, because its properties over time can change significantly [38,40,42,49, 54]. In addition to the person with complicated malicious intentions can easily capture a normal movement compared with a fingerprint or even a password [15,40,41,51,67]. The challenges surrounding authentication are interconnected with the field of behavioral biometrics due to several factors. In the first place, an individual with nefarious intentions can effortlessly record a typical movement in contrast to a fingerprint or even a password [14,46]. Moreover, the process of authentication also encompasses natural movements, such as using the device while walking, positioning it close to the user's ear, and carrying the device [71]. Furthermore, light sensors are utilized to safeguard against 2D virtual camera and media attacks, ensuring swift authentication without any detrimental impact [68].

4.2.6. Simulation scenarios

A simulation scenario is related to data collection in that developers propose a scenario for data collection. This scenario includes the number of users as well as the steps involved in carrying out the experiment. To validate the newly developed approach, various conditions and scenarios are designed and proposed by research. On a random basis, the researchers propose the number of participants, data collection scenarios, and testing environments [20,33,35,56,82]. The 3D touchscreen sensor is only available in iPhones devices but not in Android devices. Unfortunately, utilizing the pattern lock in android devices only makes it challenging to apply it using the 3D touchscreen sensor of the iPhone device. Therefore, the aim was to build a new technique by simulate 3D touchscreen sensor and apply it in android. The simulation process made a new sensor in android without any cost to embedded h/w. The developer provided the similar environment of iPhone devices then applied it in android devices [40,83,84].

4.2.7. Sensors and authentication methods

In order to replicate or simulate authentication techniques, specific sensor characteristics are required. Understanding new sensor-based authentication techniques requires a thorough understanding of sensor behavior, specification, output data, and visible action. So, if a researcher wants to investigate hand waving as a biometric, they must first investigate the hand waving's individuality. To provide this motion, he must first identify the motion sensor [23,24,26,35]. Ashraf proposed, in 2018, that user movements deform the original magnetic field [4, 85-87]. The sensor must also be low-cost, easy to deploy, and energy-efficient. Researchers in behavioral biometrics tried to test the authentication technique's accuracy, effectiveness, and user differences [45,46,61,88]. Authentication with PINs and passwords is time consuming and unfriendly to users [9,18,28].

4.3. Recommendations

Several recommendations propose in order to alleviate the challenges that developers, users, and researchers have in avoiding illegal usage of smartphones. Recommendation categories for smartphone authentication of sensor-based, see the Fig. 9 above.

4.3.1. Users

Many smartphone users who have extremely sensitive data require extensive guidance and recommendations to follow safe procedures in their daily use. When using cell phones, users should exercise caution [53,56]. The position of a smartphone user may be determined using the smartphone's sensors, and his/her activity data can be collected [21]. More secure techniques are available than the traditional username password and similar methods; consequently, users must utilize more advanced authentication approaches [11,38]. Usability is one of the reasons why users do not utilize advanced authentication techniques. Acien and Fortin proposed a simple system based on an accessory that users carry in public every day; the touch gesture or fingerprint gesture and controlling the mobile phone, making the recognition process more accessible and seamless [34,43].

4.3.2. Developers/providers

Developers and security providers serve an important in developing new authentication techniques. The developers' investigations yielded many research recommendations. One of the sensor-based authentication approaches is behavioral authentication using gestures. Due to the imposter's replication challenges, this authentication approach offers a wide range of applications without requiring developers to provide extra hardware support [22]. The data obtained from these sensors can identify smartphone users by evaluating the user's interaction with the device [67]. Smartphone sensors are ideal for providing implicit and explicit authentication mechanisms, which should coexist to ensure device security [22,36,49,89]. This type of biometric approach can provide authentication in the background service. However, developers should be mindful that not every feature acquired as expected [65]. Orientation sensors can provide many features (e.g., 56–304 unique features obtained from the orientation sensors alone in specific experiments), making this technique viable [67,74]. Multiple features of the user's activity and the mobile device's reaction may be included in user behavior models; the verification method should also be established [17, 31,60,65]. The issue is now how the system know which classifier to employ. Determining the user's behavior requires context-awareness, which requires further study. A longitudinal real-life gait-based dataset should be collected to assess unique recognition model ability in non-lab environments [67], in which gait models are immediately stored in the device and function well independent of location [53]. The explicit authentication should offer a backup authentication strategy if the authentication fails [27,65]. Background service authentication is needed to ensure the user's identities [76]. Smartphone sensors can use to track a user's location and gather data on their activities [21]. However, attackers may be able to monitor the smartphone if they have unrestricted access to the sensors [50].

