"A Comprehensive Survey of Wearable Technology and its Barriers for Forensic Investigation"

Ms. Swagata Shashikant Zarkar

PG-Research Scholar

Government Institute Of Forensic Science, Aurangabad, Maharashtra, India 431001

Mr. Rahul Kailas Bharati

Assistant Professor

Government Institute Of Forensic Science, Aurangabad, Maharashtra, India 431001

*Dr. Shobha Kamalakar. Bawiskar

Assistant Professor

Government Institute Of Forensic Science, Aurangabad, Maharashtra, India 431001

Corresponding Author - * Dr. Shobha Kamalakar Bawiskar

Address - Government Institute of Forensic Science, Nipat Niranjan Nagar, Near Caves Road, Aurangabad, Maharashtra, 431001 India

Abstract:

Smart watches are wearable devices that combine the functions of a traditional watch with those of a smartphone. They are typically equipped with a touchscreen display, wireless connectivity, and the ability to run apps, collect fitness statistics, and receive notifications from a linked smartphone. Depending on the type and software installed, smart watches can perform a number of functions. This article focused on health indicators such as heart rate monitoring, breathing activity, sleep quality, and physical activity. The purpose of this research paper is to study the various components related with the use of smart watches in the field of health in order to assess the security features and associated hazards. The accuracy and utility of health parameters indicated in hardware and software are investigated.

Keyword: Wearable Technology, Fitness Tracking, Smart Watches, Device Security, Survey

INTRODUCTION

1.1 Introduction to smartwatch:

Investigating crimes and other legal matters using scientific methods and procedures is known as forensic science. On the other hand, smartwatches are wearable gadgets that may monitor a variety of physiological and physical data, including heart rate, level of activity, and sleep habits. The potential use of smartwatch data as evidence in criminal investigations is what ties forensic science and smartwatch readings together. For instance, if a crime took place at a particular time and place, the smartwatch data of a suspect or victim may reveal important details about their whereabouts and activities at that moment. Similar to this, if a suspect says they were asleep when the crime was committed; their smartwatch sleep data may either confirm or disprove their alibi. It's crucial to remember that using wristwatch data as evidence in court cases is still a very new practice, and there are still a number of concerns that need to be resolved, including those relating to data accuracy and privacy. The individual laws and rules of a particular jurisdiction may also have an impact on whether such evidence is admissible in court. Since its introduction in the early 2000s, smartwatches have advanced significantly. In 2004, Microsoft introduced the SPOT watch, the first wristwatch. It was a wristwatch that displayed news, sports results, and other information using FM radio transmissions. However, the SPOT watch didn't become very well-known because of its few features and high cost. [1]

Wearable gadgets known as smartwatches have become increasingly popular in recent years thanks to their versatility in performing tasks including messaging, phone calls, and fitness tracking, among others. Typically, a smartwatch has a touchscreen display, wireless connectivity, and sensors that can track bodily functions and health indicators. With the development of technology, smartwatches have evolved to include capabilities like voice assistants, mobile payments, and stand-alone cellular connectivity. [2] The global smartwatch market was estimated to be worth $20.64 billion in 2019 and is anticipated to reach $96.31 billion by 2027, rising at a CAGR of 19.7% from 2020 to 2027 (Allied Market Research, 2020). One of the factors boosting the growth of the smartwatch market is the rising consumer awareness of health and fitness as well as the growing acceptance of wearable technology. [2]

