IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 January 2023, accepted 16 February 2023, date of publication 6 March 2023, date of current version 14 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3252903

RESEARCH ARTICLE

The Role of IoT in Woman's Safety: A Systematic Literature Review

MUHAMMAD SHOAIB FAROOQ[1], AYESHA MASOOMA[1], UZMA OMER[2], RABIA TEHSEEN[3], S. A. M. GILANI[4], AND ZABIHULLAH ATAL[5]

[1]Department of Computer Science, University of Management and Technology, Lahore 54000, Pakistan
[2]Department of Information Science, Division of Science and Technology, University of Education, Lahore 54770, Pakistan
[3]Department of Computer Science, University of Central Punjab, Lahore 54590, Pakistan
[4]Department of Computer Science, National University of Computer and Emerging Sciences, Lahore 54700, Pakistan
[5]Department of Computer Science, Kardan University, Kabul 1007, Afghanistan

Corresponding author: Zabihullah Atal (z.atal@kardan.edu.af)

ABSTRACT Women's safety has been highlighted as one of the major concerns of any society where several women are dealing with various safety issues like harassment, rape, molestation, and domestic violence due to different social or cultural reasons. Internet of Things (IoT) is becoming a promising technology to support day-to-day concerns and provide support in handling various affairs. Many IoT-based devices have been introduced by the community to help women deal with their potential safety threats. This study presents a systematic literature review of research studies exhibiting the IoT devices for women's safety, the main features these devices offer as well as the wearable, sensors used, and the machine learning algorithms used. The review is carried out by carefully examining and synthesizing the research articles published between 2016 to 2022 in well-reputed research venues. The results revealed that different types of sensors are used to capture the state of women undergoing safety issues where the pulse-rate, and pressure sensors are most commonly used sensors in these devices. In addition, the devices used different technology to transmit the alerts including global positing system (GPS), global system for mobile communication (GSM), and Raspberry pi. Furthermore, several machine learning algorithms such as logistic regression, hidden Markov, and decision trees are used to identify the potential under threat women and help prevent the undesirable situation for women beforehand. It was identified that despite producing notable research in the underlying domain the systems emphasizing auto-activation of alert generation with lesser human interaction and improved accuracies are required to be developed for effectively addressing the concern. In addition to reviewing the literature, this study suggests a taxonomy posing different techniques, features, wearables, and sensors used in IoT-based women safety devices. Furthermore, the gaps and challenges pertaining to the IoT devices and their usability for women's safety have also been highlighted. In addition, this work proposes an architectural model that presents prominent components necessary to develop IoT-based women's safety devices. Lastly, this study emphasizes the use of combinations of sensors to get multiple types of input data that could lead to determining the possibility of threat with better accuracies and precisions.

INDEX TERMS Women's safety, women's safety using IoT, safety devices, human safety, machine learning, IoT-based security devices.

I. INTRODUCTION

Women's safety has been one of the critical issues where several women are globally facing different types of threats such as violence, molestation, and harassment. Many organizations reported the statistics about women's violence cases indicating the worldwide severity of the issue. ActionAid UK reported at International Safe Cities for Women that nine out of ten women have dealt with some sort of violence [1]. The findings of WHO (World Health Organization) also showed that every one in three women are subject to violence globally [2]. The Global Gender Gap

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

Report showed that every fifth woman is suffering sexual violence globally [3]. These figures show that the women re becoming unsafe day-by-day [4], [5]. Women face safety issues at public places, which include workplaces and markets, as well as in their houses. Women are harassed not only during night-time or evening but also during daylight even in public places. Almost 80% of women have fear of being not safe at all [6]. In the recent situation, women are employed and working outside to meet their ends but there is a lack of safety for them. The crimes against women are increasing where the security of women is becoming one of the most important concerns of societies these days. Efforts are required to prevent occurrences of these cases enabling the women to live their lives with confidence and perform their roles in society effectively. The infusion of technology supported many walks of life in combatting the prevailing issues and difficulties [7]. In the same vein, the use of technology needs to be explored to find how it can support to prevent occurrence of women's violence cases and help women deal with potential situation of security threat and danger.

Internet of Things (IoT) has emerged as a promising field of study that provides support through technological assisted solutions of connected devices. Several IoT-based devices have been introduced by the community for the safety and protection of women. Some of these devices automatically capture and identify the safety concerns through their voice recognition systems [8] while some are operated by sending explicit alerts through mobile phones [9]. These devices offer different types of features to help support the cause that is mainly related to sending alert to the guardian of the women under threat. Reference [10] proposed a device with fingerprint sensor and shock generator along with facility of voice recording. Then the global positing system (GPS) and global system for mobile communication (GSM) are used to trace the location and send message of danger to the guardian of the woman. Another study [11] presented a device that is used to protect women by tracking the exact location and send alert or the message of danger to the guardian of the woman.

The advancements in IoT-based devices for women's safety are observed as they become wireless and embedded in wearables of women. IoT-based wearable devices are interconnected with different sensors. These devices are small and wireless. The wearable devices have to be worn on human body in different forms like gadgets, cloths, accessories, and even as smart tattoos. The devices are associated with the sensors that are used to take the readings from the particular device and activates the modules. The choices of sensors are conducted on the validation of methods related to the targeted device [12].

In the domain of women's safety, the wearable devices are incorporated in smart gadgets, smart foot device and even smart jacket. All of these devices have built-in sensors depending on the targeted device. Like the smart foot device is inaugurated with only accelerometer or acceleration sensor [13].

The IoT-based devices for women's safety also use several sensors to sense the state and movement of women in order to detect any safety threats. Such sensors gather data from different parts of the body. This includes the acceleration sensor [14], pulse-rate sensor [15], heartbeat sensor [16] and temperature sensor [17]. Some of the sensors are body-area specific such as heartbeat and pulse-rate sensors while some could work by taking input from any part of the body such as temperature and tilt sensors. Although some sensors can relate to specific body areas whilst there are sensors which could generally be related to movement of any body part such as tilt sensor [18], and flex sensors [19].

Applying the machine learning algorithms on the input data captured through these sensors would result in making decisions reflecting whether the particular state of women could be considered as unsafe or not. Hence, various machine learning algorithms are applied in IoT devices for women's safety to decide the state of the women [20], [21]. In addition, different technology like GPS, GSM, and Raspberry Pi [19], [20], [21], [22] is applied to transmit alerts to the guardian. Although a number of these devices are in place yet their working and effectiveness need to be explored in order to identify areas for further improvements and determine the directions for future research in the specified field of study.

A number of research articles have been published by the researchers to throw light and due attention on the underlying issues. It has been observed that with the development of the world, instead of decreasing, women's unsafety issues are increasing. This reflect the gap of any comprehensive studies that could guide the future research direction to optimize the efforts of community and make better solutions as the phenomenon is highly affecting the economies and societies considering the significant role of in the development and growth of any economy or society.

The prime focus of this literature review is to highlight the flaws of apps and devices introduced to date. Many studies have been published in this field and gaining importance due to women's independence and courage to go out from home for work purposes. Hence, a comprehensive investigation is important to recognize and summarize the current research developments in the field. This SLR (Systematic Literature Review) proposes a taxonomy for IoT-based women's safety devices, reflects gaps in various apps and devices, proposes an architecture for women safety system based on the gaps and challenges identified in existing devices including the solutions used for the betterment of security systems.

Further sections of this paper are categorized as: Section II identifies the related work and section III has been designated for the research methodology adopted in this review, elaborates research objectives, the research questions and motivations, search strategy, selection procedure to obtain relevant articles, abstract based keywording to classify the articles and quality assessment criteria. Analysis and results representation has been presented in section IV, taxonomy along with open issues and challenges have been discussed for help in future aspect.

II. RELATED WORK

Few studies identified the IoT-based devices for women's safety, to the best of our knowledge. A research presented survey on women's safety using IoT [6]. The scope of this survey was mainly focused on mechanisms used for detecting human body sensors as well as highlighted the limitations of previous studies. Another study [22] presented a survey and comparison of existing works discussing the guardian device for the protection of women. The researcher developed a novel guardian device to receive alerts. The device is designed to work with the sensors and women in danger require to trigger the button for sending alert to guardian. Though the device depicts an effective solution for potential victims, yet a shortcoming is observed, as the victim has to operate the device for its activation where the people in danger are generally immobilized due to which some specific actions from them could not be taken.

Reference [23] presented a literature review on recent and emerging technologies used for the safety and protection of the women. The researchers gathered and conducted online searches on women's safety devices showing new as well as emerging technologies. However, this study has utilized the IoT-based technologies efficiently by proposing an IoT-based women's safety architectural model. The study in [5] conducted a systematic literature review on evolution of women's safety devices using IoT by reviewing a few sensors and dominating features used in existing IoT-based women's safety devices. However, the taxonomy proposed in this review highlights a number sensors and dominating features of IoT-based women's safety devices. Whereas, the researchers in [24] presented a Woman Safety System (WSS) that is designed especially for the protection of women and send message for the situation of danger. The WSS device is designed in a smart jacket that is not wearable everywhere and anytime. However, the model presented in this study is designed to be adjusted in various number of wearables that can be used in any situation.

Reference [25] showed the comparison of IoT-based mobile applications and IoT-based hardware gadgets and found that IoT-based smart hardware gadgets are more helpful and effective in protecting a woman in danger. This study is more focused on comparative analysis of IoT-based mobile application and IoT-based hardware gadgets while our work synthesizes the state-of-the-art IoT-based smart devices with detailed analysis of the sensors, wearables, as well as advanced machine learning algorithms used in IoT-based systems for women's safety.

The above discussion showed that our review differentiates itself from the existing reviews by concentrating on the publication channels related to IoT-based women's safety devices, deeply exploring the technologies and identifying the gaps and challenges faced by women of modern era. Furthermore, we followed a more balanced and comprehensive approach than the existing reviews as we selected techniques, technologies and sensors in a systematic way, and utilized them in presenting the state-of-the-art enhancements in women's safety devices based on IoT. In addition to this, we suggest a taxonomy for IoT-based women's safety devices based on the gaps and challenges identified in existing devices and propose an architecture for women safety system that could work on multiple sensors and machine learning algorithms having the potential of providing more accurate results of attack on women.

III. RESEARCH METHODOLOGY

The Systematic literature review (SLR) has been carried out to conduct this review as it provides organized approaches to search, classify and synthesize the literature based on pre-defined objectives leading to highlight the areas that could guide the future research dimensions in the specified domain [26]. The research methodology of this review is sketched in Figure 1 depicting three stages.