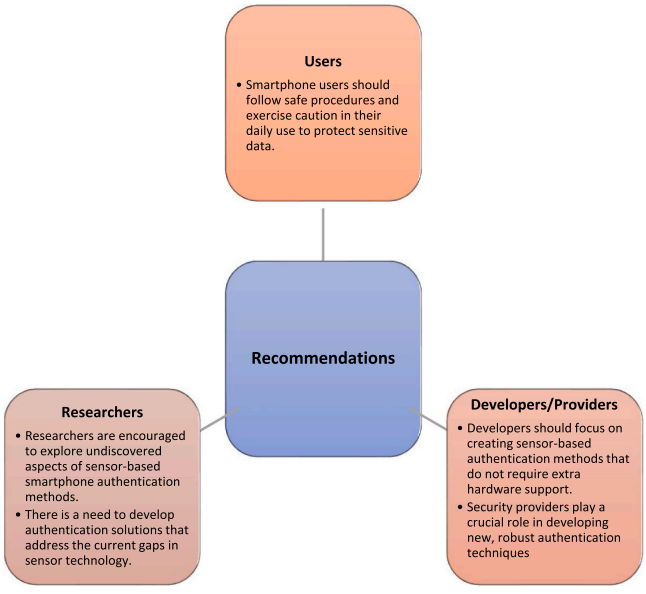

Fig. ↱9. Shows a Summary of Recommendations.

4.3.3. Researchers

The analyzed articles suggested five main research directions. For the first issue, the new authentication method should be focus upon how to determine the nature of the activity the user is undertaking through devising context-awareness [67]. Al-Obaidi et al. focus upon collect longitudinal real-life gait data to assess recognition ability outside of the lab [38,67]. The recommendation for "feature selection" came in the second direction. Biometric combination and feature selection were the most difficult challenges [13,57,74,76]. As privacy expectations rise, Anusas-Amornkul [62] recommended feature selection, which features dimensions should be decreased to provide equal or better performance to improve smartphone usability. The outcome can be improved if the developers or researchers use advanced gait segmentation techniques and extract additional characteristics to enhance the proposed multimodal biometric system [24]. The third approach included creating datasets effective that researchers could use to evaluate new techniques instead of gathering data for each experiment. For example, creating a dataset with actual injection assaults might assist research on injection management [46,89]. The experiment's environment was the fourth feature study direction. The new authentication methods work well in a controlled setting [4,40]. However, changing the phone's location or other environmental constraints would impact the uncontrolled environment [4,40]. For environmental veracity, the researchers recommend collecting trials over several sessions [31]. Finally, while evaluating scalability, one of the intriguing issues was how long users would need to train their devices and how smartphone real-time categorization would respond to increasing numbers of users [35].

5. Conclusion

In conclusion, the area of sensors-based smartphones authentication has been getting a huge intention by researchers and developers. With the widespread usage of smartphones, users not just using their smartphone for calls and messaging only, but they are using it for a variety of purposes such as banking transactions, e-mailing, chatting, online shopping, video conferencing, health monitoring, and many more. Biometric based authentication solutions are promising techniques to replace traditional authentication mechanisms. However, this area is still suffering from different challenges and issues as discussed above.

Most of the challenges are related to data accessibility, usability of authentication, data security, data collection, behavioral biometric, simulation scenarios, and authentication methods. The proposed recommended solutions may overcome the current challenges and issues in the area of sensors-based smartphone authentication. These proposed solutions may participate in reducing the gaps mentioned above to advance the biometric solutions.

Declaration of Competing Interest

The authors declare no conflict of interest.

References

[1] M.L. Shuwandy, B.B. Zaidan, A.A. Zaidan, Novel authentication of blowing voiceless password for android smartphones using a microphone sensor, Multimed. Tools Appl. 81 (30) (2022) 44207–44243.