1.2 Basic Facts Regarding Smartwatches

Sr.No.	Features of watch	Device 1 Fire Boltt BSW007 [3]	Device 2 Boult Drift Bluettoth Calling [4]	Device 3 Gadgetzone I8 Pro Max [5]	Device 4 Gizmore GIZFIT 907 [6]	Device 5 Noise ColorFit Pro 2 [7]	Device 6 Boat Wave Beat [8]
1	Price @ 19 April 2023	1,599	1,799	840	1,899	1,199	1,499
2	Water resistant	Yes	Yes	Yes	Yes	Yes	Yes
3	Scratch resistant screen	No	No	No	No	No	No
4	Crash detection and emergency SOS	No	No	No	No	No	No
5	Battery life	5 days	10 days	10 days	12 days	10 days	7 days
6	Advanced sensors	Yes	Yes	Yes	Yes	Yes	Yes
7	ECG tracker	No	No	No	No	No	No
8	Design	Full metal body & ultra lightweight	Lightweight	Lightweight	Lightweight	Stylish & lightweight	Slim metallic design
9	Display size	1.3 inches	1.69 inches	44 mm	14 inches	1.3 inches	1.69 inches
10	Track sleep	Yes	Yes	Yes	Yes	Yes	Yes
11	GPS system	No	No	No	No	No	No
12	Calling	No	Yes	Yes	No	No	No
13	Mobile payment	No	No	No	No	No	No
14	Compatibility OS-iOS, Android	Android & iOS	Android & iOS	Android & iOS	Android & iOS	Android & iOS	Android & iOS
15	Music	No	Yes	Yes	No	No	Yes
16	Connectivity	Bluetooth	Bluetooth	Bluetooth	Bluetooth	Bluetooth	Bluetooth
17	Touchscreen	Yes	Yes	Yes	Yes	Yes	Yes

Table No.[1] – General information about smartwatches used for study.

Images of smartwatch used for study:

Fig[1.1]- Fire Boltt smartwatch	Fig[1.2]- Boult Drift Smartwatch	Fig[1.3]-I8 Pro Max smartwatch
Fig[1.4]- Gizmore smartwatch	Fig[1.5]- Noise smartwatch	Fig[1.6]- Boat Wave Beat smart watch

Fig. [1]- Smartwatch images for research Work

Hardware Devices

    A. Basic Parameters

        1. Blood Pressure(diastolic, systolic mm/hg(millimeter of mercury)), 60/90

        2. Heart Rate BPM(Beats per minute) , 60-100 bpm

        3. sleep(hours and minutes), 8 hours

        4. walking steps(steps), target 7000 steps/day

        5. Blood oxygen Level(% percenage),95-100%

6. Outdoor running, mileage as per Time(Hrs and Min), Pace(min/km), consumption of calorie(Kcal)

7. Female Menstrual Cycle Tracking,

8. Drink water reminder

   B. Training Parameters

1. Cycling (bpm and KCAL)

2. Swimming

3. Football(steps, bpm and KCAL)

4. Skipping (bpm and KCAL)

5. Badminton (steps, bpm and KCAL)

6. Basketball (steps, bpm and KCAL)

Software Application

1. Heart Rate Monitor-Pulse App

2. Step counter-Pedometer

3. GoogleFit: Activity Tracking

4. Blood Pressure Measurement App

5. Samsung Health

Health care Sector vis- a vis data breach :

Health care security refers to the rules and practices in place to protect the privacy, accuracy, and accessibility of sensitive patient and healthcare provider personal and medical information. Data breaches, cyberattacks, theft, and unauthorized access to medical records are all protected from in this. [9,10] Cyber security is becoming more important than ever in the healthcare sector since sensitive patient information is stored and sent through electronic health records (EHRs) and other digital technologies. Health care organizations are required by the Health Insurance Portability and Accountability Act (HIPAA) and other laws to protect patient data; failure to do so may result in expensive data breaches and legal action. The confidentiality, integrity, and availability of patient data must be guaranteed, and medical devices and systems must be protected from outside attacks as part of cyber security in healthcare. [11, 12]

Wearable technology and digital health platforms' legal ramifications

When you purchase a wearable gadget, you enter all of your personal information into it, raising questions about how safe the data is stored. Whether the service provider or the device's manufacturer is in charge of such data. These inquiries are essential to answering in order to assess the dangers to people's privacy rights whose data is stored in such devices. The right to privacy is a fundamental right guaranteed by Articles 14, 19, and 21 of the Indian Constitution, according to the Supreme Court's decision in the case of K.S. Puttaswamy v. Union of India. [13]

Even though users of social media and wearable technology may not think they are providing information voluntarily, their use and participation lead to the gathering of vast amounts of information about people's preferences, choices, and lives. A legitimate expectation of privacy exists for certain types of data, including medical information. This underscores the Court's commitment to protecting individual medical information and the reasonable expectation that no one will violate a person's right to privacy.

