2023 IEEE/ACIS 21st International Conference on Software Engineering Research, Management and Applications (SERA) | 979-8-3503-4588-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/SERA57763.2023.10197713

Are We Aware? An Empirical Study on the Privacy and Security Awareness of Smartphone Sensors

Arifa I. Champa Md Fazle Rabbi Farjana Z. Eishita Minhaz F. Zibran
Department of Computer Science, Idaho State University, USA
{arifaislamchampa, mdfazlerabbi, farjanaeishita, minhazzibran}@isu.edu

***Abstract*—Smartphones are equipped with a wide variety of sensors, which can pose significant security and privacy risks if not properly protected. To assess the privacy and security risks of smartphone sensors, we first systematically reviewed 55 research papers. Driven by the findings of the systematic review, we carried out a follow-up questionnaire-based survey on 23 human end-users. The results reflect that the participants have a varying level of familiarity with smartphone sensors, and there is a noticeable dearth of awareness about the potential threats and preventive measures associated with these sensors. The findings from this study will inform the development of effective solutions for addressing security and privacy in mobile devices and beyond.**

***Index Terms*—smartphone sensor attacks, security, privacy, awareness, perception**

I. Introduction

Smartphones are an indispensable part of our lives, with small and discreet sensors that play the crucial role of functioning and user experience. Many different types of sensors are found in smartphones, each with its unique function [1]. In addition to providing a better user experience, smartphone sensors also have the potential to improve safety and security [2]. For instance, setting a passcode, the inclusion of fingerprint scanners, and facial recognition technology on smartphones can help protect against unauthorized access to sensitive information.

In recent years, a variety of studies have been carried out to look at the threats and defense mechanisms of various systems [3], [4]. These investigations, however, have frequently concentrated on well-known system vulnerabilities or network-based risks that result from bad architectural design. The thorough explanation of sensor-based risks has thus far mostly been disregarded. This instigates a high level of risk in terms of security and privacy since these systems can be seriously endangered by sensor-based threats.

The usage of smartphone sensors raises significant concerns about security and privacy. For example, an attacker could use a smartphone's GPS sensor to track a user's location without their knowledge [5]. Similarly, a phone's camera or microphone can be hacked to record an audio or video clip without the user's knowledge [6]. Motion sensors on mobile devices could be exploited to secretly infer the PINs or passwords inputted by users on mobile web applications [7].

While some users may be aware of smartphone sensors' potential security and privacy risks, others may possess less or no awareness of the risks associated with the sensors. Lack of awareness could lead to users unknowingly sharing their sensitive information, resulting in security breaches or loss of privacy. A clear understanding of the present scenario is required to understand this level of risks and awareness. With this level of understanding, individuals and organizations can initiate informed decisions for protection against cyber attacks and data leaks.

Therefore, in this work, we first conduct a systematic review of existing research in the literature on smartphone sensors' security and privacy issues. Later, an end-user survey is conducted to assess user awareness and perception of the privacy and security risks associated with smartphone sensors. In particular, we address the following research questions:

RQ1: To what extent are individuals familiar with sensors in smartphones?

RQ2: How well are people aware of the existing mobile phone sensor attacks?

RQ3: How do people perceive the use of these sensors?

Several works in the past have explored smartphone sensor-based threats including end-user awareness and perception of the threats [8]–[12], [12]–[16]. These earlier studies were conducted either as literature reviews or end-user surveys only. Ours is the first work along this direction taking on wholistic approach combining both a systematic literature review and follow-up end-user survey.

We organize our paper as follows. First, we describe our systematic literature review in Section II. Then, in Section III, we describe our end-user survey, which is designed based on the findings from the systematic literature review. In Section IV, we further discuss the results from both the literature review and end-user survey including the threats to validity of the results as well as our plan for future work. Finally, Section V concludes the paper.

II. Systematic Literature Review

A. Methodology

Our systematic review was carried out using the following four phases:

Phase-1 (Search of Research Articles): The seven databases mentioned in Table I were chosen for their well-known sources of scholarly research in a wide range of fields to identify relevant research articles. The search for articles to be included in this systematic review began in November 2022 using a keyword-based substring search method. These searched keywords are listed in Table I.

979-8-3503-4588-9/23/$31.00 ©2023 IEEE
SERA 2023, May 23-25, 2023, Orlando, USA

TABLE I
KEYWORDS USED FOR SEARCHING RELEVANT PAPERS

Database	Searched Keywords
ACM Digital Library	[[‘Smartphone’ OR ‘Mobile’] AND [‘sensor’]] AND [‘security’ OR ‘privacy’ OR ‘awareness’]
ScienceDirect	[[‘Smartphone’ OR ‘Mobile’] AND [‘sensor’ OR ‘sensors’]] AND [‘security’ OR ‘privacy’ OR ‘awareness’]
IEEE Xplore	[[‘Smartphone’ OR ‘Mobile’] AND [‘sensor’ OR ‘sensors’]] AND [‘security’ OR ‘privacy’ OR ‘awareness’] NOT [‘IoT’ OR ‘Wearable’]
Springer	[‘Smartphone’ OR ‘Mobile’] AND [‘sensor’ AND ‘security’ AND ‘privacy’ AND ‘awareness’]
Taylor & Francis	[[‘Smartphone’ OR ‘Mobile’] AND [‘sensor’]] AND [‘security’ OR ‘Sensor privacy’] NOT [‘IoT’ OR ‘Wearable’]
PubMed	[[‘Smartphone’ OR ‘Mobile’] AND [‘sensors’]] AND [‘security’ OR ‘privacy’] NOT [‘IoT’ OR ‘wearable’]
MDPI	[‘Smartphone sensor’ OR ‘Mobile sensor’ AND [‘security’ OR‘privacy’ OR ‘awareness’]] NOT [‘IoT’ OR ‘wearable’]

TABLE II
INCLUSION AND EXCLUSION CRITERIA

Inclusion criteria	Exclusion criteria
Smartphone sensors and security or privacy or awareness	Irrelevant to smartphone sensors security or privacy or awareness
Research article	Book, chapter, reviewed article
Published between 2010 and 2022	Not peer-reviewed papers
Written in English language	Papers not accessible online
	Articles related to wearable smart devices and IoT

Phase-2 (Preliminary Filtering): Table II outlines the specific criteria that have been applied to determine the articles that are included in the review and those that are excluded.

