Fast Review of Sensor-based Smartphone Authentication: Challenges and Motivations at last three years.

Omar Ahmed Shareef

Computer Sciences Department, College of Computer and Mathematical Sciences, Tikrit University Tikrit, Iraq

omar93ahmd@gmail.com

Abstract:

Nowadays, the usage of smartphones has expanded beyond simple phone calls and text messages, with people using them for online banking, shopping, video chats, and tracking their health. This necessitates the storage of private information on the device, and unauthorized access to this data can have catastrophic consequences. Therefore, safeguarding smartphones from falling into the wrong hands is of utmost importance. Researchers have developed various approaches to make sensor-based smartphone authentication simple for users by establishing clear requirements. However, many aspects of sensor-based smartphone authentication solutions still remain unexplored.

In this context, the authors seek to investigate the current issues and concerns in the field of sensor-based smartphone authentication through a comprehensive literature review. To achieve this, they utilized three digital scientific databases, namely ScienceDirect, IEEE Xplore, and Scopus. Potential studies were identified, and from a total of 450 papers, only 62 met the inclusion criteria. To help researchers understand the included research, a taxonomy was developed.

In conclusion, this literature review provides a comprehensive overview of sensor-based smartphone authentication, highlighting its importance and potential to enhance smartphone security. The study identifies the current challenges and limitations in this field and suggests future directions for research. By addressing these issues, researchers can develop more effective sensor-based authentication solutions that are user-friendly, secure, and privacy-preserving.

Keywords: (quick review, smartphone, challenges and motivations)

Introduction

In recent years, there has been a significant amount of interest from researchers and developers in sensor-based smartphone authentication. Smartphones have become ubiquitous, and as a result, people are increasingly using them for a variety of purposes such as online banking, shopping, and video conferencing. These tasks require the user to store their private information on their device, and if an outsider were to gain access to this information, it could have catastrophic consequences [1].

Therefore, protecting the smartphone from unauthorized access has become a top priority [2]. Cyberattacks are a significant threat, and the possibility of data exposure is a serious concern. As a result, regulations for using smartphones need to be strengthened. The traditional method of protecting smartphones has been through the use of a PIN, password, or pattern [3, 4]. However, the proliferation of various smartphone sensors has led researchers to develop novel authentication mechanisms that utilize these sensors to enhance convenience and safety. These sensors include orientation sensors, camera sensors, finger sensors, microphone sensors, touchscreen sensors, Magnetic sensors, and 3D touchscreen sensors [1, 5–8]. Biometric-based authentication solutions are now being considered as potential replacements for traditional authentication mechanisms. Biometric techniques are viewed as being more secure and capable of distinguishing between a legitimate user and an impostor [9–

12].

Biometric measures are becoming more popular as a means of combating identity theft and the misuse of a smartphone's internal resources [13]-[16]. Furthermore, the proliferation of sensors in smartphones has necessitated the development of more sophisticated methods for securing them.

The development of these novel authentication mechanisms has been driven by the difficulty of personal identity password-based authentication mechanisms. Biometric-based authentication solutions are viewed as being more secure and capable of distinguishing between a legitimate user and an impostor. Biometric measures are becoming more popular as a means of combating identity theft and the misuse of a smartphone's internal resources. They are also seen as being more convenient for users since they do not require the user to remember a password.

One of the challenges faced by researchers in this field is developing authentication mechanisms that are both convenient and secure. Methods that are too cumbersome may deter users from using them, while methods that are too simple may be easily compromised. As a result, researchers are continually exploring new ways to enhance the security of smartphone authentication mechanisms while also ensuring that they are easy to use.

Furthermore, the use of biometric authentication mechanisms raises concerns about privacy and security. For instance, if the biometric data is stored on the device, then there is a risk that it could be stolen by a cybercriminal. Similarly, if the biometric data is stored on a central server, then there is a risk that it could be compromised in a data breach. Therefore, it is essential to ensure that biometric authentication mechanisms are designed with privacy and security in mind.

In addition to biometric authentication mechanisms, researchers are also exploring other methods of securing smartphones. For example, some researchers have developed mechanisms that rely on the user's facial recognition or voice recognition. Others have explored the use of sensors such as the accelerometer or gyroscope to detect whether the smartphone is being used by the legitimate user.