The Ministry of Family and Health Welfare approved the DISHA, or Digital Information Security in Healthcare Act of 2018, which is sometimes abbreviated as DISHA. This law would include both the collection and processing of health data as well as the rights of data owners. A National Authority and other State entities make up the panel of digital health authorities that has been established. Although it focuses on information gathered voluntarily at healthcare facilities, it also discusses other methods of gathering medical information.[14]

The primary component of Indian law governing data protection issues is the Information Technology Act of 2000 (IT ACT 2000). As the first piece of legislation to address these issues, it created a paradigm of notice and consent for privacy. Additionally, it set penalties for breaches of data privacy. The 2016 Electronic Health Record Standards are advised but not required by law. These are frequently mentioned in the customer data protection policies of firms. In the lack of any national or international standards particular to wearable technologies, it is recommended that wearable technology and service providers have acceptable security practices and processes in place to safeguard sensitive personal data and user information.[15]

Forensic significance of smartwatch:

Smart watches have forensic relevance because of the abundance of data they can supply, which makes them useful instruments in forensic investigations. Smartwatches specifically can offer location data, heart rate tracking, and biometric data that can be used in investigations. According to one study, a suspect's movements can be reconstructed using the location monitoring capabilities of a smartwatch, which can then be used as evidence in a criminal case. [16] A different study discovered that heart rate tracking data from smartwatches can be utilized to confirm a person's alibi or disprove a suspect's assertions. [17] Last but not least, forensic investigations can benefit from the biometric data collected by smartwatches, such as fingerprints or facial recognition. [18]In conclusion, smartwatches can be useful forensic evidence in investigations and should be taken into account.

Experimental Methodology:
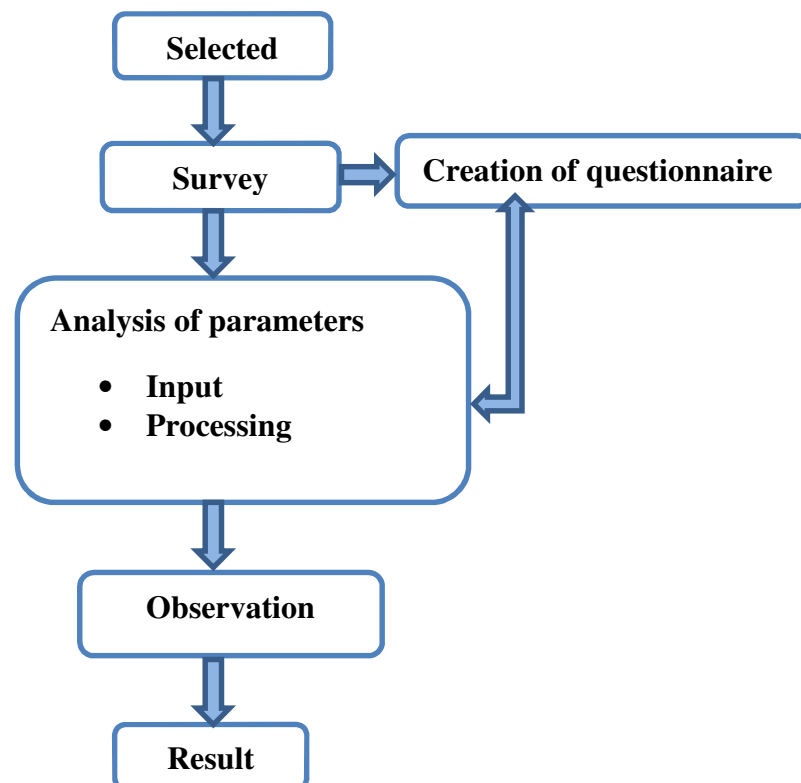
Fig.[2] - Proposed Methodology

METHODOLOGY

We conduct research on the security characteristics of smartwatches. Ten questions pertaining to the security aspects and health parameters of smartwatches are framed in this survey (questionnaire).

Study design: A questionnaire regarding the security characteristics of smartwatches was created.

Selection criteria – Who are utilizing a smartwatch in their daily lives and are willing to participate in the study were the selection criteria.