Phase-3 (Final Filtering): The PRISMA-P (Preferred Reporting Items for Systematic Reviews and Meta-Analyses Protocols) [17] guidelines were followed (as shown in Figure 1) to identify relevant papers, ensuring a systematic and thorough review.

Phase-4 (Analysis): The relevant information identified from the reviewed research articles is then further analyzed around the research questions outlined before. This analysis leading to findings is elaborated in the following section (Section II-B).

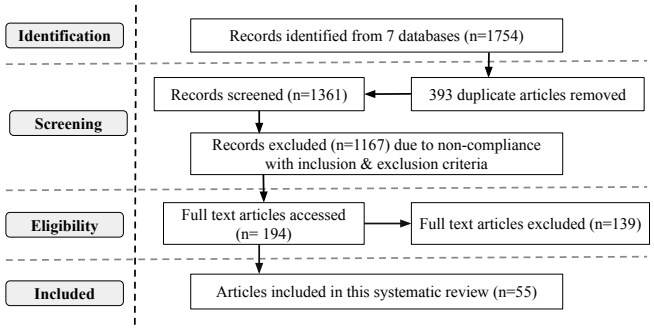

Fig. 1. States of our work at different stages of PRISMA-P

TABLE III
NUMBER OF PAPERS SELECTED FROM DIFFERENT SOURCES

Database	Identification	Eligibility	Included
ScienceDirect	327	25	9
IEEE Xplore	477	79	18
Springer	308	24	10
Taylor & Francis	34	7	1
PubMed	399	12	3
MDPI	26	6	2
ACM Digital Library	183	41	12
Total	1754	194	55

B. Analysis and Findings

The searched keywords in Table I were used to identify relevant studies published from 2010 to 2022 for the systematic review. The search result yielded 1754 articles among which 393 were duplicate articles. After removing the duplicates, 1361 articles were left for the screening phase. 139 papers were excluded from 194 eligible articles for full-text evaluation. Finally, 55 articles were included in the study. The states of the work at different stages of PRISMA-P [17] are summarized in Figure 1 and the numbers of articles selected from different sources are listed in Table III. We thoroughly read all 55 papers and identified various kinds of attacks that can be carried out using smartphone sensors.

1) Sensor-related Security Threats: We found eight such threats that are most commonly discussed in the literature. These eight common threats are briefly described below.

Keystroke Inference (KIn): An attacker can potentially determine the exact keystrokes entered, including sensitive information such as passwords or credit card numbers, by analyzing the subtle vibrations and movements of the device as the user types.

Location Inference (LIn): A LIn attack using smartphone sensors is when data is collected and the physical position of a smartphone user is determined without the user’s knowledge or consent.

Device Fingerprinting (DFP): A DFP attack based on smartphone sensor data encompasses creating a unique device profile or ‘fingerprint’ based on the sensor data, which can then be used to track the device and its user across various applications and services.

Task Inference (TIn): A TIn attack is to infer the user’s current activity or task, such as browsing the internet or sending a message without the user’s knowledge or consent.

Eavesdropping (Evd): An Evd attack refers to the unauthorized interception and recording of audio using the smartphone’s microphone, without the user’s awareness or consent.

Transmitting Malicious Sensor Commands (TMC): TMC involves the unauthorized manipulation of sensor data by sending malicious commands to the device’s sensors.

Pin Inference (PinIn): A PinIn involves the unauthorized inference or extraction of the user’s PIN or password by analyzing the sensor data.

Physical and Behavioral Activity Recognition (PhBAR): An attacker can potentially deduce the user’s current

TABLE IV
VARIOUS THREATS AND ISSUES RELATED TO SMARTPHONE SENSORS

Threats	#	Research Articles	Smartphone Sensors
LIn	11	[18]–[28]	Barometer, Gyroscope, Accelerometer, Speaker, Camera, Magnetometer, Microphone, GPS, Compass, WiFi, NFC
TIn	10	[6], [7], [29]–[36]	Gyroscope, Accelerometer, Speaker, Ambient Light Sensor, Magnetometer, Microphone, Biometric Sensors, Camera, GPS, WiFi, Bluetooth, NFC
KIn	6	[37]–[42]	Gyroscope, Accelerometer, Speaker, Ambient Light Sensor, Magnetometer, Microphone, Biometric Sensors, Camera, Proximity Sensor, WiFi, Bluetooth, NFC
Evd	8	[35], [43]–[49]	Gyroscope, Accelerometer, Speaker, Ambient Light Sensor, Magnetometer, Microphone, Bluetooth
TMC	2	[35], [46]	Ambient Light Sensor, Microphone, WiFi, Bluetooth
DFP	7	[41], [48], [50]–[54]	Gyroscope, Accelerometer, Speaker, Microphone, Camera, Biometric Sensors, WiFi, Bluetooth, NFC
PinIn	4	[9], [45], [55], [56]	Biometric Sensor, Gyroscope, Accelerometer, Magnetometer, Barometer, Proximity Sensor, Ambient Light Sensor
PhBAR	13	[6], [18], [19], [21], [22], [26]–[28], [30], [57]–[60]	GPS, Camera, Microphone, Speaker, Biometric Sensor, Gyroscope, Accelerometer, Magnetometer, Barometer, Compass, WiFi

activity or behavior by analyzing the patterns and timing of the user's interactions with the device's sensors.

Table IV identifies the smartphone sensors associated with these threats and the articles in the literature that at least mentioned them. We also identified that 15 sensors are particularly reported susceptible to threats. Based on the type of smartphone's operations these sensors are used for, they are categorized into four groups and presented in Table V. The literature suggests that environmental sensors, which measure factors such as temperature and humidity, are generally less known to users compared to other types of sensors [11], [13].