Overall, the development of novel authentication mechanisms for smartphones is an area of active research. As smartphones become increasingly ubiquitous and people rely on them for more sensitive tasks, the need for secure and convenient authentication mechanisms will only continue to grow. Therefore, it is crucial that researchers continue to explore new ways to enhance the security of smartphone authentication mechanisms while also ensuring that they are easy to use and protect user privacy. Authentication can be divided into four subtopics: mechanism authentication [5, 17], implicit authentication [18, 19], continuous authentication [8, 20], and hybrid tracking [21, 22]. Recent advancements in this field have led to the emergence of various user-friendly, sensor-based smartphone authentication techniques [18], [20], [23], [24]. Although these approaches show promise, there is still much to be learned in this area. The purpose of our work is to conduct a thorough evaluation of these techniques so that individuals can gain a comprehensive understanding of this emerging field, including its current problems and concerns. This overview is intended to provide insight that may assist future researchers in filling gaps and discovering viable solutions. Furthermore, the study proposes possible approaches to guide future research towards the most effective direction to address the many gaps in this field of study. In conclusion, we believe that our work will contribute to the advancement of knowledge in the area of sensor-based smartphone authentication techniques and lead to the development of practical solutions that can be applied in real-world scenarios.

Method

Sensor-based authentication in mobile devices is a burgeoning area of research in academia. The term "Smartphone Authentication" is of significant importance to this study since it excludes other devices that do not employ smartphones for authentication purposes. The study aims to identify and present all relevant information pertaining to authentication methods, including password-based systems and various types of sensors. A Systematic Literature Review (SLR) is the methodology employed to gather and analyze copious amounts of data on a particular subject matter. The SLR then utilizes a pre-determined set of methods to draw conclusions on the reliability of the collected data. This approach is indispensable for researchers seeking to comprehensively investigate and evaluate the validity of their findings.

Information sources

In order to conduct a targeted search for articles, we opted to utilize three digital databases: namely IEEE Xplore, ScienceDirect, and Scopus. IEEE Xplore is a reliable and all-encompassing compilation of scholarly articles spanning across numerous disciplines within the realms of engineering and technology. ScienceDirect, on the other hand, is a comprehensive and trustworthy repository that accommodates a vast collection of scholarly articles in science, technology, and medicine. Meanwhile, Scopus serves as an extensive repository of abstracts and citations that envelop various scholarly journals, conference proceedings, and books. These three databases extensively address Sensor-based authentication and its smartphone applications, while simultaneously offering an elaborate survey of existing literature across multiple academic fields. Therefore, by utilizing these three databases, we were able to conduct a thorough and comprehensive exploration that enabled us to gather relevant scholarly articles that are highly valuable in our research study.

Study Selection

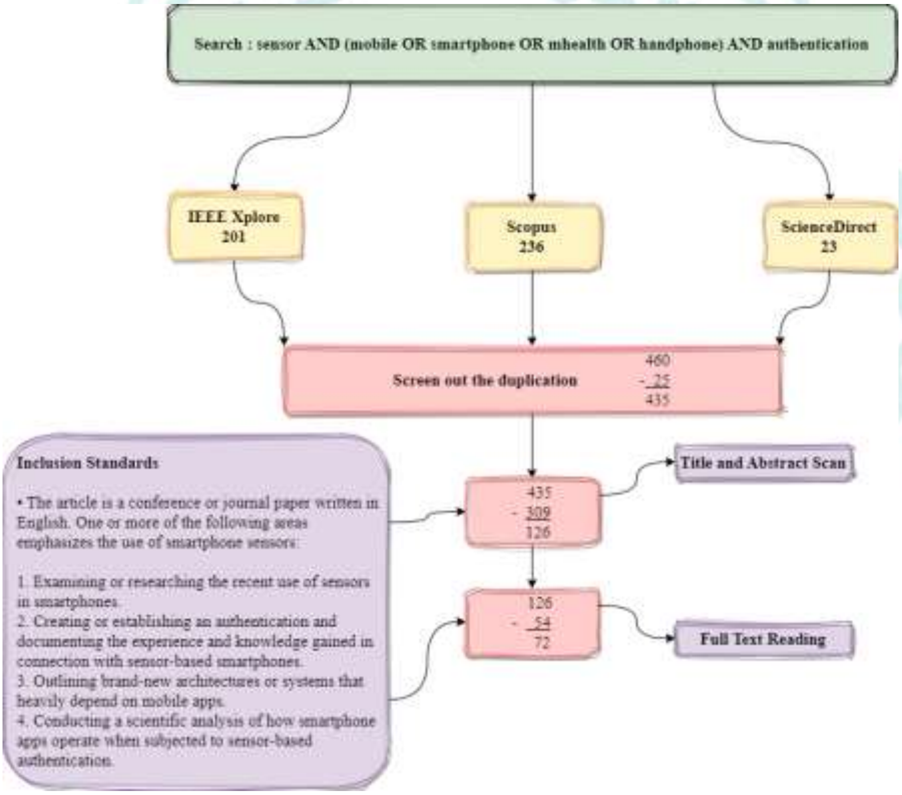
The research was conducted over a period of two years, commencing in 2021 and concluding in 2023. The study began with an all-inclusive search of literature, followed by two phases of screening and filtering. In the first phase, duplicates and articles that were considered irrelevant were removed based on the examination of their titles and abstracts. The second phase involved a comprehensive evaluation of the literature by thoroughly reading the articles that had been filtered during the first phase, as is demonstrated in Figure 1. The research employed a meticulous and rigorous approach to ensure that only the most relevant and high-quality literature was included in the study. Ultimately, the researchers were able to obtain a comprehensive understanding of the topic at hand, due to the exhaustive nature of their literature review.