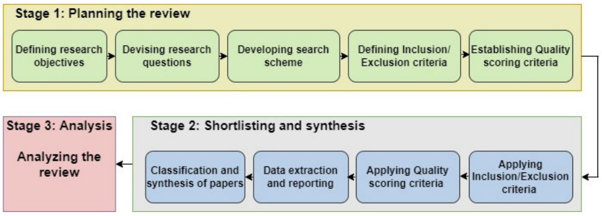

Stage 1: Planning the review
Defining research objectives
Devising research questions
Developing search scheme
Defining Inclusion/ Exclusion criteria
Establishing Quality scoring criteria
Stage 3: Analysis
Analyzing the review
Stage 2: Shortlisting and synthesis
Classification and synthesis of papers
Data extraction and reporting
Applying Quality scoring criteria
Applying Inclusion/Exclusion criteria

FIGURE 1. **Research methodology.**

Initially the review is planned by defining the research objectives based on which the research questions are elaborated. After this, the search scheme to identify the suitable literature is established. This was followed by devising the inclusion/exclusion and quality scoring criteria.

The shortlisting of the studies was then carried out by applying the inclusion/exclusion criteria. This was followed by ranking the studies on the basis of the quality scoring criteria. Then, the classification and synthesis of the shortlisted studies according to the investigating areas of this study has been conducted. Lastly, the discussion and analysis on the results were made.

A. RESEARCH OBJECTIVES (ROs)

The fundamental objective of this study is to ascertain the IoT-based devices for women's safety in order to identify the areas that could lead to guide the future efforts in the specified domain. In this context, more specific objectives of conducting this SLR includes:

RO1: To explore the state-of-the-art technologies used in IoT-based women's safety devices.

RO2: To evaluate the use of different sensors and major features the IoT-based women's safety devices exhibit.

RO3: To examine the impacts and effectiveness of decision-making algorithms used in women's safety devices.

RO4: To identify the wearables used for women's safety and the sensors these wearables used.

B. RESEARCH QUESTIONS (RQs)

The research questions to investigate the underlying domain along with the respective motivations are listed in Table 1.

TABLE 1. Research questions with respect to motivations.

	Research Question	Major Motivation
RQ1	What technologies are used in IoT-based women's safety systems?	To understand various mechanisms involved in the field
RQ2	What are the prominent features and sensors used in used in IoT-based women's safety systems?	To examine the dominating features and sensors used in IoT-based women's safety devices
RQ3	Which machine learning algorithms are used to identify the women's safety threats?	To understand the applicability of various machine learning algorithms in identifying the safety threat.
RQ4	Which IoT-based wearables are used for women's safety?	To identify various IoT-based wearables used for women's safety

C. SEARCH SCHEME

The most important step of conducting an SLR is the preparation of a search plan to collect relevant and authentic research on the particular area. This step entails identifying resources to search the relevant literature, developing search string, and establishing the inclusion/ exclusion criteria. The articles selected for this literature review are searched and collected from well-reputed digital repositories such as IEEE, Springer Link, Elsevier, Research Gate, ACM digital library and Academia. We have also considered google scholar to search the articles that have overlooked from the previous search cycles. The journals related to the field and those, which are most prominent, have been searched using a number of keywords categorized as primary, secondary, and tertiary. The keywords used to devise the search string are listed in Table 2.

TABLE 2. Keywords used for searching.

Primary keywords	Secondary Keywords	Tertiary Keywords
• IoT-based • IoT • Internet of Things	• Women's safety • Smart women's safety • Women's security • Women's safety devices	• Violence • Harassment • Molestation • Threat • Rape

The search string, to search the relevant records, is shown as listing 1, which is formed by combining the types of keywords as well as the Boolean operators. Mapping the search string with specific primary, secondary and tertiary keywords resulted in formulating the general form of string shown as listing 2. Table 3 lists the search string applied to specific digital repositories.

∀ Primary keyword ∧ ∀ Secondary keyword ∧ Tertiary keyword

LISTING 1. Combination of types of keywords and Boolean operators in search string.

∀(IoT-based V IoT V Internet of things) ∧ ∀(smart women's safety v Women's safety V Women's security V Women's safety devices) ∧ (Violence V Harassment V Rape V Threat V Molestation)

LISTING 2. General search string for repositories.

TABLE 3. Specific search strings with respect to digital repositories.

Repository	*Search Strings*
IEEE XPLORE	***("IOT-BASED" OR "IOT" OR "INTERNET OF THINGS") AND ("WOMEN'S SAFETY" OR "SMART WOMEN'S SAFETY" OR "WOMEN'S SECURITY" OR "WOMEN'S SAFETY DEVICES") AND ("VIOLENCE" OR "HARASSMENT" OR "MOLESTATION" OR "RAPE" OR "THREAT")***
Springer Link	***'("IOT-BASED" OR "IOT" OR "INTERNET OF THINGS") AND ("WOMEN'S SAFETY" OR "SMART WOMEN'S SAFETY" OR "WOMEN'S SECURITY" OR "WOMEN'S SAFETY DEVICES") AND ("VIOLENCE" OR "HARASSMENT" OR "MOLESTATION" OR "RAPE" OR "THREAT")'***
ACM Digital Library	***[[ALL: " IOT- BASED "] OR [ALL: " IOT "] OR [ALL: " INTERNET OF THINGS "]] AND [[ALL: " WOMEN'S SAFETY "] OR [ALL: " WOMEN'S SAFETY DEVICES "] OR [ALL: " WOMEN'S SECURITY"] OR [ALL: " SMART WOMEN'S SECURITY"]] AND [[ALL: "VIOLENCE"] OR [ALL: " HARASSMENT "] OR [ALL: " MOLESTATION "] OR [ALL: " RAPE"]OR[ALL: "THREAT"]]***
Elsevier	***(("IOT-BASED"OR "IOT") AND (WOMEN'S SAFETY OR WOMEN'S SAFETY DEVICES OR WOMEN'S SECURITY OR SMART WOMEN'S SAFETY) AND (THREAT OR MOLESTATION OR RAPE OR HARASSMENT OR VIOLENCE))***
Science Direct	***(("IOT-BASED"OR "IOT" OR "INTERNET OF THINGS") AND ("WOMEN'S SAFETY" OR "SMART WOMEN'S SAFETY"OR "WOMEN'S SECURITY"OR "WOMEN'S SAFETY DEVICES") AND ("VIOLENCE" OR " HARASSMENT " OR " MOLESTATION" OR "RAPE"OR "THREAT"))***

D. INCLUSION/EXCLUSION CRITERIA

Inclusion criteria (IC) and exclusion criteria (EC) were carefully devised to shortlist the relevant literature from the papers identified by applying the search string to the digital repositories. Following criteria were devised to include the studies.

- **IC-1:** Study is primarily conducted for security of women.
- **IC-2:**Study is targeting the IoT-based devices for women's security.

The studies are excluded on the basis of the following exclusion criteria.

- **EC-1:** Study is focused holistically on applications of IoT.
- **EC-2:** Study is not written in English Language.
- **EC-3:** Study is published before 2016.

E. STAGE-WISE SHORTLISTING

Applying the search string to digital repositories resulted in acquisition of a large volume of data, which was required to be shortlisted by going through multi-stage shortlisting process, Figure 2 shows the stage-wise shortlisting of studies along with the number of papers included and excluded at each stage. This process is started through an initial search and scrutiny of papers from the databases. Then, the papers were shortlisted by excluding the duplicate records. After this, the shortlisted paper obtained till that stage were further examined by reading the titles and abstracts. The exclusion of papers was further made by reading the introductions and conclusions. The shortlisting at various stages was made by applying the IC/EC criteria. This process resulted in identification of 34 articles to carry out the review process.

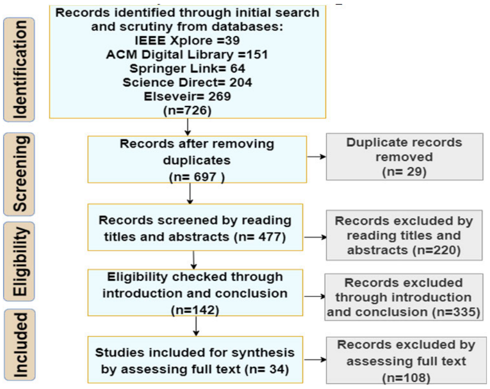

Identification
Screening
Eligibility
Included
Records identified through initial search and scrutiny from databases:
IEEE Xplore =39
ACM Digital Library =151
Springer Link= 64
Science Direct= 204
Elseveir= 269
(n=726)
Records after removing duplicates (n= 697)
Duplicate records removed (n= 29)
Records screened by reading titles and abstracts (n= 477)
Records excluded by reading titles and abstracts (n=220)
Eligibility checked through introduction and conclusion (n=142)
Records excluded through introduction and conclusion (n=335)
Studies included for synthesis by assessing full text (n= 34)
Records excluded by assessing full text (n=108)

FIGURE 2. Stage-wise shortlisting of studies.

F. QUALITY SCORING

Quality assessment is one of the important steps of SLRs to appraise the quality of included studies. The shortlisted studies have been scored for quality based on the criteria presented in Table 4.

TABLE 4. Quality scoring criteria.

Criteria	Description	Rank	Score
	Internal scoring		
a)	Did the abstract clearly define the technology and method of the device?	Yes Partially No	1 0.5 0
b)	Did the study show comparison of the particular system with previously designed devices?	Yes Partially No	1 0.5 0
c)	Was methodology clearly defined?	Yes Partially No	1 0.5 0
d)	Was the conclusion based on results?	Yes Partially No	1 0.5 0
	External scoring		
e)	What is the ranking of the publication source ?	Q1 Q2 Q3 Core A Core B Core C	2 1.5 0.5 1 1.5 0.5

G. RESULTS AND FINDINGS

This section explains the results obtained and the main findings after performing classification and synthesis of thirty-four articles selected for review. The classification of studies on different investigating aspects and quality scoring are shown in Table 5. The studies are classified according to the investigating areas of this work where the respective study for a particular investigating area is marked as None in case a required information is not clearly provided in a study.