TABLE V
15 SMARTPHONE SENSORS CATEGORIZED IN GROUPS

Sensor Type	Sensors
Identity-related	GPS, Microphone, Speaker, Camera, Biometric
Communicational	WiFi, Bluetooth, Near-field communication (NFC)
Motion	Gyroscope, Accelerometer, Proximity, Magnetometer
Environmental	Ambient Light Sensor, Barometer, Compass

2) Protection Mechanisms: We also identified various mechanisms that were discussed in the literature for protection against attacks on smartphone sensors. In Table VI, we briefly present the synopsis, performance, and overhead of the security and privacy preserving mechanisms identified.

III. END USER SURVEY

Now, we want to understand three aspects: (a) to what extent the smartphone end-users are familiar with the 15 smartphone sensors (classified in four categories) that are identified (from literature survey) as susceptible to attacks or data leaks. (b) To what extent the end-users are aware of the smartphone sensor-related security threats and the identified mechanisms identified from the literature survey. (c) How the end-users perceive the use of the 15 smartphone sensors. Aspects (a), (b), and (c) are respectively addressed in research questions RQ1, RQ2, and RQ3 outlined in Section I. We, therefore, carried out a questionnaire based survey on smartphone end-users as described below.

A. Survey Procedure

1) Questionnaire: The questionnaire we used for the survey is briefly presented in Table VII. The Likert-scale questions (i.e., 12, 14, 15, and 17) about familiarity, the participants had the followings five options to choose from: extremely, moderately, somewhat, slightly, and not at all. Along with the questionnaire, a set of three appendices were also provided to the participants. The appendices included brief description of the 15 sensors, the sensor-based attacks, and the security mechanisms against the sensor-based attacks.

2) Participant Recruitment: First, we recruited 15 student participants from a computer science class at the Idaho State University. Then additional eight participants were recruited for the study from the entire institution. Out of the total 23 participants, 14 completed the survey in person, while the remaining nine participants completed it online via Google Forms. More than half of the participants are Asians, and none are African Americans. Out of the 23 participants recruited, seven are females and 16 are males with ages between 20 and 40 years, with the majority (13) falling in the age range of 20-24. Among these participants, nine (39.13%) have a bachelor's degree, eight (34.78%) have a college degree, five (21.74%) have a graduate degree, and one (4.35%) have a high school degree. Among the 23 participants, 13 use iOS and the rest use Android. Most of the participants have good technical knowledge, either as students or from a work environment. The amount of time spent per day on the internet, using apps, and the duration of smartphone ownership on average are 3.33 hours per day, 2.42 hours per day, and 11.8 years respectively. The details of the participants' internet and smartphone usage is shown in Table VIII.

3) Participants' Response Analysis: After collecting the questionnaire responses from all the participants, a thorough analysis was performed on these collected data. To gain insight into the participants' perception of smartphone sensors, we identify True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN) in participants responses. Then, we compute precision (ρ) and recall ($\mathcal{R}$) for the responses.

B. Survey Outcome

1) Familiarity (RQ1): The participants are found the most familiar with the camera and least familiar with the magnetometer. The ranking of the smartphone sensors' familiarity among the participants based on the responses to the survey

TABLE VI
SECURITY AND PRIVACY PRESERVING MECHANISMS IDENTIFIED

Mechanisms	Synopsis	Performance
SemaDroid [61]	• Android sensor management system • Uses simulated data to evaluate the potential risks of apps • Offers users the ability to customize sensor policies to their liking	100% accurate against sensor-based malware
AWare [62]	• An authorization framework • Allows users to authorize sensitive sensor operations • Binds application operation requests to the corresponding user input events	Successful compatibility and usability test with 1000 most downloaded Android apps
EnTrust [63]	• Android Sensor authorization framework • Generates authorization queries in response to input occurrences from complying programs and delegation graphs	Low overhead in Android smartphones
6thSense [64]	• An intrusion detection system • Employs sensor data to comprehend the context of the user's activity • Identifies malicious activity on the device	Achieved 96% accuracy against many sensor-based threats with minimal overhead
LocPPM [65]	• Employs Synthetic data to mimic real data • Uses targeted movements to combine real and synthetic sensor data	Decreases the likelihood of a white-box attack by 3%
AuDroid [66]	• A trust evaluation framework • Scrutinizes app demands for sensor access and decides whether the access is legit • Detects instances of over-privilege and defend sensors from unauthorized access	High accuracy tested with 17 mobile applications on an Android smartphone
SensorSafe [67], [68]	• Based on trusted remote data stores and a broker who arbitrates access to the data stores of the users	Prevents unauthorized access to sensed data of workers' identity and position
Perceptual Assistant [69]	• A privacy protection system • Allows modification of personalized sensor policy for all third-party sensing apps	Less than 7.6% overhead and high adaptability
Android Extension [70], [71]	• Manages information and stops malicious applications • Uses semantically rich context models (Xposed framework)	Effectively enforces privacy over sensed and contextual data without scalability issues

TABLE VII
SURVEY QUESTIONNAIRE

1. Age? (15-19, 20-24, 25-29, 30-34, 35-39, 40 years or more)
2. Gender? (Male, Female, Other)
3. What is the highest educational level you have attained? (High School, College, Bachelors, Masters, Doctoral)
4. What is your profession?
5. Ethnicity? (Caucasian, African American, Asian, Hispanic, Other)
6. Time spent on the internet per day in hours? (>2, 2-5, 6-10, <10)
7. What do you use the internet for? Check all that apply. (Social Media, Research, Education, Entertainment, Financial Purpose, Others)
8. How many hours per day do you spend browsing the internet?
9. Average number of hours spent using smartphone apps per day?
10. How long have you been using a smartphone (in years)?
11. Operating system of your smartphone (Android, iOS, or Windows)?
12. What is your level of concern (in Likert scale) about unauthorized access to data?
13. Have you personally experienced privacy or security issues while using a smartphone? Check all that apply (options in Table X).
14. Familiarity with 15 smartphone sensors (Table V) in Likert scale?
15. Awareness about the security threats (Table IV) in Likert scale?
16. Perception of 15 smartphone sensors (Table V) with respect to the security threats (Table IV), (i.e., sensor × threats)?
17. Familiarity with the security mechanism (Table VI) in Likert scale?