[2] S. Gupta, A. Buriro, B. Crispo, Demystifying authentication concepts in smartphones: ways and types to secure access (vol), Mob. Inf. Syst. 2018 (2018), https://doi.org/10.1155/2018/2649598.

[3] M.L. Shuwandy, "Smile Mask to Capsulation MOLAZ Method," IJCSNS Int. J. Comput. Sci. Netw. Secur., no. July, 2013, [Online]. Available: http://paper.ijcsns.org/07_book/201312/20131210.pdf.

[4] M.L. Shuwandy, B.B. Zaidan, A.A. Zaidan, A.S. Albahri, Sensor-based mhealth authentication for real-time remote healthcare monitoring system: a multilayer systematic review, J. Med. Syst. vol. 43 (2) (2019), https://doi.org/10.1007/s10916-018-1149-5.

[5] M.S. Obaidat, I. Traore, and I. Woungang, Biometric- Based Physical and Cybersecurity Systems.

[6] L. Hernández-álvarez, J.M. de Fuentes, L. González-Manzano, L.H. Encinas, Privacy-preserving sensor-based continuous authentication and user profiling: a review, Sens. (Switz.) vol. 21 (1) (2021) 1–23, https://doi.org/10.3390/s21010092.

[7] Shuwandy, Moceheb Lazam, H. A. Aljubory, N. M. Hammash, M. M. Salih, M. A. Altaha, and Z. T. Alqaisy. "BAWS3TS: Browsing Authentication Web-Based Smartphone Using 3D Touchscreen Sensor." In 2022 IEEE 18th International Colloquium on Signal Processing & Applications (CSPA), pp. 425-430. IEEE, 2022.

[8] T. Osman, M. Mannan, U. Hengartner, A. Youssef, Appveto: mobile application self-defense through resource access veto, ACM Int. Conf. Proceeding Ser, 2019, pp. 366–377, https://doi.org/10.1145/3359789.3359839.

[9] D.M. Shila and E. Eyisi, "Adversarial Gait Detection on Mobile Devices Using Recurrent Neural Networks," *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 316–321, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00055.

[10] J. Zhang, A.R. Beresford, and I. Sheret, "SensorID: Sensor calibration fingerprinting for smartphones," in *Proceedings - IEEE Symposium on Security and Privacy*, 2019, vol. 2019-May, pp. 638–655, doi: 10.1109/SP.2019.00072.

[11] J.M. de Fuentes, L. Gonzalez-Manzano, A. Ribagorda, Secure and usable user-in-a-context continuous authentication in smartphones leveraging non-assisted sensors, Sens. (Switz.) vol. 18 (4) (2018), https://doi.org/10.3390/s18041219.

[12] M.L. Shuwandy, A.K. Salih, F.L.K. Alameen, A.M.M. Habbal, Switching between the AES-128 and AES-256 using Ks * & two keys, IJCSNS Int. J. Comput. Sci. Netw. Secur. vol. 10 (8) (2010) 136–139 ([Online]. Available), http://paper.ijcsns.org/07_book/201008/20100821.pdf.

[13] R. Wang and D. Tao, "DTW-KNN Implementation for Touch-based Authentication System," *Proc. - 5th Int. Conf. Big Data Comput. Commun. BIGCOM 2019*, pp. 318–322, 2019, doi: 10.1109/BIGCOM.2019.00055.

[14] D. Shukla, G. Wei, D. Xue, Z. Jin, V.V. Phoha, Bodytaps: authenticating your device through few simple taps, 2018 IEEE 9th Int. Conf. Biom. Theory, Appl. Syst. BTAS 2018 (2018) 1–8, https://doi.org/10.1109/BTAS.2018.8698602.

[15] R.Blanco Gonzalo *et al.*, "Attacking a Smartphone Biometric Fingerprint System: A Novice's Approach," Proc. - *Int. Carnahan Conf. Secur. Technol.* , vol. 2018-Octob, no. 675087, pp. 1–5, 2018, doi: 10.1109/CCST.2018.8585726.

[16] C. Lunerti, R. Guest, J. Baker, P. Fernandez-Lopez, and R. Sanchez-Reillo, "Sensing Movement on Smartphone Devices to Assess User Interaction for Face Verification," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2018-Octob, pp. 1–5, 2018, doi: 10.1109/CCST.2018.8585547.