Research Literature Taxonomy

Over the course of three years, from 2021 to 2023, an extensive research literature taxonomy was conducted in order to identify relevant papers published during this time period. In total, 450 papers were initially found through databases, including IEEE Xplore, Scopus, and ScienceDirect. After removing duplicates, a total of 425 papers remained. Through a meticulous review of titles, abstracts, and complete material, the number of papers was further reduced to 116, and finally, to 62.

These final 62 articles were then categorized into three distinct groups: defense, offense, and others. The "Defense" category included research papers that focused on safeguarding smartphones from potential attackers, while the "Attack" category included research papers that centered on attacking and hacking smartphones. The third category was composed of research papers that aimed to develop an attack or defense strategy through surveys.

Out of the total of 62 articles, it was found that the majority, comprising (n = 54/62) articles, centered around the theme of defense, while only a minimal proportion of (n = 3/62) articles dealt with assault, leaving the remaining (n = 5/62) articles to cover other miscellaneous topics.



• The article is a conference or journal paper written in English. One or more of the following areas emphasizes the use of smartphone sensors:

1. Examining or researching the recent use of sensors in smartphones.
2. Creating or establishing an authentication and documenting the experience and knowledge gained in connection with sensor-based smartphones.
3. Outlining brand-new architectures or systems that heavily depend on mobile apps.
4. Conducting a scientific analysis of how smartphone apps operate when subjected to sensor-based authentication.

Figure 1. SLR Protocol

Articles of Defense

These scholarly articles aim to determine and establish techniques for securing smartphones by utilizing the many sensors that are embedded in these devices. Specifically, these articles have predominantly centered on the orientation sensor, which comprises diverse sensors such as an accelerometer, gyroscope, and magnetometer. Additionally, certain research suggests that the fingerprint could be integrated as part of the phone's security measures. In contrast, other studies have proposed the use of a camera sensor, while some have considered using a touch screen sensor or a microphone sensor.

Out of the total number of articles analyzed, a significant proportion (n = 36/62) were focused on the orientation sensor and its application in gait authentication. In contrast, finger sensors were the subject of only a single article (n = 1/62), while the touch screen sensor had six articles (n = 6/62), the camera sensor had eight articles (n = 8/62), and the microphone sensor had three articles (n = 3/62). These findings indicate a clear preference for the orientation sensor among researchers, with other sensors receiving considerably less attention in the literature. However, further investigation is necessary to determine the efficacy of these various sensors in ensuring the security of smartphones. Additionally, future research could explore the potential benefits of combining multiple sensors to enhance the robustness and reliability of smartphone security measures. Overall, these articles represent a crucial contribution to the field of smartphone security and provide valuable insights into the potential of sensor-based approaches for securing mobile devices.

Articles of Attack

The present articles endeavor to assail smartphones by leveraging the sensors integrated within these devices and capitalizing on the vulnerabilities that exist therein. Specifically, among the attack articles (with a sample size of n = 3/62), one article scrutinizes the authentication mechanism predicated on gait, alongside other methods, and subsequently compromises it. Such exploits pose a significant threat to the security and privacy of smartphone users worldwide, necessitating proactive measures to mitigate the risks associated with sensor-based attacks.

Others Research Related to Sensor

These publications were not included in the study (5/62). This is because they are articles that are not in the field of offense or defense, but rather surveys to determine which sensors are ideal for smartphone defense and which sensors are the most practical and widely used. And it was not related to the aim of the research.