TABLE VIII
PARTICIPANTS' USAGE OF INTERNET AND SMARTPHONES

Age Range	#	Internet Usage (in hours/day)	App Usage (hours/day)	Owning Smartphone (in years)
20-24	13	3.23	2.69	8.38
25-29	6	3.83	3.00	8.33
30-34	2	3.50	2.00	11.50
35-40	2	2.75	2.00	19.00

questionnaire is listed in Table IX. From the systematic review part, it was found that environmental sensors are not well-known to users [11], [13]. However, this is not reflected in the results of our survey, as the participants are found to be least familiar with motion sensors. Table X presents the percentage of participants who reported to have first-hand experience of facing privacy and security issues when using a smartphone in given different scenarios. When questioned about their experiences with privacy and security threats, 13 (57%) participants reported having experienced at least one attack, while six (26%) reported experiencing two or more attacks. Their response to the possibility of facing privacy and security issues while using a smartphone is shown in Table X. Furthermore, among participants who used the internet for more than 10 hours per day, 18 (80%) reported being exposed to at least one attack. This implies that heavy internet users may be particularly vulnerable to these types of attacks. We derive the answer to RQ1 as follows:

Ans. to RQ1: *Identity-related sensors are the most familiar, while motion sensors are the least familiar to the end-users.*

TABLE IX
PARTICIPANTS' FAMILIARITY WITH SMARTPHONE SENSORS

Rank*	Sensors	Rank*	Sensors
1	Camera	09	Ambient Light Sensor
2	Microphone	10	NFC
3	Speaker	11	Gyroscope
4	WiFi	12	Accelerometer
5	GPS	13	Proximity Sensor
6	Bluetooth	14	Barometer
7	Compass	15	Magnetometer
8	Biometrics		

*Rank 1 indicates the most familiar

TABLE X
SECURITY/PRIVACY ISSUES FACED BY THE PARTICIPANTS

Privacy and security issues	Faced
The smartphone had a virus or other harmful software installed	26%
Passwords or other account information for banking, email, social networking, or other personal accounts were stolen and exploited	35%
Was misled to pay for or use a service that turned out to be a scam	17%
Personal or private information was posted on the Internet on social networks or online forums without permission	10%
Nothing suspicious was ever noticed	43%
Other	10%

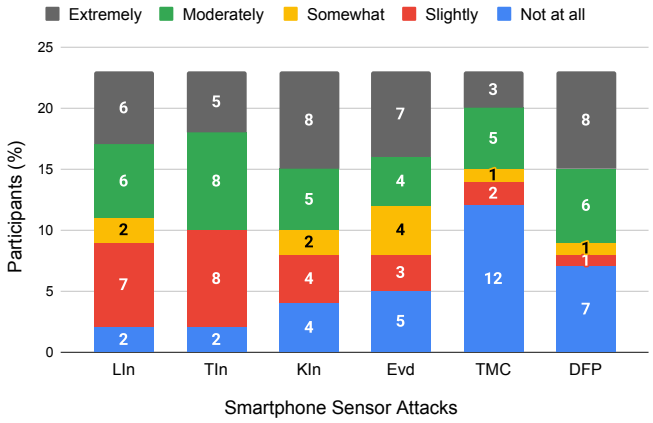

Fig. 2. Participants' awareness of smartphone sensor-based attacks

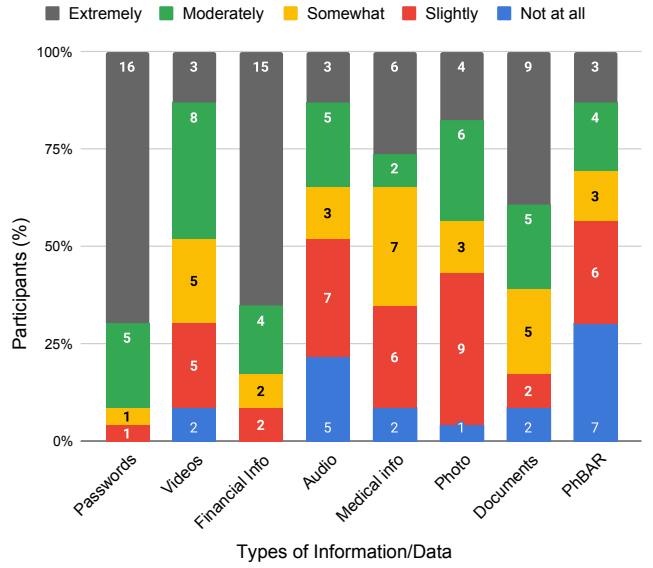

Fig. 3. Participants' levels of concern about unauthorized access

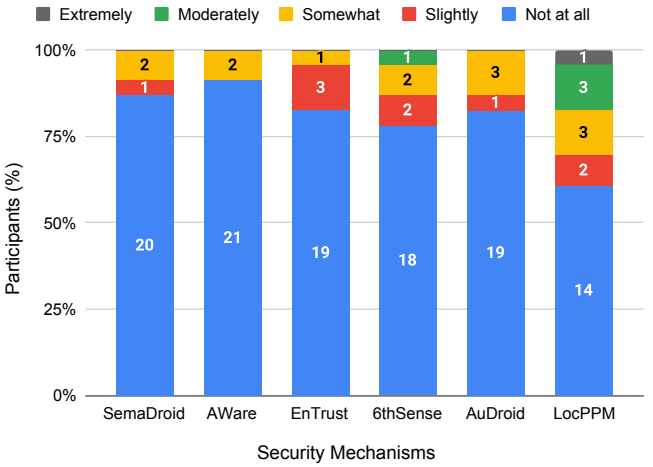

Fig. 4. Participants' familiarity with existing security mechanisms

2) Awareness (RQ2): On average, the participants are aware of the six sensor attacks mentioned in the survey. However, the participants are least aware of TMC and most aware of DFP and KIn. Figure 2 provides a visual representation of the level of awareness associated with all the attacks. The majority of the participants exhibit the most concern about the security of their passwords and financial information in response to unauthorized access. In contrast, only a small number of participants expressed concern about the potential for PhBAR to be used to access their information without their permission. The level of concern for each aspect of unauthorized access is illustrated in Figure 3. However, the majority of the participants in the study are not at all aware of the security mechanism's capabilities for protecting against sensor attacks, with only a small number being somewhat familiar, and only one individual being extremely familiar with one of the mechanisms. Familiarity of the participants with the available security preserving mechanisms is presented in Figure 4. We, therefore, formulate the answer to RQ2 as follows:

> ***Ans. to RQ2:*** *Participants are the least aware of TMC threat. The majority of the participants are not aware of the security mechanisms against sensor attacks.*

TABLE XI
PERCEPTION OF THE THREATS ASSOCIATED WITH SMARTPHONE SENSORS

Sensors	LIn	TIn	KIn	Evd	TMC	DFP	TP	TN	FP	FN	ρ	$\mathcal{R}$
Camera	11	4	2	5	5	3	20	48	10	60	0.67	0.25
Microphone	3	10	2	18	4	4	41	0	0	97	1.00	0.30
Speaker	2	8	2	11	3	5	28	20	3	87	0.90	0.24
WiFi	8	9	2	3	7	5	34	0	0	104	1.00	0.25
GPS	17	3	3	1	2	3	20	83	9	26	0.67	0.43
Bluetooth	3	10	3	6	8	5	32	20	3	83	0.91	0.28
Compass	14	2	1	0	3	4	14	105	10	9	0.58	0.61
Biometrics	1	3	1	0	8	10	14	60	9	55	0.67	0.20
Ambient Light Sensor	0	7	1	1	9	2	18	44	2	74	0.90	0.20
NFC	2	6	1	2	9	5	14	35	11	78	0.56	0.15
Gyroscope	12	7	1	0	4	3	23	19	4	92	0.85	0.20
Accelerometer	14	4	3	2	7	2	25	16	7	90	0.78	0.22
Proximity Sensor	8	3	2	2	10	5	2	87	28	21	0.07	0.09
Barometer	1	1	0	5	4	7	14	104	11	16	0.39	0.30
Magnetometer	8	7	5	0	6	1	21	17	6	94	0.78	0.18

3) Perception (RQ3): To measure participants' perception of smartphone sensors and sensor attacks, a survey question (i.e., question 16) asked them to identify which attacks are possible for which of the 15 sensors. The seven columns from the left in Table XI shows the participants' perceptions of sensor-related threats as well as the facts drawn from the literature review as well as the computed TP, TN, FP, FN, precision (ρ), and recall ($\mathcal{R}$). Here, a reddish-colored cell indicates that the literature identified corresponding sensor *susceptible* to the corresponding security threat. For example, according

to the literature, the camera can potentially cause LIn, TIn, KIn, and DFP threats. A white/colorless cell indicates that literature identified corresponding sensor *not* susceptible to the corresponding security threat. For example, according to the literature, the camera is not vulnerable to Evd or TMC attacks.

A value in a cell reports the number of survey participants reported to believe/perceive the corresponding sensor susceptible to the corresponding security threat. For example, 11 participants correctly perceived that camera is susceptible to the LIn attack. But five participants incorrectly thought that the camera is vulnerable to Evd. Five participants incorrectly also thought that the camera is vulnerable to TMC.

That is why the FP value for the camera is 10, while TP is 20 as a total of 20 participants correctly identified the LIn (11 participants), TIn (four participants), KIn (two participants), and DFP (three participants) threats posed by the camera. We see that the proximity sensor has the lowest precision and recall values. This indicates that participants have the most incorrect perceptions about the proximity sensor. In contrast, their perceptions of the WiFi and microphone sensors are more accurate. Based on the precision (ρ) and recall ($\mathcal{R}$) values, it can be concluded that participants have relatively accurate perceptions of the other surveyed sensors in smartphones. We derive the answer to RQ3 as follows:

Ans. to RQ3: *Participants' perceptions of the proximity sensor are the most inaccurate, whereas their views of the WiFi and microphone sensors are the most precise.*

IV. Discussion

While a systematic literature review identifies the gaps in the current state of the art, a follow-up end-user study complements with a comprehensive understanding of the topic with new insights, as accomplished in our work. In our study, the survey result demonstrates that the participants are less familiar with motion sensors, which differs from the findings of our systematic review where environmental sensors were the least familiar [13]. In terms of sensor attacks, there is a conflicting familiarity with device fingerprinting, with some users being extremely knowledgeable and others having no knowledge at all. Additionally, the participants are not familiar with security and privacy-preserving mechanisms against smartphone sensor attacks. This lack of familiarity may make participants more vulnerable to sensor-based attacks, as they may not be aware of the potential risks or know how to protect themselves from these types of attacks.

A concerning factor the survey demonstrated is that a majority of participants reported experiencing at least one attack during the usage of a smartphone. It is noticed that those who spend a significant amount of time online are at a higher risk of experiencing privacy and security issues while using their smartphones. Individuals need to educate themselves about smartphone sensor attacks to protect themselves.

Passwords or PINs are an essential barrier to preventing unauthorized access. Participants show the highest level of concern for password protection for their personal information. However, participants have the least concern about the risks associated with PhBAR. But they do not understand that this collects a large amount of data about a person's activity, location, speed, duration of the activity, and even stress level. These data can be accessed by unauthorized parties and lead to sensitive personal information being exposed to third parties. Then this information can be used for a variety of nefarious purposes, such as targeted marketing, information selling, disclosing classified data, and inferring and manipulating user habits [72]. By understanding the different ways in which sensors can be exploited, they can take steps to prevent these attacks and protect their sensitive information.

The survey illustrates that the participants have the highest number of incorrect perceptions about the proximity sensor, as indicated by its low precision and recall values. Moreover, the familiarity of sensors is somewhat in line with the participant perception level, except for the magnetometer. The participant's perception of this sensor is moderately clear with 78% precision, even though it is the least familiar one. The survey findings suggest that familiarity with a sensor may not necessarily correlate with participant perception.

A. Threats to Validity

We recognize that our participant group is not very diverse and consists primarily of individuals with a technical background. While analyzing the survey responses, we did not take into account whether the participants used iOS or Android smartphones. Analyzing this aspect could have revealed some interesting findings. From the systematic literature review, we identified eight sensor attacks (listed in Table IV), from which we chose six sensors for the survey. We identified nine security measures (Table VI) from the literature review. In our survey, we chose the recently reported six security measures. This may be argued as a limitation of our work.