[17] K. Yoneda, G.M. Weiss, Mobile sensor-based biometrics using common daily activities (Janua), 2017 IEEE 8th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2017 vol. 2018 (2017) 584–590, https://doi.org/10.1109/UEMCON.2017.8249001.

[18] Z. Akhtar, A. Buriro, B. Crispo, and T.H. Falk, "Multimodal smartphone user authentication using touchstroke, phone-movement and face patterns," *2017 IEEE Glob. Conf. Signal Inf. Process. Glob. 2017 - Proc.*, vol. 2018-Janua, pp. 1368–1372, 2018, doi: 10.1109/GlobalSIP.2017.8309185.

[19] H. Ketabdar, P. Moghadam, B. Naderi, M. Roshandel, Magnetic signatures in air for mobile devices, MobileHCI'12 - Companion Proc. 14th Int. Conf. Hum. Comput. Interact. Mob. Devices Serv. (2012) 185–188, https://doi.org/10.1145/2371664.2371705.

[20] N. Kala, T. Bhatia, and N. Aggarwal, "Person Identification and Characterization from Gait Using Smartphone," *2019 11th Int. Conf. Commun. Syst. Networks, COMSNETS 2019*, vol. 2061, pp. 492–495, 2019, doi: 10.1109/COMSNETS.2019.8711131.

[21] M. Ehatisham-ul-Haq, et al., Authentication of smartphone users based on activity recognition and mobile sensing, Sens. (Switz.) vol. 17 (9) (2017), https://doi.org/10.3390/s17092043.

[22] Y. Zhang, M. Yang, Z. Ling, Y. Liu, W. Wu, FingerAuth: 3D magnetic finger motion pattern based implicit authentication for mobile devices, Futur. Gener. Comput. Syst. vol. 108 (2020) 1324–1337, https://doi.org/10.1016/j.future.2018.02.006.

[23] C. Shen, Y. Chen, X. Guan, Performance evaluation of implicit smartphones authentication via sensor-behavior analysis, 430–431, Inf. Sci. (Ny.). vol (2018) 538–553, https://doi.org/10.1016/j.ins.2017.11.058.

[24] I. Lamiche, G. Bin, Y. Jing, Z. Yu, A. Hadid, A continuous smartphone authentication method based on gait patterns and keystroke dynamics, J. Ambient Intell. Humaniz. Comput. vol. 10 (11) (2019) 4417–4430, https://doi.org/10.1007/s12652-018-1123-6.

[25] S. Guo, G. Niu, Z. Wang, and M.O. Pun, "Magnetic Field Strength Sequence-based Indoor Localization Using Multi-level Link-node Models," *IEEE Int. Conf. Commun.*, vol. 2020-June, no. 61731018, 2020, doi: 10.1109/ICC40277.2020.9148721.

[26] Q. Zou, Y. Wang, Q. Wang, Y. Zhao, Q. Li, Deep Learning-Based Gait Recognition Using Smartphones in the Wild, IEEE Trans. Inf. Forensics Secur. vol. 15 (2020) 3197–3212, https://doi.org/10.1109/TIFS.2020.2985628.

[27] J. Varga, D. Švanda, M. Varchola, P. Zajac, Authentication based on gestures with smartphone in hand, J. Electr. Eng. vol. 68 (4) (2017) 256–266, https://doi.org/10.1515/jee-2017-0037.

[28] G. Li, P. Bours, Studying WiFi and accelerometer data based authentication method on mobile phones, ACM Int. Conf. Proceeding Ser, 2018, pp. 43–49, https://doi.org/10.1145/3230820.3230824.

[29] S. Garfan, et al., Telehealth utilization during the Covid-19 pandemic: a systematic review (April, p), Comput. Biol. Med. vol. 138 (no) (2021) 104878, https://doi.org/10.1016/j.compbiomed.2021.104878.

[30] A.H. Alamoodi, et al., Multi-perspectives systematic review on the applications of sentiment analysis for vaccine hesitancy (no. October, p), Comput. Biol. Med. vol. 139 (2021) 104957, https://doi.org/10.1016/j.compbiomed.2021.104957.