Motivations and Challenges

The objective of this research is to present authentication mechanisms for smartphones that rely on the sensors embedded within these devices. Furthermore, the paper's taxonomy provides valuable insights into the latest scientific literature on the subject matter. There are several other advantages to using literature-based classification. Taxonomy is an effective tool for categorizing and ranking a vast array of papers, and it can be particularly beneficial for novice researchers who are exploring sensor-based smartphone authentication.

In addition, the study proposes a classification system that groups multiple actions and behaviors into a meaningful, coherent, and manageable framework. Taxonomy can also offer scholars fresh perspectives on various issues related to this field. It is a valuable tool for understanding the key concepts and trends in the literature and can aid in the development of new research questions and hypotheses.

Moreover, the taxonomy-based approach can facilitate the identification of research gaps, inconsistencies, and areas that require further exploration. By using this framework, researchers can gain a comprehensive understanding of the current state of the field, potential research directions, and future trends. Ultimately, this research has the potential to contribute to the development of more secure and reliable authentication mechanisms for smartphones that rely on sensor-based technology.

Motivation

In-depth exploration is being conducted by scholars in the field of smartphone authentication by means of sensors installed in these devices. The rationales underpinning the articles can be categorized into three groups: advantages linked to the usability of smartphones, benefits affiliated with the security of smartphones, advantages associated with the ability to utilize biometric authentication in smartphones. It is therefore expected that this research shall furnish crucial insights into the benefits of utilizing sensors for smartphone authentication and would pave the way for further research in this area.

Benefits related to usability of smartphones

Mobile technology has become an integral part of our daily activities, being adopted by all age groups, especially smartphones, which have undergone rapid development and widespread adoption [1]-[3]. Nowadays, it is impossible to conduct business or purchase items online without a mobile phone. Smartphones provide users with numerous benefits, including social networking and online purchasing, but due to their ability to store personal and sensitive information, they have become an attractive target for cybercriminals. Consequently, mobile security has become a pressing concern, and users must remain vigilant and take precautions to safeguard their devices from malicious software, phishing assaults, and unauthorized access.

Manufacturers and software developers are also continuously working to improve the security features of smartphones to protect the privacy of users' sensitive data [4]. Smartphones have become a fundamental instrument for various purposes, including professional tasks, recreational activities, and the facilitation of financial and personal transactions [5].

Mobile devices, such as smartphones and tablets, play significant roles in our everyday existence. The prevalence of mobile devices has resulted in a growing trend of individuals storing more personal and confidential data, including photographs and electronic correspondence, making it vital to mitigate the risks associated with unauthorized access to safeguard private data [6].

Smartphones are increasingly becoming a convenient way to process and exchange sensitive information with online services, and security-sensitive financial transactions are no exception [7]. Mobile phones are revolutionizing the way we do business and commerce, with emerging smartphone commerce apps and services requiring secure access to sensitive and personal data to function properly. However, the availability of this information has led to an increase in cyber-attacks [8]-[10].

Benefits related to security impact on smartphones

The protection of sensitive data on smartphones is crucial, given the wide range of applications available that require high-level security access. Biometric recognition systems are now increasingly necessary to ensure user privacy and prevent unauthorized access [17]. The use of behavior modeling in mobile devices has raised concerns about potential security and privacy issues, but implicit authentication systems are being developed to mitigate these risks [6]. Biometric methods, such as fingerprint scanning, facial verification, and voice recognition, have become popular for their speed and simplicity.

Financial applications on smartphones face a significant security risk from malware that can circumvent current security protocols. Continuous authentication is an important technology that allows for real-time verification of user identity, providing seamless device access for authorized users while preventing unauthorized access attempts. However, the use of complex passwords can be challenging for individuals with limited long-term memory, leading to compromised authentication procedures.

The proliferation of smartphone usage has increased concerns about personal data privacy and security. The storage of confidential information on mobile devices, such as medical records, social security numbers, and bank account numbers, has made users vulnerable to identity theft and financial harm. Traditional authentication mechanisms, such as PINs and passwords, are becoming less prevalent, and novel cybersecurity solutions for smartphones are needed. These solutions should prioritize speed, simplicity, and reliability, as traditional password-based methods are susceptible to replication and deployment.