Sample size –participants between the age group of 15 to 50.
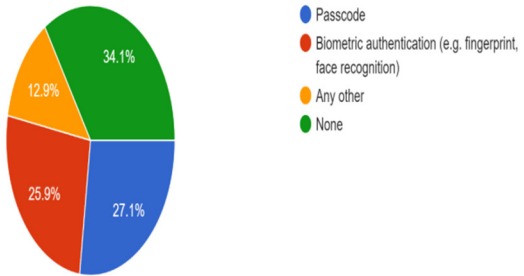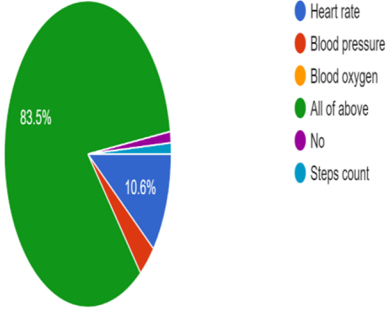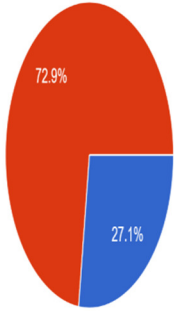
Inclusive Participation of Population - Normal population within age limit 15 to 50 yrs.
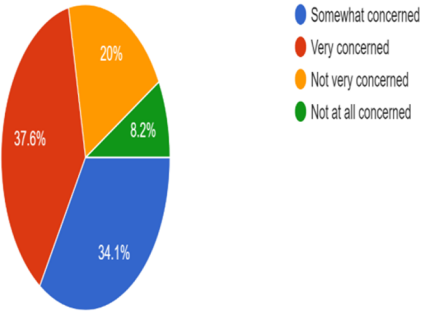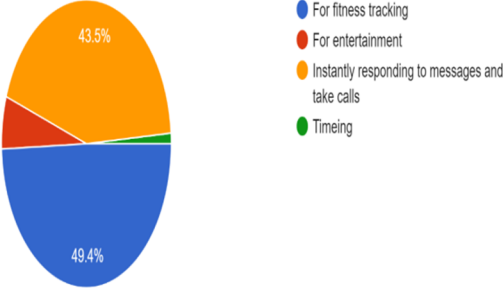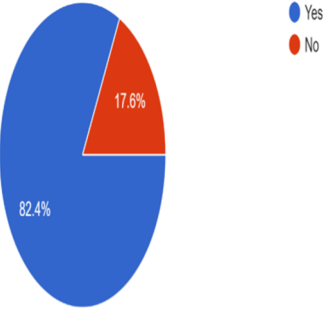
Exclusive Participation of Population - We excluded the population like pregnant women's, HIV patients, Cancerous patients' abnormal behavior and who have any kind of disorder or disease

Procedure: The simple questionnaire was prepared containing 10 questions related to the security features and health parameters of smartwatch. The participants have to fill the Google form by selecting the appropriate option according to smartwatch they use. Each question in the questionnaire has multiple choice options. Questions from the survey and replies received are shown in Table No. [2].

Experimental Observation

Sr. No.	Questions	Options	Diagrammatic representation of survey responses
1.	Which brand of smartwatch do you prefer?	1. Noise 2. Samsung 3. Fastrack 4. Other	
2.	How much often do you update the security features on your smartwatch?	1. Regularly 2. Once a week 3. Once a year 4. Never	

3.	What security features does your smartwatch have?	1. Passcode 2. Biometric authentication (e.g. fingerprint, face recognition) 3. Any other 4. None	**3) What security features does your smartwatch have?** 85 responses Passcode 27.1%, Biometric authentication (e.g. fingerprint, face recognition) 25.9%, Any other 12.9%, None 34.1%
4.	Which of the following health parameters do you track using your smart watch?	1. Heart rate 2. Blood pressure 3. Blood oxygen 4. All of above	**4) Which of the following health parameters do you track using your smartwatch?** 85 responses Heart rate 10.6%, Blood pressure, Blood oxygen, All of above 83.5%, No, Steps count
5.	Have you shared your health data collected by smartwatch with your healthcare provider?	1. Yes 2. No	**5) Have you shared your health data collected by smartwatch with your healthcare provider?** 85 responses Yes 27.1%, No 72.9%