[31] M.M. Al-Jarrah, S.S. Al-Khafaji, S. Amin, and X. Feng, "Finger-drawn signature verification on touch devices using statistical anomaly detectors," Proc. - *2019 IEEE SmartWorld, Ubiquitous Intell. Comput. Adv. Trust. Comput. Scalable Comput. Commun. Internet People Smart City Innov. SmartWorld/UIC/ATC/SCALCOM/IOP/SCI 2019*, no. May, pp. 1700–1705, 2019, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00303.

[32] Y. Barlas, O.E. Basar, Y. Akan, M. Isbilen, G.I. Alptekin, O.D. Incel, DAKOTA: continuous authentication with behavioral biometrics in a mobile banking application, 5th Int. Conf. Comput. Sci. Eng. UBMK 2020 (2020) 298–303, https://doi.org/10.1109/UBMK50275.2020.9219365.

[33] Y. Li, H. Hu, G. Zhou, Using data augmentation in continuous authentication on smartphones, IEEE Internet Things J. vol. 6 (1) (2019) 628–640, https://doi.org/10.1109/JIOT.2018.2851185.

[34] A. Acien, A. Morales, R. Vera-Rodriguez, J. Fierrez, MultiLock: mobile active authentication based on multiple biometric and behavioral patterns, Adv. Sci. Technol. Secur. Appl. (2020) 161–177, https://doi.org/10.1007/978-3-030-39489-9_9.

[35] C. Shen, Y. Li, Y. Chen, X. Guan, R.A. Maxion, Performance analysis of multi-motion sensor behavior for active smartphone authentication, IEEE Trans. Inf. Forensics Secur. vol. 13 (1) (2018) 48–62, https://doi.org/10.1109/TIFS.2017.2737969.

[36] M. Abuhamad, T. Abuhmed, D. Mohaisen, D. Nyang, AUToSen: deep-learning-based implicit continuous authentication using smartphone sensors, IEEE Internet Things J. vol. 7 (6) (2020) 5008–5020, https://doi.org/10.1109/JIOT.2020.2975779.

[37] H. Kalita, E. Maiorana, P. Campisi, Keystroke dynamics for biometric recognition in handheld devices, 2020 43rd Int. Conf. Telecommun. Signal Process. TSP 2020 (2020) 410–416, https://doi.org/10.1109/TSP49548.2020.9163524.

[38] K. Kašys, A. Dundulis, M. Vasiljevas, R. Maskeliūnas, R. Damaševičius, BodyLock: human identity recogniser app from walking activity data (LNCS), Lect. Notes Comput. Sci. (Incl. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinforma. vol. 12250 (2020) 307–319, https://doi.org/10.1007/978-3-030-58802-1_23.

[39] P.K. Rayani, S. Changder, Continuous Gait Authentication Against Unauthorized Smartphone Access Through Naïve Bayes Classifier, vol. 1034, Springer, Singapore, 2020.

[40] M.L. Shuwandy, et al., mHealth authentication approach based 3D touchscreen and microphone sensors for real-time remote healthcare monitoring system: comprehensive review, open issues and methodological aspects, Comput. Sci. Rev. vol. 38 (2020) 100300, https://doi.org/10.1016/j.cosrev.2020.100300.

[41] P. Bours and T. Denzer, "Cross-pocket gait recognition," Proc. - *2018 Int. Conf. Cyberworlds,* CW 2018, pp. 331–338, 2018, doi: 10.1109/CW.2018.00067.

[42] E. Rahmawati *et al.*, "Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone," Proc. IES-ETA *2017* - Int. Electron. Symp. Eng. Technol. Appl., vol. 2017-Decem, pp. 234–238, 2017, doi: 10.1109/ELECSYM.2017.8240409.

[43] P.E. Fortin, Y. Huang, and J.R. Cooperstock, "Exploring the use of fingerprint sensor gestures for unlock journaling: A comparison with slide-to-X," *Proc. 21st Int. Conf. Human-Computer Interact. with Mob. Devices Serv. MobileHCI 2019*, 2019, doi: 10.1145/3338286.3340135.

[44] C. Gehrmann, M. Rodan, N. Jönsson, Metadata filtering for user-friendly centralized biometric authentication (vol), Eurasip J. Inf. Secur 2019 (1) (2019), https://doi.org/10.1186/s13635-019-0093-3.