Article Challenges

Smartphones which depend on sensor authentication have been found to be inadequate in ensuring data security. Through their research, the scholars have identified numerous critical issues regarding the use of sensors, including data accessibility, and the usability of authentication mechanisms. It is imperative that these concerns be addressed in order to improve the overall security of sensor-based authentication systems.

Concern on Data Access

Data access poses a significant challenge to authentication, and the provision of access to only authorized individuals is of utmost importance [16]. For new smartphone trading applications and services to function properly, they must have secure access to sensitive and personal information [4], [8]. It is crucial that the authentication system remains constantly vigilant against potential intruders after the first login, as unauthorized users may gain access to the equipment in violation of the law [6].

Many individuals store confidential data on their mobile devices, including financial information, medical records, and personal identification documents, which exposes them to the risk of identity theft. Consequently, the process of user authentication is essential in verifying individuals' identities and mitigating the risk of impersonation. Maintaining the confidentiality of passwords is imperative for the effectiveness of authentication systems reliant on password-based mechanisms [12].

Concern on Usability of Authentication

With the increasing use of mobile devices, security concerns have become a major issue for individuals using smartphones. Despite the widespread use of text passwords (such as passcodes) for authentication, such methods have been observed to have a number of well-known problems. One of the main issues is that users may struggle to remember lengthy and unpredictable passcodes due to the constraints of short and long-term memory. Additionally, users may opt for a password that is too simplistic, thereby compromising the authentication process [11]– [13], [19]. This has led to a growing demand for novel security solutions that are efficient, user-friendly, and reliable. The conventional password-based authentication technologies can be easily duplicated and disseminated, hence the need for more secure options [4], [8].

In recent times, there has been a considerable interest in tactile behavioral authentication, as traditional methods like PIN have limitations and downsides in the security field [4]. However, authentication methods that rely solely on behavioral biometrics may not be accurate enough due to the irregular nature of the movements [20]. Therefore, a persistent authentication system has been proposed whereby the authentication process occurs in real-time throughout the entire interaction. This reduces the need for explicit authentication requirements, thereby providing a more user-friendly experience [22].

Mobile authentication plays a crucial role in protecting users' personal information [21] ،[22].

Previous Research Methodology Aspects

Experimental research necessitates the provision of references to validate the methodology employed in prior research. This involves justifying elements such as the sample size, device type. The inclusion of this data is of paramount importance for the investigation of a new authentication system, as it ensures the soundness of the research and the reliability of the results obtained. Therefore, a comprehensive understanding of these methodological aspects is mandatory for the successful execution of experimental research in this domain.

Size of the Sample

In this particular section, we present a tabulation of the sample size that has been utilized in the studies that were previously selected. The majority of the research articles, approximately nine, indicated a sample size of 2 to 30 individuals, while around three studies made use of a dataset that was obtained from other research articles. It was observed that only three of these papers failed to specify the number of participants that were involved in their study. Based on the literature, it was determined that they developed their tests using 18 sample size articles. Out of the published publications, around 50% of them, which is equivalent to nine out of 18, utilized 30 or fewer individuals, whereas approximately 33% of them, which is equivalent to six out of 18, used 31 to 60 participants. The total sample size that was used in the studies that were selected ranged from 2 to 60 individuals, which was utilized in around 83% of the published publications (n = 15/18). Apart from these studies, three more studies made use of datasets that were gathered by other researchers. It was also observed that three publications mentioned frameworks but did not specify the number of participants that were involved. Figure 2 depicts the Number of samples reported in the academic literature related to the reviewed articles.

Age Group

The selection of participants in research studies varies with regard to the age range considered. The chosen range is not consistent among several selected research. However, most volunteers involved in these studies fall between the ages of 8 and 89 years. Despite there being a study that revealed the participants' ages, 11 other studies did not mention the age of the sample. Nevertheless, some literature papers mentioned the age groups used in the samples during the development of their experiments, and 12 studies reported distinct age groups. The age of the participants was not a significant concern or primary focus of the study in most cases.