The data extraction and synthesis of the selected articles are performed according to the investigating areas of this work. The years for selecting the papers for this review ranged from 2016 to 2022. Figure 3 shows the distributions of IoT-based women's safety devices over the specified range of years. The synthesis on years of publications of selected studies depicts an increasing trend of publications in the underlying domain from the year 2019 where most of these publications are made in years 2021 and 2022. Out of the 34 papers selected for review, 50% (17) are presented in conferences while 50% (17) of these papers are published in journals. The journal publications are more in the years 2019, 2020, and 2021 than conference papers unlike the years 2016, 2017, 2018 and 2022, which show more conference papers. The years 2016 and 2017 are outliers exhibiting no journal article in the pool of selected studies for this review.

The validation has been carried out in 59% (20) of the selected studies while 41% (14) of these studies are not validated, which has generally made through real time processing of the particular devices specifically based on machine learning algorithms. Real time sensors readings are fed to the devices for training and then tested by creating real time harassment and molestation scenarios.

The quality assessment results according to different scoring classes such as above average, below average, and average are presented in Figure 4.

Table 6 enlists the studies according to the total quality scores the studies obtained. It shows that 24% studies are below average, 41% studies have an average score and 35% of papers have above average scoring.

The studies are scored based on investigating areas of this work and the comparison with already conducted research. The papers clearly demonstrated the investigating areas of this work are ranked higher than others. The studies provided no or lesser details of sensors, dominating features, wearables and machine learning algorithms obtained the lesser aggregate score. The facts gained after synthesizing the selected studies were discussed with respect to the research questions.

TABLE 5. Classification of shortlisted studies.

Ref No.	Publication		Classification					Empirical Validation	Internal Scoring				External Scoring	Total Score
	Channel	**Year**	**Machine learning algorithm**	**Technology**	**Sensors**	**Dominating Features**	**Wearable**		**1**	**2**	**3**	**4**	**5**	
[4]	Journal	2020	None	Bluetooth, GPS	Pulse-rate sensor	Location tracking	None	Validated	1	1	1	1	0.5	4.5
[5]	Journal	2020	None	None	None	None	None	Not validated	0.5	0.5	0	0.5	0	1.5
[6]	Journal	2018	None	None	None	None	None	Not validated	0.5	0.5	0	0.5	0	1.5
[8]	Journal	2021	None	GPS, GSM, Bluetooth	Vibration sensor	Location, shock wave generator	Smart band	Not validated	1	1	1	1	0	4
[9]	Conference	2018	None	Raspberry Pi	None	Image capture, location tracking	Smart ring	Not validated	1	0.5	0.5	1	0	3
[10]	Journal	2019	None	GSM, GPS	Fingerprint sensor	Shock wave, audio record, location tracking	None	Validated	1	0.5	1	1	1.5	4.5
[11]	Journal	2019	None	GPS, GSM	Vibration sensor	Location tracking, shock generator	Smart band	Validated	1	1	1	0.5	0.5	4
	Channel	**Year**	**Machine learning algorithm**	**Technology**	**Sensors**	**Dominating Features**	**Wearable**		**1**	**2**	**3**	**4**	**5**	
[13]	Conference	2016	Decision Tree	Bluetooth	Acceleration sensor	Location tracking	Smart shoe	Validated	1	0.5	1	1	0	3.5
[14]	Journal	2020	None	GPS, GSM	Acceleration sensor	Location tracking	None	Validated	0.5	0	0.5	0.5	0.5	2
[15]	Conference	2019	None	GPS, GSM, Raspberry Pi	Pulse-rate sensor	Location tracking	Smart band	Not validated	1	0.5	0.5	0	0	2
[16]	Journal	2021	Logistic regression	Raspberry pi	Heartbeat and temperature sensors	Location tracking	Smart band	Validated	1	1	1	1	0.5	4.5
[17]	Conference	2018	Logistic regression	GPS, GSM	Temperature, pulse-rate, heartbeat sensors	Location tracking, alarm	None	Validated	1	1	0.5	1	0	3.5
[18]	Journal	2018	None	GPS, Raspberry Pi	Tilt, heartbeat, vibration, flex sensors	Location tracking	None	Not validated	0	1	0.5	0	0.5	2
[19]	Conference	2021	None	Raspberry pi, GPS, GSM	Flex sensor	Location tracking	Inner wear	Validated	0.5	1	1	1	0	3.5
[20]	Conference	2018	Hidden Markov Model	GPS, GSM	Pressure, pulse-rate, temperature sensors	Location tracking	None	Validated	1	1	1	1	0	4
[21]	Journal	2022	Logistic regression	GPS, Bluetooth	Pulse-rate, tilt sensors	Location tracking	Smart band	Validated	1	0.5	0.5	1	0.5	3.5
[22]	Conference	2021	None	GPS, GSM	Vibration, pulse-rate sensors	Location tracking, Image capture, alarm	None	Not validated	0.5	0	0	1	0.5	2
[23]	Journal	2019	None	None	None	None	None	Not validated	0.5	0.5	0.5	1	2	4.5
[24]	Journal	2021	None	GPS, GSM	Temperature, heartbeat and vibration sensors	Audio record, location tracking	Smart jacket	Not validated	0	0.5	0.5	0	0.5	1.5
[27]	Conference	2020	Outlier detection	GPS, GSM	Pressure, temperature, pulse-rate sensor	Location tracking	None	Validated	1	1	1	1	0	4
[28]	Conference	2017	Decision tree	GPS	Breathing, heartbeat	Location tracking	Smart band	Not validated	1	1	1	1	0	4
[29]	Journal	2021	Logistic regression	Raspberry pi	Pulse-rate, temperature sensors	Location tracking	Smart band	Validated	1	1	1	1	0	4
[30]	Conference	2022	None	GPS	Pressure sensor	Live video, shock wave generator, location tracking	None	Validated	1	1	1	0	0	3

TABLE 5. *(Continued.)* Classification of shortlisted studies.

[31]	Conference	2016	None	GPS, GSM	Motion, temperature , pulse-rate sensors	Location tracking	Smart band	Validated	1	1	1	0	0	3
[32]	Conference	2021	None	GPS, GSM	None	Location tracking	Smart band	Not validated	1	0.5	0.5	0.5	0	2.5
[33]	Conference	2021	None	Raspberry pi, GPS	Flex sensor	Location tracking	Smart jacket	Validated	1	0.5	1	1	1.5	5
[34]	Journal	2019	Logistic Regression	GPS	Pulse-rate, temperature , motion, vibration sensors	Location tracking	Smart band	Validated	0	0.5	0.5	0.5	0.5	2
[35]	Conference	2019	None	GPS, GSM	None	Location tracking, shock wave generator	None	Validated	1	1	0.5	1	0	3.5
	Channel	**Year**	**Machine learning algorithm**	**Technology**	**Sensors**	**Dominating Features**	**Wearable**		**1**	**2**	**3**	**4**	**5**	
[36]	Conference	2022	None	GPS, GSM	None	Location tracking	None	Validated	1	0.5	0.5	0.5	0	2.5
[37]	Conference	2021	None	GPS, GSM	Vibration sensor	Location tracking	Smart band	Not validated	1	0.5	0.5	0.5	0	2.5
[38]	Journal	2020	None	GPS, Raspberry Pi, GSM	None	Location tracking	None	Not validated	1	1	0.5	0.5	0.5	3.5
[39]	Journal	2021	Hidden Markov Model	GPS	None	Location tracking	Smart band	Not validated	0.5	0.5	0.5	0.5	0.5	2.5
[40]	Journal	2020	Logistic regression	GPS, GSM	Pressure sensor	Location tracking	Smart garb	Validated	0.5	1	1	0.5	0	4
[41]	Conference	2020	None	Raspberry Pi, GPS, GSM	None	Image capturing, location tracking	None	Validated	1	0.5	0.5	1	0	3

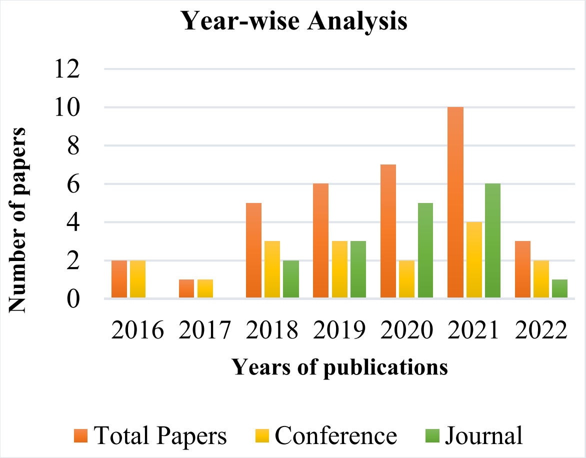


FIGURE 3. Distribution of selected studies over the years.

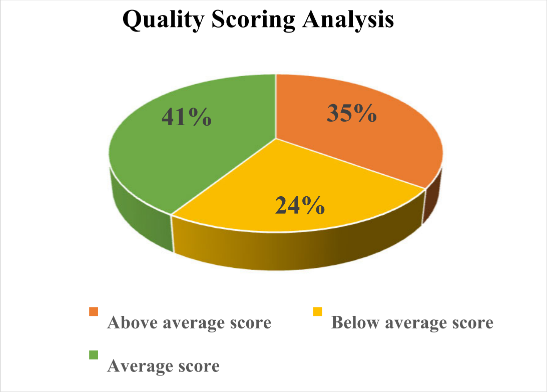


FIGURE 4. Quality scoring classification analysis.

TABLE 6. Quality assessment of selected papers.

References	Score	Total
[33]	5	1
[4] [16] [10] [23]	4.5	4
[27] [8] [20] [28] [29] [11] [40]	4	7
[19] [17] [20] [35] [38]	3.5	5
[9] [30] [31] [41]	3	5
[32] [36] [37] [39]	2.5	4
[15] [18] [14] [22] [34]	2	5
[5] [6] [24]	1.5	3

All the questions are answered concisely to clarify the respective investigating areas of the selected domain.

1) ASSESSMENT OF QUESTION 1- WHAT TECHNOLOGIES ARE USED IN IOT-BASED WOMEN'S SAFETY DEVICES?

IoT-based women's safety devices use technologies that activate various features and play important role in sending the danger alert to the guardian of the woman under threat. Some of the main technologies used in women's safety devices are GPS (Global Positioning System), GSM (Global System for Mobile Communication) and Raspberry Pi. GPS is used to track and locate the location of the victim whereas GSM is used to send the alert of danger to the guardian. Raspberry pi is a small computer chip-based technology used in IoT-based devices, which has further extensions such as Raspberry pi zero and Raspberry pi 3. Like GPS and GSM, Raspberry pi is also used to activate dominating features in women's safety devices. Bluetooth is another technology used in IoT-based women's safety devices to detect other nearby devices.