A limitation of our end-user survey is that it relies only on self-report questionnaire responses, which may be subject to exaggeration or other biases. It would have been more informative to conduct a live interview with the participants to get a more accurate understanding of their perceptions. This could have provided a more in-depth understanding of their views and experiences.

B. Future Work

By addressing these limitations, we gain a better understanding of the human impact of this rapidly advancing technology and provide reliable recommendations. Therefore, we plan to increase diversity by reaching out to a varied demographic groups, communities, and/or organizations. The inclusion of participants with little to no technical knowledge would provide a more comprehensive picture of the actual situation. Additionally, we aim to analyze the survey responses based on the smartphone's two major operating systems (i.e. Android and iOS).

V. Conclusion

Smartphone sensor awareness is a crucial kind of literacy required to secure individual's confidential information to

avoid breach or cyber attack. The utmost goal of this research was to investigate individuals' familiarity, their level of awareness and perception on smartphone sensors. To achieve this goal, in this study, we analyzed the privacy, security, and awareness concerns of smartphone sensors involving an extensive systematic review and a subsequent questionnaire-based survey conducted both online and in person.

The systematic literature review highlights the complex and multifaceted nature of smartphone technology, with both benefits and risks to consider. We conducted the descriptive investigation to establish the foundation for the research, to identify interesting phenomena, and developed the research questions to analyze further. The results from the end-user survey revealed that identity-related sensors are the most familiar to the participants, while motion sensors are the least familiar. Furthermore, participants have a distorted perception of the proximity sensor and are unaware of the security mechanisms available to protect against various sensor-related attacks.

These findings emphasize the importance of users being aware of the potential risks and taking steps to protect their data and privacy. In future, we plan to address the limitations identified in subsection IV-A and extend this work for further research on the vulnerabilities and attacks associated with different types of smartphone sensors.

REFERENCES

[1] "Sensors overview — android developers," https://developer.android.com/guide/topics/sensors/sensors_overview, (Accessed on 02/13/2023).

[2] S. Brady, "The brainpower behind smart sensors and their use in security," 2018.

[3] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and A. Ribagorda, "Evolution, detection and analysis of malware for smart devices," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 961–987, 2013.

[4] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *2016 IEEE symposium on security and privacy (SP)*, 2016, pp. 636–654.

[5] S. M. Maharjan, A. Poudyal, A. van Heerden, P. Byanjankar, A. Thapa, C. Islam, B. A. Kohrt, and A. Hagaman, "Passive sensing on mobile devices to improve mental health services with adolescent and young mothers in low-resource settings: the role of families in feasibility and acceptability," *BMC medical informatics and decision making*, vol. 21, no. 1, pp. 1–19, 2021.

[6] C. Stachl, Q. Au, R. Schoedel, S. D. Gosling, G. M. Harari, D. Buschek, S. T. Völkel, T. Schuwerk, M. Oldemeier, T. Ullmann *et al.*, "Predicting personality from patterns of behavior collected with smartphones," *Proceedings of the National Academy of Sciences*, vol. 117, no. 30, pp. 17 680–17 687, 2020.

[7] R. Song, Y. Song, Q. Dong, A. Hu, and S. Gao, "Weblogger: Stealing your personal pins via mobile web application," in *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, 2017, pp. 1–6.

[8] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats and attacks to smart devices and applications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1125–1159, 2021.

[9] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "Stealing pins via mobile sensors: actual risk versus user perception," *International Journal of Information Security*, vol. 17, no. 3, pp. 291–313, 2018.

[10] K. Crager and A. Maiti, "Information leakage through mobile motion sensors: User awareness and concerns," in *Proceedings of the European Workshop on Usable Security (EuroUSEC)*, 2017.

[11] M. Mehrnezhad, E. Toreini, and S. Alajrami, "Making sense of sensors: mobile sensor security awareness and education," in *7th Workshop on Socio-Technical Aspects in Security and Trust*, 2018, pp. 40–52.

[12] J. L. Kröger, L. Gellrich, S. Pape, S. R. Brause, and S. Ullrich, "Personal information inference from voice recordings: User awareness and privacy concerns." *Proc. Priv. Enhancing Technol.*, vol. 2022, no. 1, pp. 6–27, 2022.

[13] M. Mehrnezhad and E. Toreini, "What is this sensor and does this app need access to it?" in *Informatics*, vol. 6, no. 1, 2019, p. 7.

[14] L. Hernández-Álvarez, J. M. de Fuentes, L. González-Manzano, and L. Hernández Encinas, "Privacy-preserving sensor-based continuous authentication and user profiling: a review," *Sensors*, vol. 21, no. 1, p. 92, 2020.

[15] C. Gao, K. Fawaz, S. Sur, and S. Banerjee, "Privacy protection for audio sensing against multi-microphone adversaries," *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 2, pp. 146–165, 2019.

[16] B. Struminskaya, V. Toepoel, P. Lugtig, M. Haan, A. Luiten, and B. Schouten, "Understanding willingness to share smartphone-sensor data," *Public Opinion Quarterly*, vol. 84, no. 3, pp. 725–759, 2020.

[17] L. Shamseer, D. Moher, M. Clarke, D. Ghersi, A. Liberati, M. Petticrew, P. Shekelle, and L. A. Stewart, "Preferred reporting items for systematic review and meta-analysis protocols (prisma-p) 2015: elaboration and explanation," *Bmj*, vol. 349, 2015.

[18] M. Ehatisham-ul Haq, M. A. Azam, Y. Asim, Y. Amin, U. Naeem, and A. Khalid, "Using smartphone accelerometer for human physical activity and context recognition in-the-wild," *Procedia Computer Science*, vol. 177, pp. 24–31, 2020.

[19] K. Muralidharan, A. Ramesh, G. Rithvik, S. Prem, A. Reghunaath, and M. Gopinath, "1d convolution approach to human activity recognition using sensor data and comparison with machine learning algorithms," *International Journal of Cognitive Computing in Engineering*, vol. 2, pp. 130–143, 2021.

[20] H. Ye, L. Sheng, T. Gu, and Z. Huang, "Seloc: Collect your location data using only a barometer sensor," *IEEE Access*, vol. 7, pp. 88 705–88 717, 2019.