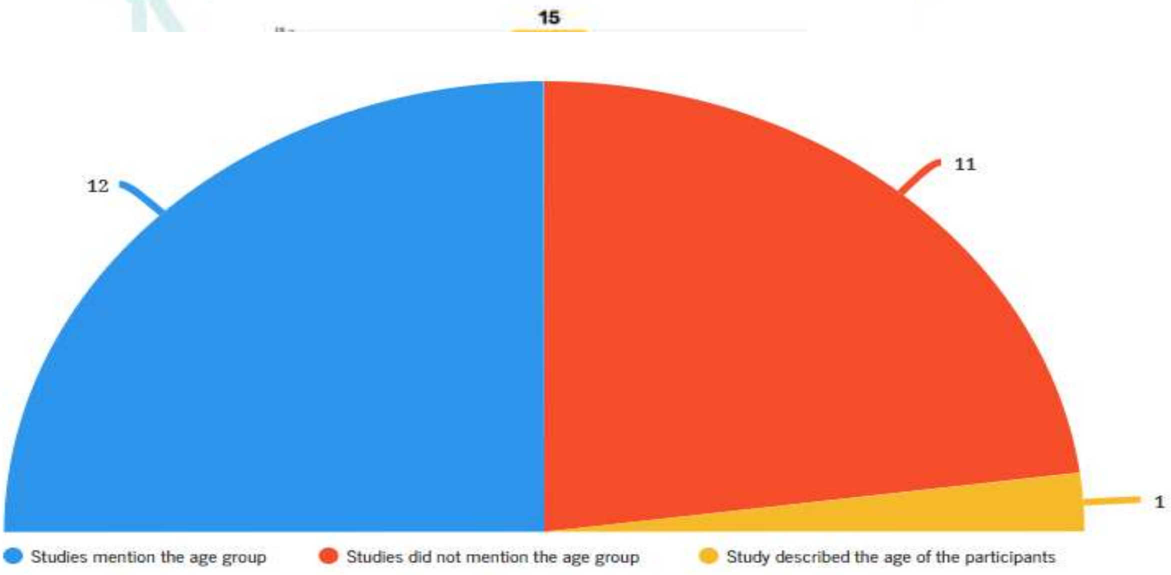


Figure 3. Age group

Due to the varying age groupings, it is challenging to select or divide studies based on age group.

Gender Group

When developers wish to compare the distinct gender groups of the samples utilized in their studies, the gender of the participants plays a significant role. However, none of the selected research had examined or compared gender groupings. Out of the chosen publications, only seven specified the gender of the participants in the samples, while only one described the percentage of the gender of the participants in the sample, and sixteen articles did not mention the gender of the participants. The collected data shows that the number of males outnumbers the number of females. There were eight research publications that dealt with the subject of gender in some capacity. Previous studies have reported the gender distribution without any apparent explanation. With the exception of one study, which favored females over males, all studies favored males over females.

To conduct a comprehensive study, it is crucial to consider the gender of the participants and the different gender groups. However, the literature review indicates that gender groupings have not been adequately explored. Out of the selected research publications, only a few mentioned the gender of the participants, and the number of males was higher than females. This discrepancy in gender distribution may affect the overall results of the studies. Therefore, it is important to take gender into account when selecting participants and analyzing the data. Future studies should focus on creating a balanced gender distribution to ensure the accuracy and validity of the results. Additionally, researchers should provide a clear explanation for their choice of gender distribution to avoid any biases or misunderstandings in the findings. as Figure 4

Types of Equipment

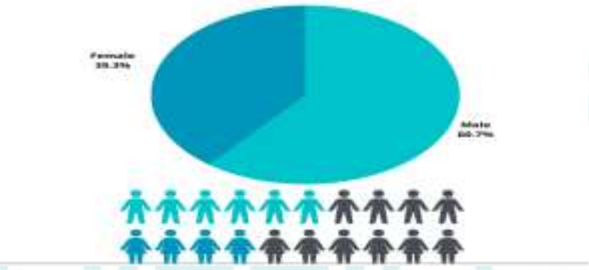


Figure 4. Gender distribution

The present study utilized various types of smartphones for research purposes. The selection of these devices lacked clear criteria. However, pertinent factors such as sensor availability, ease of use, and ease of making basic advancements on the phone were all taken into consideration while selecting a device and operating system. Based on this observation, the majority of choices in these studies were made on the Android platform rather than the iOS platform. Out of the total papers, only 13 identified the type of smart device used for conducting their investigations. The study employed eleven distinct types of smartphones for research purposes.

Samsung emerged as the most frequently used gadget, being employed 10 times, followed by Google with 4 times, and the iPhone being used thrice.

Other smartphone brands such as Huawei, Xiaomi, LG, HTC, Motorola, Sony, and Vivo were used once or twice. The previous research employed 25 smartphones with the Android operating system and three smartphones with the iOS operating system. The Android system was preferred over the iOS system due to its open-source structure, which makes it easy to design and program. Additionally, the Android system is widely distributed and continually developed by the majority of smartphone makers.