[45] I. Goicoechea-Telleria, J. Liu-Jimenez, H. Quiros-Sandoval, and R. Sanchez-Reillo, "Analysis of the attack potential in low cost spoofing of fingerprints," Proc. - *Int. Carnahan Conf. Secur. Technol.* , vol. 2017-Octob, pp. 1–6, 2017, doi: 10.1109/CCST.2017.8167798.

[46] B. Chakraborty, K. Nakano, Y. Tokoi, and T. Hashimoto, "An Approach for Designing Low Cost Deep Neural Network based Biometric Authentication Model for Smartphone User," *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, vol. 2019-Octob, pp. 772–777, 2019, doi: 10.1109/TENCON.2019.8929241.

[47] K.A. Rahman, D.J. Tubbs, and M.S. Hossain, "Movement Pattern Based Authentication for Smart Mobile Devices," *Proc. - 17th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2018*, pp. 1054–1058, 2019, doi: 10.1109/ICMLA.2018.00172.

[48] G. Li, P. Bours, A novel mobilephone application authentication approach based on accelerometer and gyroscope data, 2018 Int. Conf. Biom. Spec. Interes. Group, BIOSIG 2018 (2018) 1–4, https://doi.org/10.23919/BIOSIG.2018.8553503.

[49] Y. Liu, M. Yang, Z. Ling, and J. Luo, "Implicit authentication for mobile device based on 3D magnetic finger motion pattern," Proc. *2017 IEEE 21st Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2017*, pp. 325–330, 2017, doi: 10.1109/CSCWD.2017.8066715.

[50] S. Kulshreshtha and A.S. Arif, "Woodpecker: Secret BackofDevice Tap Rhythms to Authenticate Mobile Users," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 2020-Octob, pp. 2727–2733, 2020, doi: 10.1109/SMC42975.2020.9283239.

[51] Y. Li, B. Zou, S. Deng, G. Zhou, Using feature fusion strategies in continuous authentication on smartphones, IEEE Internet Comput. vol. 24 (2) (2020) 49–56, https://doi.org/10.1109/MIC.2020.2971447.

[52] O.E. Basar, G. Alptekin, H.C. Volaka, M. Isbilen, O.D. Incel, Resource usage analysis of a mobile banking application using sensor-and-touchscreen-based continuous authentication, Procedia Comput. Sci. vol. 155 (2019) 185–192, https://doi.org/10.1016/j.procs.2019.08.028.

[53] M. Ehatisham-ul-Haq, M. Awais Azam, U. Naeem, Y. Amin, J. Loo, Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing, J. Netw. Comput. Appl. vol. 109 (2018) 24–35, https://doi.org/10.1016/j.jnca.2018.02.020.

[54] Y. Abdrabou, O. Sherif, R.M. Eisa, and A. Elmougy, "Human-Based Fraudulent Attempts on Gait Based Profiles," *ACM Int. Conf. Proceeding Ser.*, pp. 206–209, 2018, doi: 10.1145/3283458.3283488.

[55] A. Bhattarai, A. Siraj, Increasing accuracy of handmotion based continuous authentication systems, 2018 9th IEEE Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2018 (2018) 70–76, https://doi.org/10.1109/UEMCON.2018.8796725.

[56] F. Karegar, J.S. Pettersson, and S. Fischer-Hübner, "Fingerprint recognition on mobile devices: Widely deployed, rarely understood," *ACM Int. Conf. Proceeding Ser.*, 2018, doi: 10.1145/3230833.3234514.

[57] B.S. Saini, et al., A three-step authentication model for mobile phone user using keystroke dynamics, IEEE Access vol. 8 (2020) 125909–125922, https://doi.org/10.1109/ACCESS.2020.3008019.

[58] S. Kuk, J. Kim, Y. Park, H. Kim, Empirical determination of efficient sensing frequencies for magnetometer-based continuous human contact monitoring, Sens. (Switz.) vol. 18 (5) (2018) 1–22, https://doi.org/10.3390/s18051358.

[59] M. Gadaleta, M. Rossi, IDNet: Smartphone-based gait recognition with convolutional neural networks, Pattern Recognit. vol. 74 (2018) 25–37, https://doi.org/10.1016/j.patcog.2017.09.005.

[60] L. Gonzalez-Manzano, U. Mahbub, J.M. de Fuentes, R. Chellappa, Impact of injection attacks on sensor-based continuous authentication for smartphones (March), Comput. Commun. vol. 163 (no) (2020) 150–161, https://doi.org/10.1016/j.comcom.2020.08.022.