GPS and GSM are most common technologies used for tracking and communication systems. Considering the women's safety systems, GPS and GSM play crucial role. Bluetooth is used least in women safety devices because of the reason that the Bluetooth detects the nearby devices only; so, in case of kidnapping, the kidnapper could be out of reach shortly after incident occurs. Hence, considering the Bluetooth offers limited range, it fails to work in kidnapping and snatching cases. Figure 5 shows the percentages of main technologies used in IoT-based devices for women's safety..

Technologies become the main driver in the implication of IoT applications. These technologies are used to monitor, control and track the underlying phenomenon. IoT technologies make the system durable, and exhibit low energy consumption and a wide range of coverage. With the modernization of society, the common public streets, offices and various places have become the dominion of harassers. To account for this Sogi in [9] developed a device that is comprised of Raspberry Pi Zero and Raspberry Pi Camera, the device is implemented in the form of the smart ring which is connected to the mobile phone of the victim and works by pressing the button.

As we have discussed earlier, the woman is in danger have no sense to press the button consciously. The device should work automatically to avoid human interaction. The technologies used in [20] are GPS and GSM modules. The GPS module is used to track or send the live location of the victim to the particular contact whereas the GSM is used to send the SMS or MMS to the guardian. GPS and GSM modules play a vital role in IoT-based safety devices. In this particular device the GPS and GSM modules are designed to send the warning to the guardian just in case of aftershock.

Jesudossas in [18] proposed a device comprised of technologies using GPS to track the live location of the victim and Raspberry Pi. The raspberry pi and GPS module are connected to the Arduino. The limitation of this study is that the Arduino is a microcontroller, hence the device is hardware based whereas, an automatic emergency alert system is required for the safety of women. The current version of Arduino Uno comes with USB interface, 6 analog input pins, 14 I/O digital ports that are used to connect with external electronic circuits. Out of 14 I/O ports, 6 pins can be used for PWM output [42].

In [35] the author proposed a device using IoT-based technologies of GPS and GSM modules to track the location and send the message but the device is designed in such a way that the victim has to trigger the button to activate it. After triggering the device takes three seconds for the first buzzer. The user has to again trigger the button to activate the device, it takes 10 seconds again for the second buzzer. The device is based on human interaction which takes some time for activation. During the time of the attack, no one can control the device. On the change of location, the victim has to again repeat the process for the activation of the device. The device should be designed in a way to activate automatically.

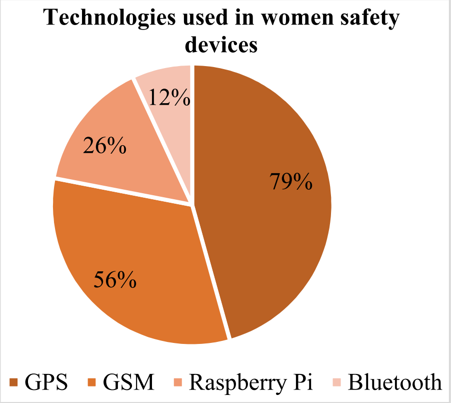


FIGURE 5. Technologies used in IoT-based women's safety devices.

Gulati in [4] designed an intellectual device using GPS, GSM and Bluetooth modules. The author has also elaborated the estimated cost of the device which seems to be high for lower class woman. Every woman should be protected either she is poor or rich. Another study uses Raspberry Pi 3 along with the GPS and GSM modules technologies. Raspberry pi 3 is used to connect automatically to the internet on the activation of the device. The device is designed to send the URL location to the guardian of the victim [41]. But the drawback of the device is that it would not be able to work at places where there is no internet. The model proposed in this paper can work even without an internet connection.

Kumar in [40] designed a device which works automatically with machine learning algorithm. It is comprised of a GSM module which makes the device expensive. The proposed device is similar to [40] but it is made cheap to be reached by every woman of society. To avoid physical human interaction Agrima in [8] proposed a device that activates by voice recognition. If the voice is recognized by the device, using GSM it automatically alerts the guardian and police station of the victim about the location via GPS. In case if the voice does not match with the features fed to the device the victim will fail to inform the guardian.

In [11] Sathyasri designed a smart band consisting of GPS and GSM. The victim has to press the trigger to activate the modules that are attached to the microcontroller. The device should be automatically operated without human interaction. In [24] a women's security system covering all the flaws of previously designed devices is comprised of GPS and GSM modules to track the location and inform the guardian. It has a built-in hidden camera and audio recorder to help police for investigating. But the device activates the buzzer on activation, which will alert the attacker and he would snatch the device. The device should be designed in such a way that no one gets to know about the device.

IoT-based evidence collecting and women protection device designed in [19] designed a device which uses GPS, GSM and Raspberry Pi. The device is wearable with the clothes of the woman. The woman has to press the button for activation. There is a probability that the woman could not get a chance to trigger the button for activation. A gadget designed for the security of woman in danger in [36] has technologies of GPS, GSM that sends a customized message for help during an alarming situation. Like many other devices designed with human interaction. This model also has the drawback of human interaction. It works by pressing the button.

A women's safety jacket in [33] is designed by using Raspberry Pi and GPS module to track the location of the woman. The woman can wear the jacket anywhere but there is sometimes weather when wearing the jacket is not possible. The system proposed in [29] uses GPS, Raspberry pi and a camera. The device works automatically using a machine learning algorithm by taking the values from attached sensors. The limitation of the particular device is that it cannot work without connectivity of the internet. In case of kidnapping, the kidnapper would take the victim to a place where there is no internet connection.

Like many other devices, the Guardian device proposed in [22] uses GPS, GSM and IoT modules and activates on pressing the button by the victim. The proposed system is free of human interaction. A BEACON device introduced in [21] is designed using the GPS and GSM module with the facility of Bluetooth. The device takes the reading from the postures of the victim and predicts whether the woman is in danger or not based by evaluating her posture.

Machine learning and Raspberry techniques utilize the sensors. These IoT-based technologies are used to minimize the difficulties, labor and time. But the devices associated with the above discussed technologies requires full time internet connection and becomes expensive with the use of wide range of technologies. Therefore, a simple and efficient system should be designed to develop communication between the women and guardians.

2) ASSESSMENT OF QUESTION 2- WHAT ARE THE PROMINENT FEATURES AND SENSORS USED IN IOT-BASED WOMEN'S SAFETY SYSTEMS?

Whenever a woman feels danger around herself, the devices must be capable of automatically sensing the danger by identifying specific state of the woman under threat. The specific state of the woman reflecting her under threat can be identified through various factors such as a fast heartbeat, body shivering, and sweating. Different devices offer different features to further process for alert generation on identifying a woman under threat. The sensors that are used to activate these features and their respective operations are listed in Table 7.

TABLE 7. Sensors involved in women's safety devices.

Sensors	Operations
Acceleration sensor	For women safety it additionally detects the presence or lack of motion and if the acceleration on any axis exceeds a user-set level, then the system is activated [14].
Temperature sensor	it is important to monitor the human body temperature constantly. For women safety purpose temperature sensors like LM35 series are used [32].
Pulse-rate sensor	it is a small chip that monitors pulse-rate. Normal pulse-rate is 80 to 90, in case of increase in this value then it activates the system [15].
Heartbeat sensor	To monitor the safety of women heartbeat is taken for every 20 milliseconds. [18]
Flex sensor	Flex sensor is a compact device that is used as a sticker with the cloths. It calculates the pressurized movement of women hand [19]
Tilt sensor	Tilt sensors are used to find orientation of body. For women safety the orientation of body is calculated every 20 milliseconds [18]
Vibration sensor	It measures the frequency of the wearable device.

Main features involved in women's safety devices are presented in Figure 6. A model designed by [24] is a jacket that tracks the location from time to time through GPS. The jacket comprises of temperature sensor along with a buzzer and electric shock generator as a protection tool in it for self-defense. The limitation of this study is that it activates the buzzer sound which would alert the attacker about the device. Similarly, [14] designed a device that consists of a panic button with GPS tracking system and GSM module. In this system, the location is tracked frequently by the IoT module. Also, the accelerometer is used to activate the buzzer that is used as an alarm if the women fall down. This jacket-based device can be carried anywhere, but it cannot be worn every time.

A smart ring [9] designed for the protection of women consists of a buzzer with a button for activation. After activation, it sends the current location through GPS and captures the image of the attacker through the Raspberry Pi camera to the emergency contacts. It has the facility of an electric shock generator that gives an electric shock to the attacker. It has the same drawback of human interaction, as seen in many other devices. A low-cost smart footwear device [13] that is activated with the tapping of one foot in front of the other three times. This activates the GPS and GSM. It has been analyzed by a decision tree classifier. The values are fed to the decision tree classifier from the motion sensor of the woman. A smart band or watch [15] with a button on it can collect information like location, body posture and pulse-rate and send it to the predefined number by using GSM via Raspberry Pi. The readings are collected from the pulse-rate sensor but the drawback is that the pulse-rate can change due to any reasons.

Another smart device [27] for the safety of women is automated to collect the pulse-rate and pressure by using outlier detection. The device does not need physical interaction with humans and sends messages with location to relatives. The blood pressure of the woman could change even due to health issues.

Similarly, a smart wearable band [29] designed by researchers for women tracks the location and sends the alert to the police station message using Wi-Fi module designed in raspberry pi 3. A machine learning algorithm "Logistic Regression" has been used to monitor the pulse-rate and temperature continuously. The algorithm should be trained by the real-time values of attack on women because the pulse-rate and temperature can change due to health issues.

Sunehra in [41] proposed a smart wearable device that sends email through GSM/ GPRS (General Radio Packet Service) technology by locating the user through GPS. It also captures the image via a USB Camera. For the activation of the device, the user has to press the panic button attached to the smart wearable device, the system discussed has no sensor attached to it which makes the device manual. However, the device should be automated that collect the readings from IoT-based sensors as proposed in this study.

An advanced smart protection system [30] that cannot just collect information and track location but also send a live video. It also activates the buzzer that makes loud noises to alert near ones. It has a shock module as a self-defense system. Many of the devices are designed by using combination of sensors. III-G3 shows the percentages of various sensors used in IoT-based devices for women's safety. Most of the devices are designed using pulse-rate and temperature sensors. Sensors are used to activate the tracking and communication modules to get the dominating features of the device. The main feature used in women's safety devices is location tracking.