In conclusion, the present study employed various types of smartphones for research purposes. The selection of devices was based on pertinent factors such as sensor availability, ease of use, and ease of making basic advancements on the phone. The Android system was preferred over the iOS system due to its open-source structure, which makes it easy to design and program. The use of smartphones in research has several advantages, including cost-effectiveness and real-time data collection. The selection of smartphones for research purposes is a crucial factor that needs to be taken into consideration while conducting research.

Sensors Used in Previous Research

To verify the identities of the users, various smartphones equipped with multiple sensors were utilized. Prior scholarly studies have suggested the employment of an orientation sensor, which includes an accelerometer, gyroscope, and magnetometer, a finger sensor, a camera sensor, a touch screen sensor, and a microphone sensor. The fingerprint sensor, which comprises only 1 out of 54 sensors, the camera sensor, which accounts for 8 out of 54 sensors, the orientation sensor, which makes up 36 out of 54 sensors, the touch screen sensor, which constitutes 6 out of 54 sensors, and the microphone sensor, which represents 3 out of 54 sensors, are the most commonly used sensors, as per research. Notably, no previous studies have explored the applicability of a light sensor for authenticating smartphones. Therefore, the results of this study suggest that further research should be conducted to determine the feasibility of incorporating a light sensor into the user authentication process of smartphones.

Conclusion

Researchers and developers have shown a keen interest in sensors-based smartphone authentication, given the ubiquitous presence of smartphones in our daily lives. These devices are used for an array of tasks such as banking, emailing, chatting, online shopping, video conferencing and health monitoring, among others. The conventional authentication methods used for these tasks may be replaced by biometric authentication, which is a more secure and reliable method. However, the sector still faces numerous concerns, such as data accessibility and authentication usability, which must be addressed. Fortunately, there are several innovative ideas that have been proposed to solve the problems associated with sensors-based smartphone authentication. These solutions hold promise in bridging the gaps in biometric solutions. In addition, these proposed solutions may well serve to enhance the overall security of smartphone authentication, thereby making our daily lives more secure and convenient. Therefore, it is imperative to continue research in this area and develop comprehensive solutions that address all concerns in a holistic manner. Ultimately, this will enable us to leverage the full potential of smartphones while ensuring the safety and security of our personal data.

Reference

1. K. Jiokeng, G. Jakllari, and A.-L. Beylot, “I Want to Know Your Hand: Authentication on Commodity Mobile Phones Based on Your Hand’s Vibrations,” vol. 1, no. 2, doi: 10.1145/3534575ï.
2. A. S. Jouda, A. M. Sagheer, and M. L. Shuwandy, “MagRing-SASB: Static Authentication of Magnetism Sensor Using Semi-Biometric Interaction Magnetic Ring,” *2021 IEEE 11th International Conference on System Engineering and Technology, ICSET 2021 - Proceedings*, pp. 183–188, 2021, doi: 10.1109/ICSET53708.2021.9612555.
3. L. Hernández-álvarez, J. M. de Fuentes, L. González-Manzano, and L. H. Encinas, “Privacy-preserving sensor-based continuous authentication and user profiling: A review,” *Sensors (Switzerland)*, vol. 21, no. 1, pp. 1–23, 2021, doi: 10.3390/s21010092.
4. M. L. Shuwandy, 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 and Applications, CSPA 2022 - Proceeding*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 425–430. doi: 10.1109/CSPA55076.2022.9781888.
5. J. M. Espín López, A. Huertas Celdrán, J. G. Marín-Blázquez, F. Esquembre, and G. Martínez Pérez, “S3: An AI-Enabled User Continuous Authentication for Smartphones Based on Sensors, Statistics and Speaker Information,” *Sensors (Basel)*, vol. 21, no. 11, May 2021, doi: 10.3390/s21113765.
6. X. Zeng, X. Zhang, S. Yang, Z. Shi, and C. Chi, “Gait-Based Implicit Authentication Using Edge Computing and Deep Learning for Mobile Devices,” *Sensors (Basel)*,

vol. 21, no. 13, Jul. 2021, doi: 10.3390/s21134592.