[21] A. Subasi, D. H. Dammas, R. D. Alghamdi, R. A. Makawi, E. A. Albiety, T. Brahimi, and A. Sarirete, "Sensor based human activity recognition using adaboost ensemble classifier," *Procedia computer science*, vol. 140, pp. 104–111, 2018.

[22] Y. Watanabe and S. Sara, "Toward an immunity-based gait recognition on smart phone: a study of feature selection and walking state classification," *Procedia Computer Science*, vol. 96, pp. 1790–1800, 2016.

[23] Z. Fyke, I. Griswold-Steiner, and A. Serwadda, "Prying into private spaces using mobile device motion sensors," in *2019 17th International Conference on Privacy, Security and Trust (PST)*, 2019, pp. 1–10.

[24] S. Azzakhnini and R. C. Staudemeyer, "Extracting speech from motion-sensitive sensors," in *ESORICS 2020 International Workshops on Data Privacy Management, Cryptocurrencies and Blockchain Technology*, 2020, pp. 145–160.

[25] F. Zhao, L. Gao, Y. Zhang, Z. Wang, B. Wang, and S. Guo, "You are where you app: An assessment on location privacy of social applications," in *2018 IEEE 29th International Symposium on Software Reliability Engineering (ISSRE)*, 2018, pp. 236–247.

[26] W. Zhang and X. Wang, "A lightweight user state monitoring system on android smartphones," in *ICSOC 2014 Workshops on Service-Oriented Computing*, 2014, pp. 259–269.

[27] S. Zhuo, L. Sherlock, G. Dobbie, Y. S. Koh, G. Russello, and D. Lottridge, "Real-time smartphone activity classification using inertial sensors—recognition of scrolling, typing, and watching videos while sitting or walking," *Sensors*, vol. 20, no. 3, p. 655, 2020.

[28] R. Wampfler, S. Klingler, B. Solenthaler, V. R. Schinazi, M. Gross, and C. Holz, "Affective state prediction from smartphone touch and sensor data in the wild," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1–14.

[29] S. Aguinaga and C. Poellabauer, "Stealthy health sensing to objectively characterize motor movement disorders," *Procedia Computer Science*, vol. 19, pp. 1182–1189, 2013.

[30] S. Zhao, Z. Zhao, R. Huang, Z. Luo, S. Li, J. Tao, S. Cheng, J. Fan, and G. Pan, "Discovering individual life style from anonymized wifi scan lists on smartphones," *IEEE Access*, vol. 7, pp. 22 698–22 709, 2019.

[31] J. Massollar and A. C. B. Garcia, "Fencebot: an elderly tracking app for mitigating health risk contacts," in *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 2021, pp. 1009–1014.

[32] X. Liu, J. Liu, and W. Wang, "Exploring sensor usage behaviors of android applications based on data flow analysis," in *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, 2015, pp. 1–8.

[33] E. Struse, J. Seifert, S. Üllenbeck, E. Rukzio, and C. Wolf, "Permissionwatcher: Creating user awareness of application permissions in mobile systems," in *Int.l Joint Conf. on Ambient Intelligence*, 2012, pp. 65–80.

[34] W. Han, C. Cao, H. Chen, D. Li, Z. Fang, W. Xu, and X. S. Wang, "sendroid: Auditing sensor access in android system-wide," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 407–421, 2017.

[35] R. Zhang, X. Chen, S. Wen, and J. Zheng, "Who activated my voice assistant? a stealthy attack on android phones without users' awareness," in *2nd International Conference Machine Learning for Cyber Security*, 2019, pp. 378–396.

[36] R. Ning, C. Wang, C. Xin, J. Li, and H. Wu, "Deepmag: Sniffing mobile apps in magnetic field through deep convolutional neural networks," in *2018 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2018, pp. 1–10.

[37] S. Huang, R. Wu, Y. Wang, Y. Sun, J. Zhang, and X. Li, "Inferring user input through smartphone gyroscope," in *2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, 2022, pp. 623–628.

[38] A. Al-Haiqi, M. Ismail, and R. Nordin, "On the best sensor for keystrokes inference attack on android," *Procedia Technology*, vol. 11, pp. 989–995, 2013.

[39] R. Song, Y. Song, S. Gao, B. Xiao, and A. Hu, "I know what you type: Leaking user privacy via novel frequency-based side-channel attacks," in *2018 IEEE Global Communications Conference*, 2018, pp. 1–6.

[40] L. Cai and H. Chen, "On the practicality of motion based keystroke inference attack," in *5th International Conference on Trust and Trustworthy Computing*, 2012, pp. 273–290.

[41] Z. Yang, R. Zhao, and C. Yue, "Effective mobile web user fingerprinting via motion sensors," in *17th IEEE International Conference On Trust, Security And Privacy*, 2018, pp. 1398–1405.

[42] A. R. Javed, S. U. Rehman, M. U. Khan, M. Alazab, and H. U. Khan, "Betalogger: Smartphone sensor-based side-channel attack detection and text inference using language modeling and dense multilayer neural network," *Transactions on Asian and Low-Resource Language Information Processing*, vol. 20, no. 5, pp. 1–17, 2021.

[43] J. L. Kröger and P. Raschke, "Is my phone listening in? on the feasibility and detectability of mobile eavesdropping," in *IFIP Annual Conference on Data and Applications Security and Privacy*, 2019, pp. 102–120.

[44] S. Chakraborty and O. Tripp, "Eavesdropping and obfuscation techniques for smartphones," in *Proceedings of the International Conference on Mobile Software Engineering and Systems*, 2016, pp. 291–292.

[45] S. Naval, A. Pandey, S. Gupta, G. Singal, V. Vinoba, and N. Kumar, "Pin inference attack: A threat to mobile security and smartphone-controlled robots," *IEEE Sensors Journal*, vol. 22, no. 18, pp. 17 475–17 482, 2021.

[46] L. Lei, Y. Wang, J. Zhou, L. Wang, and Z. Zhang, "A threat to mobile cyber-physical systems: Sensor-based privacy theft attacks on android smartphones," in *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2013, pp. 126–133.