By considering the flaws of several devices Sumanth Paglada in [16] proposed a device that uses technologies like IoT and Machine Learning. The device is trained to collect the values of heartbeat and pulse-rate of women in danger through Logistic Regression. The heartbeat can change even due to fast walking or moving into the rush area.

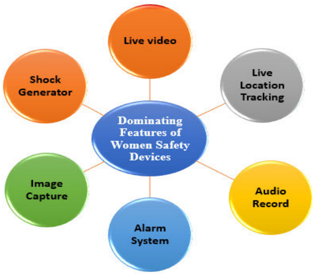


FIGURE 6. **Dominating features of women's safety devices.**

Akram in [10] designed an IoT-based smart device that has a fingerprint facility. The victim has to activate the device by fingerprint method. Also, it has a shock wave generator that works as a self-defensive system for women. It has additional features like audio recording and sending group messages. The device is activated through a fingerprint that is not sufficient at the time of attack.

A smart device [19] that is secretly kept by the women to collect pieces of evidence of harassment or molestation. It consists of a camera and flex sensor along with GPS and GSM module. The device is small in size kept with undergarments easily. As discussed above there is the chance that the woman could not get time to trigger the device.

To avoid human interaction a smart device is designed in [40] that is fully automated and needs zero per cent of human interaction in case of danger. It automatically collects the data through machine learning algorithm. As the system has to undergo many prediction sets for applying machine learning algorithms. So, once the device gets the correct prediction set it can easily alert the relatives and nearby police station in case of danger. But the device is designed to collect the values from the pressure sensor of the body, which could result in the wrong prediction because the pressure can change due to many reasons.

Similarly, [18] uses the heartbeat, flex, tilt and vibration sensors that has also the facility of capturing the images of attack. The tilt sensor collects the values of inclination.. The device is automated but using multiple sensors makes the device costly. Reference [8] is designed with several dominating IoT-based features like image capturing, location tracking and shock generator. But the device has no sensors attached to it. It is a self-defense device that is activated by the voice recognition of the victim. So, the devices have IoT-based dominating features: Live video recording, live location, audio recording, image capturing, alarm system, and shock generator

Sensors provide portability, durability, reliability and power consumption. All sensors and dominating features play vital role in women safety devices. But each feature needs special assistance which might be difficult in some situations. Like some of the features are associated with the connectivity of internet only and some sensors requires human interaction for activation. Hence, the devices should be designed in a way that they could work in any unrealistic and emergency situation quickly. Temperature, heartbeat and pulse-rate sensors are commonly used in women safety domain.

3) ASSESSMENT OF QUESTION 3- WHICH MACHINE LEARNING ALGORITHMS ARE USED TO IDENTIFY THE WOMEN'S SAFETY THREATS?

The machine learning algorithms used in IoT devices are customized to learn the individual pattern of women's state of body, e.g., heartbeat patterns and changing patterns of body temperature. Firstly, the devices are trained with the normal heartbeat and temperature readings and then the devices are trained. Incase readings are higher than the normal readings, a signal of danger might be generated. Also, some of the devices encounter internet problem, which can be avoided through ZigBee Mesh network. The ZigBee Mesh network is useful when it needs to send data to multiple hop distance [17].

TABLE 8. Percentages of sensors and features used in literature.

Sensors							Dominating Features						
Pressure sensor	Pulse rate sensor	Heartbeat sensor	Tilt sensor	Temperature sensor	Flex sensor	Acceleration sensor	Vibration sensor	Image capture	Location tracking	Live audio	Live video	alarm	Shock wave
9%	29%	15%	6%	24%	6%	6%	21%	9%	91%	6%	3%	6%	15%

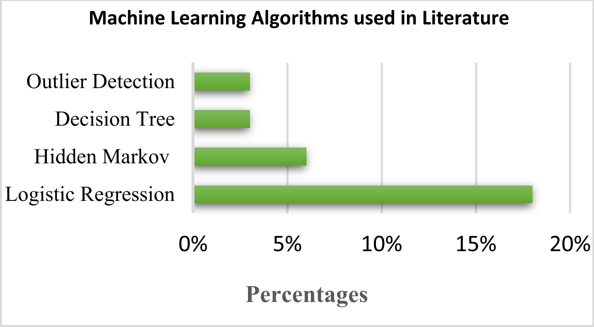


FIGURE 7. Percentages of machine learning algorithms used in literature.

Figure 7 presents the percentages of machine learning algorithms used in literature.

Machine learning algorithms used to train the devices for their betterment and advancement are discussed further:

a: LOGISTIC REGRESSION

Logistic regression is a classification problem that is used to classify binary and linear problems simply and efficiently [42]. Logistic regression is used in women's safety devices to predict danger. The danger indicator has values of yes (when there is danger) or No (when there is no danger). Pulse-rate and body temperature are used as independent variables, the predictions range from $-\infty$ to $+\infty$ but probabilities lie between 0 and 1. Hence log is applied to the dependent variable which then expressed the linear function of independent variables [17].

A smart wristband is designed in [34]. It collects the values from sensors and predicts whether the woman is in danger or not through the logistic regression model. A large amount of training and test dataset is fed into the logistic regression model for the prediction. During analysis, the sensors are continuously tested and monitored. The drawback considered in this is that the values should be real time based otherwise the prediction can be wrong.

Samantha developed a novel device in [16] which works on the logistic regression model. It detects the heartbeat rate and temperature of the woman by analyzing the readings on the online portal. If the values match the prediction of a woman in danger then the device automatically informs the guardian. But the device uses online portal for accurate prediction, which is not useful in places where internet connection is disabled.

b: HIDDEN MARKOV MODEL

Hidden Markov Model provides better prediction and provides immense sensing on suspicious activities. Regarding women's safety, it provides analysis of face recognition as well as labelling of verbal conversation. The device shows 94.7 % of accuracy [20]. The device will be activated just in case of after-shock, otherwise, only the device will be warned.

Another Hidden Markov Model-based device is designed in [39], which collects the values with the help of IoT and HMM by the voice recognition of the victim woman. Speech recognition proves to be a compatible solution for HMM. But the device can fail to protect the woman in the worst situation if the attacker recognizes the device and cover the victim's mouth also the device has no sensors attached.

c: DECISION TREE CLASSIFIER

A data set is used to make predictions in terms of yes or no and continuously splits that dataset into the tree [44]. With the help of a decision tree, the women's safety system will be able to detect whether the respective women are in danger or not.

A work in [28] designed a device named MoveFree which works on the machine learning algorithm of Decision Tree Classifier. It predicts whether the woman is in danger or not by collecting the values from breathing, heartbeat and blood flow rate and glucose count. The readings are categorized as normal and abnormal. MoveFree considers the values to be abnormal if the readings are greater than the threshold value. Whereas, the threshold values are determined based on health experts. The algorithm decides whether a woman is in danger or not, based on sweating. If the woman is sweating she is in danger otherwise not. The device also informs the guardian if she is sweating due to some health issues. There is a major limitation considered in the device, the woman could sweat even due to weather then the prediction would be wrong.

d: OUTLIER DETECTION

The pressure sensor and temperature sensors are used in women's safety systems for outlier detection. As any of the sensors detect any type of abnormality the danger is detected [27]. Like the temperature sensor activates when someone suddenly approaches the woman and the temperature of her surroundings increases then the danger is detected [27]. The limitation considered for the outlier detection would be that the temperature can increase due to many reasons; it could be a health issue.

4) ASSESSMENT OF QUESTION 4- WHICH IOT-BASED WEARABLES ARE USED FOR WOMEN'S SAFETY?

Wearable sensors are embedded in IoT-based wearable devices that collect the readings fed to the sensors. The sensors activate the modules via internet connection if the specific values fed to the sensors exceeds. Considering the women's safety devices IoT-based wearables are developed in form of smart cloths, smart bands and smart ornaments. By reviewing the literature, it has been observed that there is still limited technology in women's safety domain. The researchers developed most of the devices in form of smart band. In literature, smart band is used 35%, smart jacket and other cloth based smart devices are used about 6%, smart ring and smart shoe up to 3% as shown in Figure 8. Table 9 enlists the sensors used in different wearables.

In [9] a smart ring has been developed for the protection of woman in case of any danger, which is useful in few circumstances. However, it has limitation that, it could fail to protect the women in case of hustle or snatching there is the chance for woman to lose the smart ring.

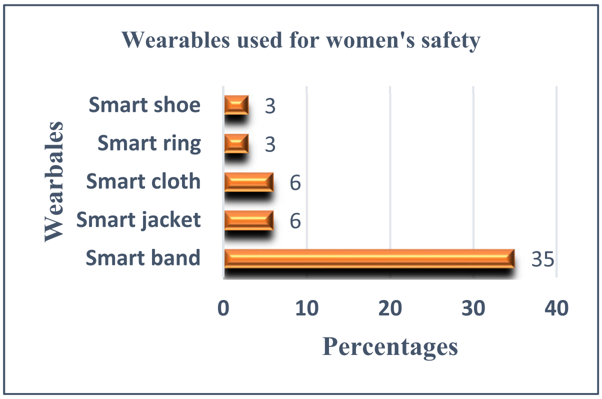


FIGURE 8. Percentages of wearables used in women's safety devices.

TABLE 9. Sensors associated to the specific wearables.

References	Wearables	Sensors
[9]	Smart ring	None
[16]	Smart band	Heartbeat and temperature sensors
[40]	Smart garb	Pressure sensor
[44]	Smart band	Vibration sensor
[24]	Smart jacket	Temperature, heartbeat and vibration sensor
[19]	Inner wear	Flex sensor
[33]	Smart jacket	Flex sensor
[29]	Smart band	Pulse-rate and temperature sensor
[21]	Smart band	Pulse-rate and tilt sensor
[37]	Smart band	Pulse-rate and tilt sensor
[28]	Smart band	Breathing and heartbeat sensor
[13]	Smart shoe	Acceleration sensor
[15]	Smart band	Pulse-rate sensor
[34]	Smart band	Pulse-rate, temperature, motion, vibration

There should be a device that is hidden from the eyes of attacker. Reference [16] proposed a novel smart band based wearable device that consist of heartbeat rate sensor and temperature sensor that takes the values from logistic regression model. The device is designed smartly for smart safety solution for women. But the device could fail to protect the women because it is also connected to the online portal that can fail in case of slow internet connection.