7. M. L. Shuwandy, B. B. Zaidan, and A. A. Zaidan, “Novel authentication of blowing voiceless password for android smartphones using a microphone sensor,” *Multimedia Tools and Applications*, 2022.
8. A. S. Jouda, R. Moceheb, and L. Shuwandy, “MagRing-SASB: Static Authentication of Magnetism Sensor Using Semi-Biometric Interaction Magnetic Ring.”
9. M. L. Shuwandy, 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,” *2022 IEEE 18th International Colloquium on Signal Processing and Applications, CSPA 2022 - Proceeding*, no. May, pp. 425–430, 2022, doi: 10.1109/CSPA55076.2022.9781888.
10. M. Bartlomiejczyk, I. El Fray, M. Kurkowski, S. Szymoniak, and O. Siedlecka-Lamch, “User Authentication Protocol Based on the Location Factor for a Mobile Environment,” *IEEE Access*, vol. 10, pp. 16439–16455, 2022, doi: 10.1109/ACCESS.2022.3148537.
11. W. Yang, M. Wang, S. Zou, J. Peng, and G. Xu, “An implicit identity authentication method based on deep connected attention CNN for wild environment,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Feb. 2021, pp. 94–100. doi: 10.1145/3456415.3457222.
12. S. Mekruksavanich and A. Jitpattanakul, “Deep learning approaches for continuous authentication based on activity patterns using mobile sensing,” *Sensors*, vol. 21, no. 22, Nov. 2021, doi: 10.3390/s21227519.
13. W. Li, W. Meng, and S. Furnell, “Exploring touch-based behavioral authentication on smartphone email applications in IoT-enabled smart cities,” *Pattern Recognit Lett*, vol. 144, pp. 35–41, Apr. 2021, doi: 10.1016/j.patrec.2021.01.019.
14. H. Wang *et al.*, “Who Is Using the Phone? Representation-Learning-Based Continuous Authentication on Smartphones,” *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/6339407.
15. G. Giorgi, A. Saracino, and F. Martinelli, “Using recurrent neural networks for continuous authentication through gait analysis,” *Pattern Recognit Lett*, vol. 147, pp. 157–163, Jul. 2021, doi: 10.1016/j.patrec.2021.03.010.
16. K. Jiokeng, G. Jakllari, and A.-L. Beylot, “I Want to Know Your Hand: Authentication on Commodity Mobile Phones Based on Your Hand’s Vibrations,” vol. 1, no. 2, doi: 10.1145/3534575ï.
17. F. Flamein, B. Bouthinon, and J. Joimel, “Fingerprint-on-Display Module Based on

Organic Optical Sensors for 1-to-4-Finger Authentication in Next-Generation Smartphones,” 2021.

18. Y. Leguesse, C. Colombo, M. Vella, and J. Hernandez-Castro, “PoPL: Proof-of-Presence and Locality, or How to Secure Financial Transactions on Your Smartphone,” *IEEE Access*, vol. 9, pp. 168600–168612, 2021, doi: 10.1109/ACCESS.2021.3137360.
19. Y. Shao, T. Yang, H. Wang, and J. Ma, “Airsign: Smartphone authentication by signing in the air,” *Sensors (Switzerland)*, vol. 21, no. 1, pp. 1–24, Jan. 2021, doi: 10.3390/s21010104.
20. M. Nerini, E. Favarelli, and M. Chiani, “Augmented PIN Authentication through Behavioral Biometrics,” *Sensors*, vol. 22, no. 13, Jul. 2022, doi: 10.3390/s22134857.
21. T. Zhu *et al.*, “EspialCog: General, Efficient and Robust Mobile User Implicit Authentication in Noisy Environment,” *IEEE Trans Mob Comput*, vol. 21, no. 2, pp. 555–572, Feb. 2022, doi: 10.1109/TMC.2020.3012491.
22. O. D. Incel *et al.*, “DAKOTA: Sensor and Touch Screen-Based Continuous Authentication on a Mobile Banking Application,” *IEEE Access*, vol. 9, pp. 38943–38960, 2021, doi: 10.1109/ACCESS.2021.3063424.
23. S. Mekruksavanich and A. Jitpattanakul, “Deep learning approaches for continuous authentication based on activity patterns using mobile sensing,” *Sensors*, vol. 21, no. 22, Nov. 2021, doi: 10.3390/s21227519.
24. P. Delgado-Santos, R. Tolosana, R. Guest, R. Vera-Rodriguez, F. Deravi, and A. Morales, “GaitPrivacyON: Privacy-preserving mobile gait biometrics using unsupervised learning,” *Pattern Recognit Lett*, vol. 161, pp. 30–37, Sep. 2022, doi: 10.1016/j.patrec.2022.07.015.