[61] S.C. Yeh, W.H. Hsu, W.Y. Lin, Y.F. Wu, Study on an indoor positioning system using earth's magnetic field, IEEE Trans. Instrum. Meas. vol. 69 (3) (2020) 865–872, https://doi.org/10.1109/TIM.2019.2905750.

[62] T. Anusas-Amornkul, "Strengthening password authentication using keystroke dynamics and smartphone sensors," *ACM Int. Conf. Proceeding Ser.*, pp. 70–74, 2019, doi: 10.1145/3357419.3357425.

[63] Y. Li, H. Hu, G. Zhou, S. Deng, Sensor-based continuous authentication using cost-effective kernel ridge regression, IEEE Access vol. 6 (c) (2018) 32554–32565, https://doi.org/10.1109/ACCESS.2018.2841347.

[64] Y. Chen, M. Zhou, Z. Zheng, Learning sequence-based fingerprint for magnetic indoor positioning system, IEEE Access vol. 7 (2019) 163231–163244, https://doi.org/10.1109/ACCESS.2019.2952564.

[65] H. Lee, J.Y. Hwang, D.I. Kim, S. Lee, S.H. Lee, J.S. Shin, Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors (vol), Secur. Commun. Netw. 2018 (2018), https://doi.org/10.1155/2018/2567463.

[66] S. Gu, R. Yao, L. Lan, C. Guo, F. Gao, and C. Xu, "The Improvement of Traditional Indoor Localization Model Using Magnetic Field Based on Smartphone," *Proc. IEEE 14th Int. Conf. Intell. Syst. Knowl. Eng. ISKE 2019*, pp. 694–700, 2019, doi: 10.1109/ISKE47853.2019.9170444.

[67] H. Al-Obaidi, F. Li, N. Clarke, B. Ghita, and S. Ketab, "A multi-algorithmic approach for gait recognition," *Eur. Conf. Inf. Warf. Secur. ECCWS*, vol. 2018-June, no. Muaaz, pp. 20–28, 2018.

[68] G. Berkovich, D. Churikov, J. Georgy, C. Goodall, Coursa venue: indoor navigation platform using fusion of inertial sensors with magnetic and radio fingerprinting, Fusion 2019 - 22nd Int. Conf. Inf. Fusion (2019) 1–3.

[69] Y. Javed and M. Shehab, "Towards Improving Comprehension of Touch ID Authentication with Smartphone Applications," *Proc. - 2017 IEEE Symp. Privacy-Aware Comput. PAC 2017*, vol. 2017-Janua, no. October 2019, pp. 206–207, 2017, doi: 10.1109/PAC.2017.27.

[70] M. Roshandel, A. Haji-Abolhassani, H. Ketabdar, MagiThings: gestural interaction with mobile devices based on using embedded compass (magnetic field) sensor,", Emerg. Perspect. Des. Use, Eval. Mob. Handheld Devices (2015) 49–74, https://doi.org/10.4018/978-1-4666-8583-3.ch003.

[71] H. Shin, G. Lee, and D. Han, "Subway stop/departure detection using a magnetic sensor of the smartphone," *ACM Int. Conf. Proceeding Ser.*, pp. 1–5, 2018, doi: 10.1145/3271553.3271614.

[72] S. Ayeswarya and J. Norman, "Seamless Personal Authentication using Biometrics," 2019 Innov. Power Adv. Comput. Technol. i-PACT 2019, pp. 1–5, 2019, doi: 10.1109/i-PACT44901.2019.8960070.

[73] M. Muaaz, R. Mayrhofer, Smartphone-based gait recognition: from authentication to imitation, IEEE Trans. Mob. Comput. vol. 16 (11) (2017) 3209–3221, https://doi.org/10.1109/TMC.2017.2686855.

[74] H. Mostafa, A.M. Elkorany, M. El-Ramly, and H. Shaban, "Behavio2Auth: Sensorbased behavior biometric authentication for smartphones," *ACM Int. Conf. Proceeding Ser.*, 2019, doi: 10.1145/3333165.3333176.