Bharadwaj designed a device named suraksha [45] for the safety and protection of women travelling alone and Kumar [40] designed a smart garb, which is any kind of special cloth. So, these systems can be used with various forms of cloths. The device can be made more portable and easier to use by replacing the solid wires with the comfortable and flexible wires. Another smart band wearable based on voice recognition of women is considered in [8] which detects vibrating motion of voice and activates the vibration sensor attached to the device. According to the analysis this device needs full time charging and exact matching of words fed to the device in case of any danger. Reference [33] proposed a smart wearable shoe device that works through human intervention and consists of only one sensor named as acceleration sensor. According to my opinion this device is not efficient and difficult to use because the single sensor attached to it could fail in any condition.

Researchers and developers are making IoT-based wearables more advanced and portable. For example, in [19] Prottasha Gosh developed a device wearable with undergarments. The device is compact in size and easy to hide from the attacker, which gives the ease to the victim.

By reviewing the literature, it has been observed that same wearable can work on different principles. The wearables proposed in [24] and [33] are based on smart jackets. By comparing both studies we get to know that [24] uses temperature, heartbeat and vibration sensors whereas [33] uses only flex sensor. According to the gaps and challenges identified in this review, the wearable consisting of multiple sensors is more vulnerable and efficient because any of the sensor can fail to detect or sense the values under certain conditions. Relying on data obtained through single sensor may not give appropriate results while determining the under potential victim as under threat or not, e.g., consider the study where a device rely only on flex sensor to measure the bending of the body where it is possible that the potential victim has to bend due to the reasons other than attack. This may cause failure of the device.

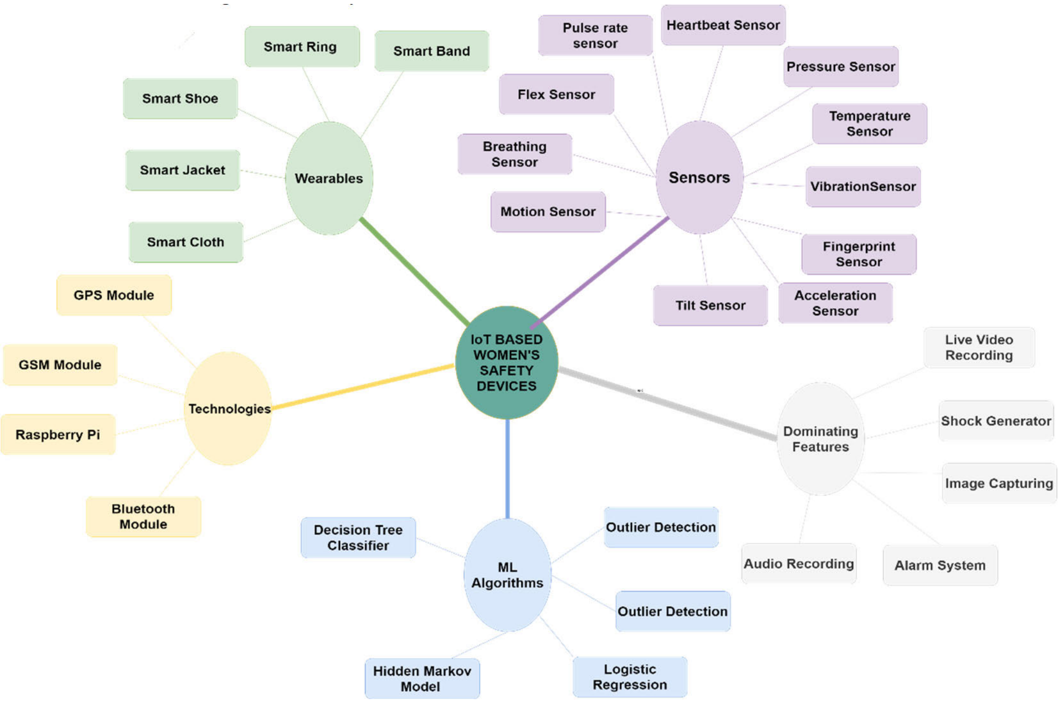


FIGURE 9. Taxonomy of IoT-based women's safety devices.

Most of the wearables for women's safety are developed in the form of smart bands. Smart bands are easier to use as compared to smart shoe or cloth-based wearables. As we have discussed smart wearables have embedded sensors that takes the values from the specific parts of body. Smart bands can have exposure to the whole body easily. But women in our society need more advanced and protected shield for safety due to increasing number of attacks. the researchers have to make more advanced wearables designed with a huge plethora of sensors. Cloth is mentioned for the studies where the specific cloth is not specified.

IV. DISCUSSIONS AND ANALYSIS

This section provides discussion and analysis on the results and findings of the review. Based on analysis of the findings, a taxonomy of IoT-based women's safety devices is proposed, the gaps and challenges of existing devices are highlighted, a model is suggested for practitioners and researchers as guideline to build the IoT-based women's safety devices, and implications as future directions of the underlying domain has been presented.

A. PROPOSED TAXONOMY

The findings of this research have been summarized by developing an IoT-based women's safety taxonomy, as shown in Figure 9.

The designed taxonomy consists of four primary attributes. These are IoT-based safety sensors, dominating features, machine learning algorithms, IoT-based wearables in which sensors are embedded and IoT-based technologies, which cover most of the findings that are analyzed in this paper. IoT-based technologies monitor, control, and track the different precision attacks and locations of victims and systems. IoT-based technologies used in women's safety devices with their sub-domains have been demonstrated. Sensors produce valuable data by sensing and monitoring multiple variables. The data generated through sensing and monitoring devices are transferred through the communication protocols (Internet, ZigBee, Bluetooth, WIFI) on the other side for a user or guardian of women.

The designed taxonomy consists of four primary attributes. These are IoT-based safety sensors, dominating features, machine learning algorithms, IoT-based wearables in which sensors are embedded and IoT-based technologies, which cover most of the findings that are analyzed in this paper. IoT-based technologies monitor, control, and track the different precision attacks and locations of victims and systems. IoT-based technologies used in women's safety devices with their sub-domains have been demonstrated. Sensors produce valuable data by sensing and monitoring multiple variables.

The sensors used in women's safety devices have been discussed in detail. Moreover, the dominating features of IoT-based women's safety devices, which make the devices efficient, used by the victim in different situations, are highlighted. Furthermore, to emphasize auto-activation of the alert generation feature, the data is collected through sensors, which on observing the readings that could depict specific state of women's body reflecting potential threat, enables the machine learning modules, after which alerts are generated and transmitted.

The machine learning algorithms are used by training these algorithms on the obtained input values of sensors under different conditions enabling the potential women under threat secretly inform the guardians without making any explicit interactions with the devices. The proposed taxonomy also presents the IoT-based wearables used for women's safety in which sensors are embedded to sense the danger and activate the algorithms of machine learning for further processing in terms of identifying the threat.

The wearable used to embed the IoT devices for women's safety rely on sensors that fetch the data from the user and make the device automated. As the sensors for taking input are required to be hidden from human eye, these are embedded in some wearables. Sogi in [9] proposed a smart ring-based device by combining the Raspberry Pi and the server but did not use any sensor. But Navya R. Sogi also mentioned that the device can be made more compatible by adding sensors. Another device proposed in [34] is comprised of multiple sensors and proves to be more efficient because smart IoT-based wearable devices turn out to be more efficient and portable by the use of wearable sensors. It has been observed that IoT-based women's safety devices using sensors are portable and easy to use without human interventions; however, the existing systems can be made more compatible by using multiple sensors in a single device. Hence, the architecture proposed in this literature review contains multiple sensors with multiple functionalities in a single wearable device to provide protection to women in any kind of undesirable situation.

B. GAPS AND CHALLENGES

The 21st century is the era of women empowerment, where not just financial security is important but also social security is necessary [8]. Although there are many ways for protection like CCTV cameras are fixed all around in this era but still women need protection from their guardians. But with the modernization of time, parents or guardians cannot travel with women all the time. Hence, there must be some technology for the protection of women by the guardians. Table 10 enlists the potential flaws of IoT-based women's safety devices presented in research.

A gap identified in IoT-based women's safety devices is that some of the devices use only one or two sensors but it has been observed that the devices consisting of different sensors provides better accuracies and improved results. It might be possible for the device not to detect the attached particular sensor during a situation. So, the devices comprising multiple sensors can sense the other attached sensor in case of failure of any of the sensors.

Since women belong to different age groups and having different normal ranges of the input readings; hence, activation of IoT-based wearables devices on sensing a threat depends upon reading of the sensor which is compared to the normal ranges as per the age group. However, only one sensor would not be given appropriate threat results as the reading could be lied out of normal range due to several other reason which could not be specifically relate to any threat. In this regard, multiple sensors reading and the combinations of their input values could be useful to reach to the more accurate results of determining whether the potential victim is under threat.

The studies generally do not mention any adjustment to the device depending upon women of which age is using the device. Another challenge faced by wearable devices is waterproofing and battery life. These devices can run out of battery at any time. In case of exposure to water and sweat, the devices will fail to work.

A major gap that most of the studies have concluded about the women's safety systems is of physical interaction of humans with the devices. There is a need to make the devices and apps automatic and free of human intervention, as discussed previously that no one remains in sense during the time of the attack. However, many researchers have proposed human interaction-free systems but still, there is a need to make these systems automatic. Lastly, problem-focused is that the accuracies the devices exhibit have the potential of improvement as none of the devices show 100% accurate results even by using machine learning algorithms. However, the algorithms applied gave better results but still, some more improvement is needed with the prediction data sets used.

Till now many devices have been designed but each of them has some flaws. The foremost drawback and challenge faced has been the human interaction with the devices as the victim never gets enough time to operate the devices. Almost all of them are manually driven or operated via mobile phone [7]. Women are not as physically strong and fit as men that's why they need a helping hand to travel alone and feel independent. Table 10 shows devices with their flaws. At the time of the attack, women are not in the state of consciousness that they could operate mobile phones or any device. We humans cannot respond aptly during any kind of attack or critical situation, there is still a need for a device which automatically rescues the victim. [29].

TABLE 10. Potential flaws in devices.