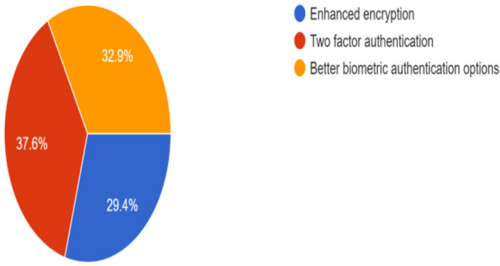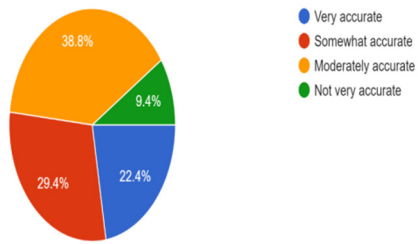|			
6.	How concerned are you about the security of your smartwatch?	1. Somewhere concerned 2. Very concerned 3. Not very concerned 4. Not at all concerned	6) How concerned are you about the security of your smartwatch? 85 responses ● Somewhat concerned ● Very concerned ● Not very concerned ● Not at all concerned 20% 8.2% 37.6% 34.1%
7.	What activities do you primarily use your smartwatch for?	1. For fitness tracking 2. For entertainment 3. Instantly responding to messages and to take calls 4. Timeing	7) What activities do you primarily use your smartwatch for? 85 responses ● For fitness tracking ● For entertainment ● Instantly responding to messages and take calls ● Timeing 43.5% 49.4%
8.	Do you feel that the health monitoring features of your smartwatch help to improve overall health and wellness?	1. Yes 2. No	8) Do you feel that the health monitoring features of your smartwatch help to improve overall health and wellness? 85 responses ● Yes ● No 17.6% 82.4%

9.	What security measures do you think smartwatch should have to prevent unauthorized access?	1. Enhanced encryption 2. Two factor authentication 3. Better biometric authentication options 4. Other	
10.	How accurate do you think the fitness tracking and health monitoring features are on your smartwatch?	1. Very accurate 2. Somewhat accurate 3. Moderately accurate 4. Not very accurate	

Table No. [2] – Questions from the survey and replies received

The brand of smartwatches and the percentage (%) of participants who use each is shown in the **Table No.[3]**.

Sr.No.	Brand of Smartwatch	Use of particular brand of smartwatch by participants (%)
1.	Fire boltt	7.2%
2.	Realme	6%
3.	Boat	4.8%
4.	Connect	1.2%
5.	Boat wave	1.2%
6.	Boult	1.2%
7.	Sonata	1.2%
8.	One plus	1.2%
9.	I8 pro max	1.2%
10.	Oppo	1.2%
11.	iPhone	1.2%
12.	T55	1.2%
13.	Redmi	1.2%
14.	Honor	1.2%
15.	Fossil	1.2%
16.	HW12	1.2%

Table No. [3]- Participants use a specific brand of smartwatch.

Conclusion:

In conclusion, this project work offers important perspectives on the forensic examination of smartwatches. The study emphasizes how crucial it is to take into the health indicators provided by smartwatches account. To look into any incidents that happened while wearing a smartwatch, forensic investigation must be performed. In order to find important evidence for criminal investigations, forensic scientists must examine the accessible digital data. This study emphasizes the necessity of this role. To keep up with the quick advancement of wearable technology devices like smartwatches, the project work emphasizes the need for ongoing investment in forensic science research. We conducted this study on a typical population, excluding people who were HIV positive, pregnant, exhibited odd behavior, or had any other type of disease. The heart rate, sleep habits, and activity levels of the wearer are among the health and fitness data that smartwatches also gather. In circumstances involving physical assaults or accidents, this information may be utilized to ascertain the wearer's physical condition at a specific time.

A. Professional medical advice Health professionals estimate that software and smart gadgets make mistakes 10–20% of the time. In actuality, individualised treatment is advised based on a variety of environmental and situational factors, and traditional approaches must be employed to obtain 100% precise health metric data. Another issue is that by constantly monitoring health results, one runs the risk of making individuals anxious and placing them in perilous situations.