[75] A. Buriro, B. Crispo, M. Conti, ANSWERAUTH: a bimodal behavioral biometric-based user authentication scheme for smartphones, J. Inf. Secur. Appl. vol. 44 (2019) 89–103, https://doi.org/10.1016/j.jisa.2018.11.008.

[76] R. Kumar, P.P. Kundu, D. Shukla, and V.V. Phoha, "Continuous user authentication via unlabeled phone movement patterns," *IEEE Int. Jt. Conf. Biometrics, IJCB 2017*, vol. 2018-Janua, pp. 177–184, 2018, doi: 10.1109/BTAS.2017.8272696.

[77] A.H. Alamoodi, et al., A systematic review into the assessment of medical apps: motivations, challenges, recommendations and methodological aspect, Health Technol. (Berl.). vol. 10 (5) (2020) 1045–1061, https://doi.org/10.1007/s12553-020-00451-4.

[78] H. Jiang, H. Cao, D. Liu, J. Xiong, Z. Cao, SmileAuth: using dental edge biometrics for user authentication on smartphone, Proc. ACM Interact., Mob., Wearable Ubiquitous Technol. vol. 4 (3) (2020), https://doi.org/10.1145/3411806.

[79] F. Zhang, S. Xin, J. Feng, Deep dense multi-level feature for partial high-resolution fingerprint matching, vol. 2018-Janua, IEEE Int. Jt. Conf. Biom., IJCB 2017 (2018) 397–405, https://doi.org/10.1109/BTAS.2017.8272723.

[80] X. Fan, J. Wu, C. Long, and Y. Zhu, "Accurate and Low-cost Mobile Indoor Localization with 2-D Magnetic Fingerprints," *CrowdSenSys 2017 - Proc. 1st ACM Work. Mob. Crowdsensing Syst. Appl. Part SenSys 2017* , pp. 13–18, 2017, doi: 10.1145/3139243.3139244.

[81] G. Baldini, G. Steri, I. Amerini, and R. Caldelli, "The identification of mobile phones through the fingerprints of their built-in magnetometer: An analysis of the portability of the fingerprints," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2017-Octob, pp. 1–6, 2017, doi: 10.1109/CCST.2017.8167855.

[82] P. Fernandez-Lopez, K. Kiyokawa, Y. Wu, and J. Liu-Jimenez, "Influence of Walking Speed and Smartphone Position on Gait Recognition," Proc. - *Int. Carnahan Conf. Secur. Technol.* , vol. 2018-Octob, pp. 1–5, 2018, doi: 10.1109/CCST.2018.8585427.

[83] J. Zhang, A.R. Beresford, and I. Sheret, "SENSOR ID: Sensor Calibration Fingerprinting for Smartphones," 2019.

[84] G. Zheng, W. Yang, M. Johnstone, R. Shankaran, C. Valli, Securing the elderly in cyberspace with fingerprints, INC (2020).

[85] I. Ashraf, S. Hur, Y. Park, mPILOT-magnetic field strength based pedestrian indoor localization, Sens. (Switz.) vol. 18 (7) (2018) 1–22, https://doi.org/10.3390/s18072283.

[86] I. Ashraf, S. Hur, Y. Park, Enhancing performance of magnetic field based indoor localization using magnetic patterns from multiple smartphones, Sens. (Switz.) vol. 20 (9) (2020), https://doi.org/10.3390/s20092704.

[87] A.S. Jouda, A.M. Sagheer, M.L. Shuwandy. MagRing-SASB: Static Authentication of Magnetism Sensor Using Semi-Biometric Interaction Magnetic Ring, IEEE, 2021, pp. 183–188.

[88] M.R. Dey, S. Sengupta, B.K. Mohanta, D. Jena, S. Chakraborty, Poster - Magneto: leveraging magnetic field changes for inferring smartphone app usage, Proc. Annu. Int. Conf. Mob. Comput. Netw., MOBICOM (2018) 777–779, https://doi.org/10.1145/3241539.3267772.

[89] S. Mohammadi, A. Bhattacharjee, S. Marcel, Domain adaptation for generalization of face presentation attack detection in mobile settengs with minimal information, ICASSP 2020 - 2020 IEEE Int. Conf. Acoust. Speech Signal Process. (2020) 1001–1005, https://doi.org/10.1109/ICASSP40776.2020.9053685.