Flaws	References
Require human interactions	[9] [11] [10] [4] [19] [41] [40] [8] [24] [33] [22] [30] [37] [21]
Precision gaps	[18] [35] [20] [29]
Smartphone dependency	[36]

The previously proposed devices are not much effective to provide full fledge protection to the women of our society. Even after using machine learning algorithms researchers faced the gaps in the accuracies and precisions in results. Because body temperature and heartbeat could change even due to some health issues or change in other physical states such as while running or walking briskly. Hence, all of these devices have some flaws. More is the accuracy more will be

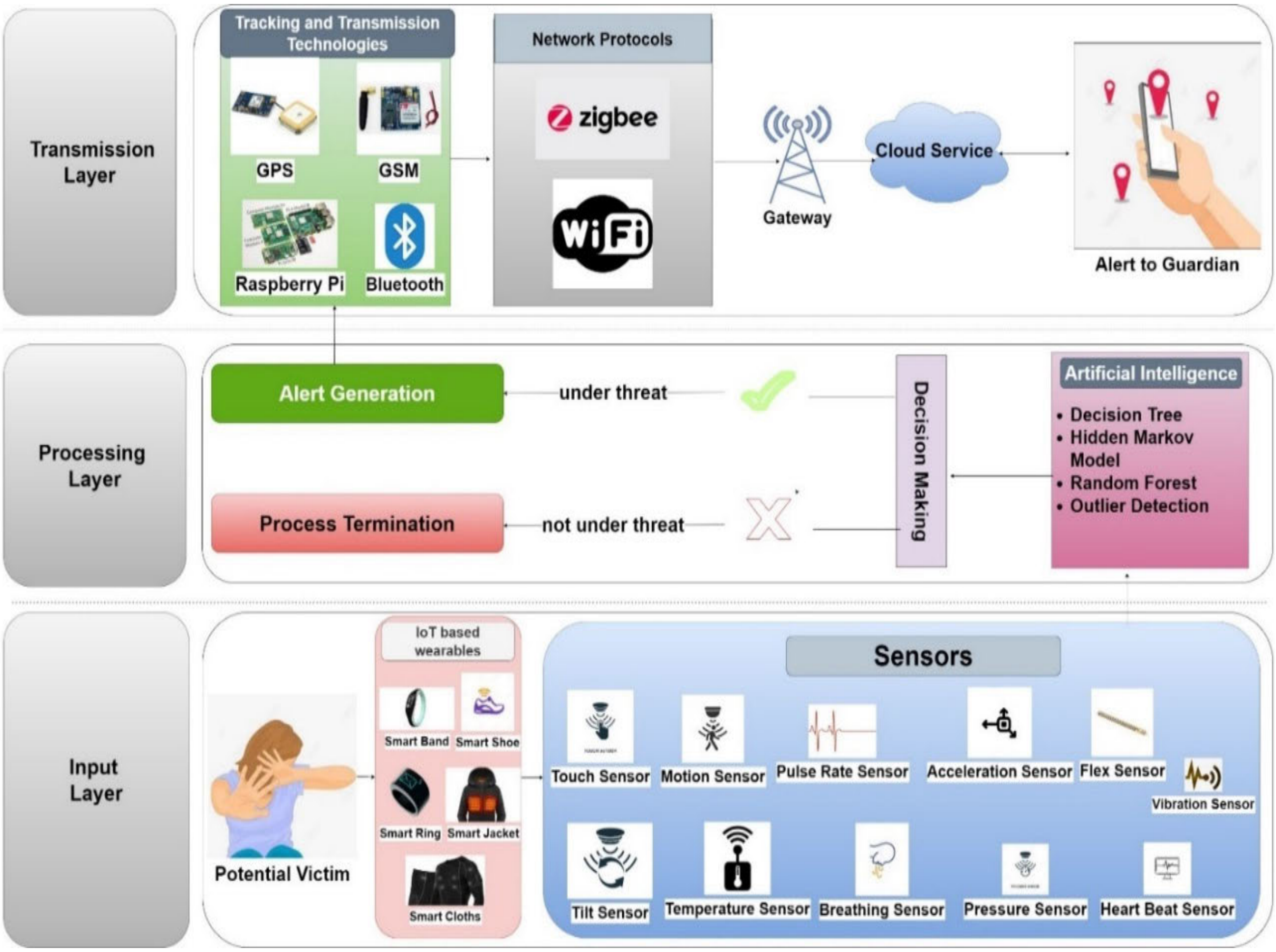


FIGURE 10. An architectural model for IoT-based women's safety devices.

the reliance on the results and surety of danger in case of identification of threat resulting in appropriate transmission of alerts so that emergency contacts could reach out on time in an alarming situation. [17]. There must be a model that can be carried anytime outside. It must be designed in a way that copes with women's safety issues in alarming situations and help them to inform guardians or police automatically [21]. Even during the case of kidnapping, the kidnapper snatches a mobile phone or any other gadget; hence, the usefulness of these devices in such scenarios could be questionable.

Moreover, some devices need more time for activation or some need to be used with smartphones, which could also be the reasons for the failure of existing devices and applications. The device proposed in [7] showed a smart band that needs two times tapping on the device after which the device is activated to track the temperature and pulse rate of the victim. It requires the victim to throw the band with force towards the attacker for sending the location to the police, it activates a piezo buzzer first before the activation of actual device, which shows the whole procedure is time taking. Even some devices need full-time internet connectivity for activation [38]. The accuracy level of detecting violations can be improved by making the devices more efficient and use more input types taken from multiple sensors.

IoT-enabled women's safety devices are not yet secured and robust because of this it is difficult to predict and identify all possible attacks on women in the IoT women's safety domain. Nonetheless, when researchers identify different security solutions to resolve predictable and manifest problems, they should have the capability to design a system that should have the capability to protect the woman from unpredictable and unseen attacks. To achieve such a security solution, a security system should be designed and implemented with vigorous properties. Consider a scenario in which the security system consists of different sensors and schemes to detect that women are under attack. Now consider that with an expansion of the women's protection system, an attacker pledges an attack that threatens women. In such cases, existing security systems are expected to be not enough to control and design a new system that is human interaction free by implementing artificial intelligence-based dynamic algorithms.

C. PROPOSED ARCHITECTURAL MODEL

Based on the review of results and findings, an IoT-based architecture for women's safety devices has been proposed as presented in Figure 10.

The proposed architecture is designed by considering the gaps and challenges of existing devices. The gaps identified in previous devices highlight the physical interaction of human required by the devices and potential of improvement in the accuracies of machine learning algorithms. The design of the architectural model is free of human interaction and uses lightweight and efficient machine learning algorithms for better decision.

The suggested system works as an automatic danger detection tool that works through artificial intelligence without human interaction and even works in places where there is no internet connection. A similar device has been proposed in [17], but the device is operated by pressing the button. The architecture proposed in this paper is free of human interaction, automatically collects the data through sensors and informs the guardian of the woman in danger. The sensors used in this proposed architectural model are designed to detect something as complicated as a human brain signal. The development of sensors allows the developers to use them technically and invent different smart wearables. The smart wearables are designed by using the microcontroller and sensors. These wearables are intelligent enough to protect a woman in danger. Sometimes, these devices have the facility to provide self-defense on spot.

ZigBee network is used in place of low internet connectivity. It uses low cost and low data consumption. And mesh is used as a type of network connectivity [46]. For women's safety, to overcome the problem of internet ZigBee Mesh Network. The ZigBee module used will only work when there is no internet. It can be noted that we can attach as many routing devices working to increase the range of data travelling to multiple hops and then reaching the gateway which is attached to the internet [17]. Muskan in [17] uses Zigbee Mesh Network to deal with scenarios where there is no internet connectivity. The same network is used in this proposed architecture to make the system more efficient. The transmission layer has a gateway connected to the cloud service which is used to send live location and attack alerts to the guardian of the victim.

The purpose of using machine learning algorithm is to make the devices learn for themselves without need of human intervention. IoT-based sensors being intelligent already, when combined and trained with machine learning produce excellent results in protecting the women from danger.

As shown in Figure 10, the proposed architecture consists of input, processing and transmission layers. The architecture proposed in model is basically designed to detect that the woman is in danger or not. These devices are constructed in form of wearables. The sensors and technologies are embedded in a smart IoT-based wearable, that a person can wear anywhere. Multiple sensors are used to detect the activity of the woman and the sensors' data is sent to the cloud where machine learning algorithms make the decision. The guardian will be alarmed if there is more accuracy in danger with more surety of danger [17].

The device will be able to read and create patterns of danger automatically. The input layer is comprised of multiple sensors used in women safety devices. The sensors are attached to the particular wearable device by the woman. Sensors are used to activate the modules, which are trained by machine learning algorithms. The sensors are linked to the Artificial intelligence based different algorithms in the processing layer. The device is trained by using real time values of woman under threat and not under threat. Existing devices are designed to collect the readings of heartbeat and pulse-rate from the sensors but these values can change due to many reasons. But the proposed model is associated with the computational models and multiple sensors that are fully trained after collecting a large number or real time values of heartbeat-rate, pulse-rate, motion-rate and temperature, when a woman is under attack.

IoT sensors are designed with different specifications and variations, such as, sensors are designed to deal with 2-mile communication distance with the included antennas and up to 28-mile range. It takes up to 50s for the IoT-based sensor to send 1000 sensor data points at a time [47]. A GSM operates on a SIM card and over a network range subscribed by the network operator. It can be connected to a computer through serial, USB or Bluetooth connection [42].

The processing layer makes the decision whether the woman is in danger or not, considering the features of machine learning algorithms. It determines whether the potential victim is under threat or not. If determined as not under threat then the woman is not in danger and the process terminates. If yes then the woman is suspected to be under attack and the alert generation process starts.

The alert is generated in transmission layer by activating the tracking and communication technologies. The GPS, GSM, Raspberry and Bluetooth technologies are used to capture the motion of the victim.

The modules then send the signal to the network protocols. After activation of tracking and transmission technologies the dominating features are activated through internet protocols. Then an alert of danger is sent to the guardian's device through gateway and cloud service. The IoT gateway is the bridge between sensors and internet protocols.

The dominating features involved in the process are image capturing, location tracking, audio and video recording and message sending. Each dominating feature is specifically associated with the tracking and transmission technologies. The location is tracked by the GPS module whereas the GSM is used to send the message and Raspberry Pi activates other features like image capturing and acquisition. The Raspberry pi is a small chip, which has many versions introduced till the date, i.e., Raspberry pi 3, Raspberry pi 4. The features and specifications of Raspberry Pi are different from version to version such as one of the raspberry is available with the dimensions of 85.60 mm × 53.98 mm × 17 mm, weighing only 45 g is given in [47].