According to a survey, the majority of participants favors the Noise wristwatch brand and mostly uses it for fitness tracking, although they also use it for entertainment and texting. The majority of responders have a passcode or biometric authentication for security, and many frequently update the security measures on their smartwatch. Heart rate is the most frequently monitored health indicator, and some respondents have disclosed their health information to healthcare professionals. Overall, the study indicates that consumers use their smartwatch for a range of activities, with health being a key one.

5.2 Discussion:

- Only a small portion of the population in the target age range of 15 to 50+ was taken into account due to time constraints in the survey.
- Health professionals estimate that software and smart gadgets make mistakes 10–20% of the time. In actuality, individualized treatment is advised based on a variety of environmental and situational factors, and traditional approaches must be employed to obtain 100% precise health metric data. The risk of making individuals worried and placing them in perilous situations if one is continually monitoring health findings is another issue. We did not include anyone who were HIV positive, pregnant, had odd behavior, or had any other form of disorder from this study's regular population.
- Researching the security features of smartwatches will reveal information about the security precautions that manufacturers are currently taking. The study can also provide insight into consumers' opinions of how much people trust the level of security offered by makers of smartwatches.

List of Abbreviations

HIV	-Not Applicable	Cal	Calorie
EHRs	-Electronic Health Records	BP	Blood Pressure
HIPAA	-Health Insurance Portability and Accountability Act	mmHg	-Millimeter(s) of mercury
DISHA	-Digital Information Security in Healthcare Act	DBP	-Diastolic Blood Pressure
&	-and	Yr/Yrs	-Year/Years
IT Act	- Information Technology Act of 2000	BPM	Beats Per Minute
%	-Percentage	SBP	-Systolic Blood Pressure

Competing interests-"The authors Ms. Swagata Shashikant Zarkar, Mr. Rahul Kailas Bharati, Dr. Shobha Kamalakar Bawiskar declares that they have no competing interests" We are not receiving or having financial competing and non-financial competing interests

Funding-This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors

Disclaimer- Researcher only conducts a pilot study on various available hardware and software tools In this research, researcher never encourages / do not promote / do not advertise any specific applications.

REFERENCES

1) Lunden, I. (2013, April 30). Pebble smartwatch raises $10.2m on Kickstarter, shipping starts January 2013. TechCrunch. https://techcrunch.com/2013/04/30/pebble-watch-raises-10-2m-on-kickstarter-shipping-starts-january-2013/
2) Allied Market Research. (2020). Smartwatch market by type, application, and operating system: global opportunity analysis and industry forecast, 2020–2027. https://www.alliedmarketresearch.com/smartwatch-market
3) Manual of Fire Boltt BSW007smartwatch.
4) Manual of Boult Drift calling smartwatch.
5) Manual of Gadgetzone I8 Pro Max smartwatch.
6) Manual of Gizmore GIZFIT 907smartwatch.
7) Manual of Noise ColorFit Pro 2 smartwatch.
8) Manual of Boat Wave Beat smartwatch.
9) U.S. Department of Health and Human Services. (n.d.). Health Information Privacy. Retrieved from https://www.hhs.gov/hipaa/index.html
10) World Health Organization. (2018). Health financing for universal coverage and health system performance: Concepts and definitions. Retrieved from https://www.who.int/health_financing/documents/health-system-performance/en/
11) U.S. Department of Health and Human Services. (n.d.). HIPAA Security Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/index.html
12) HealthITSecurity.com. (2021). Healthcare Cybersecurity. Retrieved from https://healthitsecurity.com/topics/healthcare-cybersecurity
13) Constitution of India
14) DISHA , 2018
15) IT Act and *Electronic Health Record Standards 2016*

16) Kaur, A., & Verma, M. (2018). Cyber security in healthcare industry. International Journal of Computer Science and Network Security, 18(6), 247-254.
17) Hossain, M. A., & Rahman, M. A. (2017). Biometric authentication in healthcare: A case study of improved forensic investigation. International Journal of Knowledge and Learning, 12(3/4), 295-309.
18) Bhaiji, F., Al-Wahaibi, A., Al-Alawi, M., & Al-Azri, H. (2019). Medicolegal and ethical implications of data breaches in healthcare: A review. International Journal of Healthcare Management, 1-8.