[47] Y. Liu, K. Huang, X. Song, B. Yang, and W. Gao, "Maghacker: eavesdropping on stylus pen writing via magnetic sensing from commodity mobile devices," in *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*, 2020, pp. 148–160.

[48] M. Diamantaris, F. Marcantoni, S. Ioannidis, and J. Polakis, "The seven deadly sins of the html5 webapi: A large-scale study on the risks of mobile sensor-based attacks," *ACM Transactions on Privacy and Security (TOPS)*, vol. 23, no. 4, pp. 1–31, 2020.

[49] S. A. Anand, C. Wang, J. Liu, N. Saxena, and Y. Chen, "Spearphone: a lightweight speech privacy exploit via accelerometer-sensed reverberations from smartphone loudspeakers," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021, pp. 288–299.

[50] X.-Y. Li, H. Liu, L. Zhang, Z. Wu, Y. Xie, G. Chen, C. Wan, and Z. Liang, "Finding the stars in the fireworks: Deep understanding of motion sensor fingerprint," *IEEE/ACM Transactions on Networking*, vol. 27, no. 5, pp. 1945–1958, 2019.

[51] C. Yue, "Sensor-based mobile web fingerprinting and cross-site input inference attacks," in *2016 IEEE Security and Privacy Workshops (SPW)*, 2016, pp. 241–244.

[52] R. Matovu and A. Serwadda, "Gaming the gamer: Adversarial fingerprinting of gaming apps using smartphone accelerometers," in *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2018, pp. 489–496.

[53] Y. Lee, J. Li, and Y. Kim, "Micprint: acoustic sensor fingerprinting for spoof-resistant mobile device authentication," in *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2019, pp. 248–257.

[54] R. Kosono, T. Nishio, M. Morikura, K. Yamamoto, Y. Maki, T. Goda, H. Matsukawa, and T. Indo, "Mobile user identification by camera-based motion capture and mobile device acceleration sensors," in *Proceedings of the 13th Workshop on Challenged Networks*, 2018, pp. 25–31.

[55] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "Touchsignatures: identification of user touch actions and pins based on mobile sensor data via javascript," *Journal of Information Security and Applications*, vol. 26, pp. 23–38, 2016.

[56] R. Spreitzer, "Pin skimming: exploiting the ambient-light sensor in mobile devices," in *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, 2014, pp. 51–62.

[57] A. T. Sabir, H. S. Maghdid, S. M. Asaad, M. H. Ahmed, and A. T. Asaad, "Gait-based gender classification using smartphone accelerometer sensor," in *2019 5th International Conference on Frontiers of Signal Processing (ICFSP)*, 2019, pp. 12–20.

[58] M. Ehatisham-ul Haq, M. Azam, U. Naeem, S. Rehman, and A. Khalid, "Identifying smartphone users based on their activity patterns via mobile sensing," *Procedia computer science*, vol. 113, pp. 202–209, 2017.

[59] G. KV, U. Sait, T. Kumar, R. Bhaumik, S. Shivakumar, and K. Bhalla, "Design and development of a smartphone-based application to save lives during accidents and emergencies," *Procedia Computer Science*, vol. 167, pp. 2267–2275, 2020.

[60] M. Rabbi, S. Ali, T. Choudhury, and E. Berke, "Passive and in-situ assessment of mental and physical well-being using mobile sensors," in *Proceedings of the 13th international conference on Ubiquitous computing*, 2011, pp. 385–394.

[61] Z. Xu and S. Zhu, "Semadroid: A privacy-aware sensor management framework for smartphones," in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, 2015, pp. 61–72.

[62] G. Petracca, A. Atamli-Reineh, Y. Sun, J. Grossklags, and T. Jaeger, "Aware: Preventing abuse of privacy-sensitive sensors via operation bindings." in *USENIX Security Symposium*, 2017, pp. 379–396.

[63] G. Petracca, Y. Sun, A. Atamli-Reineh, P. D. McDaniel, J. Grossklags, and T. Jaeger, "Entrust: Regulating sensor access by cooperating programs via delegation graphs." in *USENIX Security Symposium*, 2019, pp. 567–584.

[64] A. K. Sikder, H. Aksu, and A. S. Uluagac, "6thsense: A context-aware sensor-based attack detector for smart devices." in *USENIX Security Symposium*, 2017, pp. 397–414.

[65] G. Petracca, L. M. Marvel, A. Swami, and T. Jaeger, "Agility maneuvers to mitigate inference attacks on sensed location data," in *MILCOM 2016-2016 IEEE Military Communications Conference*, 2016, pp. 259–264.

[66] G. Petracca, Y. Sun, T. Jaeger, and A. Atamli, "Audroid: Preventing attacks on audio channels in mobile devices," in *Proceedings of the 31st Annual Computer Security Applications Conference*, 2015, pp. 181–190.

[67] H. Choi, S. Chakraborty, Z. M. Charbiwala, and M. B. Srivastava, "Sensorsafe: a framework for privacy-preserving management of personal sensory information," in *8th Workshop on Secure Data Management*, 2011, pp. 85–100.

[68] H. Choi, S. Chakraborty, and M. B. Srivastava, "Design and evaluation of sensorsafe: A framework for achieving behavioral privacy in sharing personal sensory information," in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012, pp. 1004–1011.

[69] K. Zhao, D. Zou, H. Jin, Z. Tian, W. Qiang, and W. Dai, "Privacy protection for perceptual applications on smartphones," in *2015 IEEE International Conference on Mobile Services*, 2015, pp. 174–181.

[70] D. Ghosh, A. Joshi, T. Finin, and P. Jagtap, "Privacy control in smart phones using semantically rich reasoning and context modeling," in *2012 IEEE symposium on Security and privacy workshops*, 2012, pp. 82–85.

[71] P. Jagtap, A. Joshi, T. Finin, and L. Zavala, "Preserving privacy in context-aware systems," in *2011 IEEE Fifth International Conference on Semantic Computing*, 2011, pp. 149–153.

[72] P. Jayakumar, L. Lawrence, R. L. W. Chean, and S. N. Brohi, "A review and survey on smartphones: The closest enemy to privacy," in *2nd International Conference on Emerging Technologies in Computing*, 2019, pp. 106–118.