Existing devices also contain the feature of shock generation. Shock generator helps the woman or the person under attack to fight against the attacker. In early times, people used to have pepper spray like stuff with them for protection but now with the advancement of technology and women's safety devices all the features are contaminated in one single wearable device. Although the model is suggested for women's safety IoT devices, yet it can be used to develop any IoT device for any person under threat. The system will decide whether the woman is in danger or not based on readings collected through the motion, breathing, pulse-, temperature and touch sensors. The motion sensor identifies the gait movement of the woman. The major sensors are heart rate, pulse-rate and breathing sensor. During the case of any attack the heartbeat, breathing, and temperature increase with the decrease in pulse-rate. The proposed architecture could be beneficial to decrease the cases of sexual harassment and crimes against women, and also provide confidence to the modern woman of this modernizing era to walk alone in society. As the proposed architecture is based on gaps and challenges identified in the existing literature. Although this architecture is suggested as guidelines to develop more useful IoT devices for women's safety yet the same components could be used for any potential victim who fear similar threats. Although the model is proposed by carefully reviewing and analyzing literature yet it has some limitations as proposing an absolute women's safety system is not realistic. IoT-based women's safety solutions can save women from any kind of physical abuse or harassment but still, there is no such active device that could prevent victims before assaulting like an acid attack. Considering state-of-the-art women's safety devices, it has been concluded that existing devices need human interaction for prevention. However, applying machine learning algorithms to women's safety systems will lead to IoT's realization.

Although women's safety system with machine learning algorithms addresses some IoT network issues, significant research issues still need to be addressed through women's safety. The real-time-based training dataset is required to achieve high accuracy of machine learning models for making efficient women's safety systems. There is a risk that the device or system might go under the wrong prediction or may stop working due to technical reasons on time. The readings of sensors may change due to any reasons it can be due to bad health, weather or any technical issue. The proposed system is free of human interaction as compared to the existing systems but still, the proposed system needs a physical attachment to the human body. There are chances to lose the device by the victim. If the decision-making step goes wrong due to uneven readings of sensors it will give wrong information to the guardian.

D. IMPLICATIONS

Considering the previous devices and apps, the future demand for women's safety devices is that they should be compact, with low prices and easy-to-use instructions. With all the features of protection. The new device should be the approach for women in rural areas because the number of physical abuse cases is higher in rural areas. The device should be designed in a way that it gives 100 per cent correct information about danger to the guardian of the woman. It has been noticed that even machine learning trained devices do not give 100 per cent accurate results. So, the devices must undergo more prediction sets. A new system needs to be developed that has a self-defense mechanism too without human intervention. The system should be designed in a way that the location of the victim changes on the guardian's phone with the actual change in location. The device should not rely on internet connectivity. As well as the device or system should be trained by real-time attacks on women.

Multiple input from more than one sensors and their combinations could give more precise and accurate results interns of determining the potential victim as under threat or not. In this regard, more full body sensors like temperature, tilt, and flex along with the sensor which can take input or related to specific body area such as heartbeat sensor should be used. As the potential victim needs to wear different gadgets having the IoT-based devices for safety, the use of multiple body-area specific sensors emerges the inherent need of wearing more than one gadgets.

If designed up to the mark, women's safety systems will be beneficial for the women who have to travel late at night or at workplaces. They will feel safe up to some extent while going out. It will help us to analyze the severity of crimes against women [17]. With the help of these devices' women‘s safety is properly protected and they won't feel alone. These devices should be compact to easily carry and the key concern should be including unique features from different approaches [38]. For providing security various smart devices should be more advanced. Currently, there is no such solution but these devices should be more effective with time as the cases of women violence are increasing day by day. There is a serious need for the advancement of these devices and apps so that parents could have watched young girls. With the advancement of time, there must be a better and more advanced security system for the safety of wo_Ref118040611

V. CONCLUSION

This study reports a systematic literature review of IoT-based devices designed for women's safety to protect them from threats like molestation, harassment, rape, and abuse. It was conducted by reviewing 34 research articles gathered through eminent publication sources. The papers for reviewing the IoT-based devices for women's safety are gathered by considering a number of keywords and their alternate words. Though a number of the keywords are used to search the relevant literature, there exist the possibility that some studies used other words and their synonyms in their work that could affect the final results. This risk was mitigated by carefully considering various keywords and classify these keywords as primary, secondary, and tertiary to form the search string and apply different Boolean operators to combine the specified classification of keywords. In addition, the classification of the studies has been made by authors, which is reviewed by two independent reviewers. In case any disagreement was observed, a comprehensive discussion among the authors was made till reaching to consensus. The interrater reliability was 0.92 that depicted a high agreement.

After detailed analysis of the shortlisted studies, it was identified that IoT-based women's safety devices use different technologies as well as exhibits a number of prominent features, sensors and machine learning algorithms. Various categories of these aspects are classified to present a taxonomy of IoT-based women's safety devices. Although each system provides different features which define the main working of those devices yet there are some shortcomings due to which these systems still not able to give effective support to deal with the potential safety threats for women. Moreover, this study presented the gaps and challenges of using the previous devices due to which some devices could not work effectively to serve the purpose. Furthermore, this review proposed an architectural model for IoT-based devices for women safety as future recommendation. This work will be helpful for the researchers to gain the state-of-the-art insight into the IoT-based women's safety devices as well as the practitioners to build useful and more effective IoT-based women safety devices.

REFERENCES

[1] *Violence Against Women and Girls*, ActionAid, World Health Org., Switzerland, 2021.

[2] *Violence Against Women*, World Health Organization, Geneva, Switzerland, 2021.

[3] *Gender Inequality*, World Economic Forum, Cologny, Switzerland, 2020.

[4] G. Gulati, T. K. Anand, T. S. Anand, and S. Singh, "Modern era and security of women: An intellectual device," *Int. Res. J. Eng. Technol. (IRJET)*, vol. 7, no. 4, pp. 212–218, 2020.

[5] K. M. Opika and C. M. S. Rao, "An evolution of women safety system: A literature review," *Int. Bilingual Peer Reviewed Peered Res. J.*, vol. 10, no. 40, pp. 61–64, 2020.

[6] B. S. Bala, M. Swetha, M. Tamilarasi, and D. Vinodha, "Survey on women safety using IoT," *Int. J. Comput. Eng. Res. Trends*, vol. 5, no. 2, pp. 16–24, Jan. 2018.

[7] S. Ahir, S. Kapadia, J. Chauhan, and N. Sanghavi, "The personal stun—A smart device for women's safety," in *Proc. Int. Conf. Smart City Emerg. Technol. (ICSCET)*, Jan. 2018, pp. 1–3.

[8] A. Agrawal, A. Maurya, and A. Patil, "Voice controlled tool for anytime safety of women," *J. Emerg. Technol. Innov. Tool*, vol. 8, no. 5, pp. a966–a975, 2021.

[9] N. R. Sogi, P. Chatterjee, U. Nethra, and V. Suma, "SMARISA: A raspberry Pi based smart ring for women safety using IoT," in *Proc. Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, 2018, pp. 451–454.

[10] W. Akram, M. Jain, and C. S. Hemalatha, "Design of a smart safety device for women using IoT," *Proc. Comput. Sci.*, vol. 165, pp. 656–662, Jan. 2019.

[11] B. Sathyasri, U. J. Vidhya, G. V. K. J. Sree, T. Pratheeba, and K. Ragapriya, "Design and implementation of women safety based on IoT technology," *Int. J. Recent Technol. Eng.*, vol. 7, no. 6, pp. 177–181, 2019.

[12] A. Ometov, V. Shubina, L. Klus, J. Skibinska, S. Saafi, P. Pascacio, L. Flueratoru, D. Q. Gaibor, N. Chukhno, O. Chukhno, and A. Ali, "A survey on wearable technology: History, state-of-the-art and current challenges," *Comput. Netw.*, vol. 193, Jul. 2021, Art. no. 108074.

[13] S. P. Raja and S. S. Rachel, "Women's safety with a smart foot device," in *Proc. 4th Int. Conf. Comput. Commun. Technol. (ICCCT)*, Dec. 2021, pp. 570–573.

[14] T. Sowmya, D. Treevani, D. Keerthana, and A. V. Laxmi, "Women' safety system using IoT," *Int. Res. J. Eng. Technol.*, vol. 7, no. 3, pp. 3301–3305, 2020.

[15] H. Nagamma, "IoT based smart security gadget for women's safety," in *Proc. 1st Int. Conf. Adv. Inf. Technol. (ICAIT)*, Jul. 2019, pp. 348–352.

[16] S. Pagadala, L. Prasanna, and A. Reddy, "A novel ML—Supported IoT device for women security," *Int. Res. J. Eng. Technol.*, vol. 8, no. 6, pp. 3287–3291, 2021.

[17] T. Khandelwal, M. Khandelwal, and P. S. Pandey, "Women safety device designed using IoT and machine learning," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov.*, Oct. 2018, pp. 1204–1210.

[18] A. Jesudoss, "Smart solution for women safety using IoT," *Int. J. Pure Appl. Math.*, vol. 119, no. 12, pp. 43–49, 2019.

[19] P. Ghosh, T. M. Bhuiyan, M. A. Nibir, Md. E. Hasan, Md. R. Islam, M. R. Hasan, and T. Hossain, "Smart security device for women based on IoT using raspberry pi," in *Proc. 2nd Int. Conf. Robot., Electr. Signal Process. Techn. (ICREST)*, Jan. 2021, pp. 57–60.

[20] D. Seth, A. Chowdhury, and S. Ghosh, "A hidden Markov model and Internet of Things hybrid based smart women safety device," in *Proc. 2nd Int. Conf. Power, Energy Environ., Towards Smart Technol. (ICEPE)*, Jun. 2018, pp. 1–9.

[21] S. Srinivasan, P. M. Kannan, and R. Kumar, "A machine learning approach to design and develop a BEACON device for women's safety," in *Recent Advances in Internet of Things and Machine Learning*. Cham, Switzerland: Springer, 2022.

[22] V. R. Balaji, N. Paramanandham, and M. Murugan, "Guardian device for women—A survey and comparison study," in *Proc. 2nd Int. Conf. Robotics, Intell. Automat. Control Technol.*, Chennai, India, 2021, Art. no. 012030.

[23] L. F. Cardoso, S. B. Sorenson, O. Webb, and S. Landers, "Recent and emerging technologies: Implications for women's safety," *Technol. Soc.*, vol. 58, Aug. 2019, Art. no. 101108.

[24] S. Das, S. Dasar, and J. S. Rao, "Women's security system," *Int. J. Eng. Res. Technol. (IJERT)*, vol. 10, no. 7, pp. 483–486, 2021.

[25] D. Kaur, R. Chahar, and J. Ashta, "IoT based women security: A contemplation," in *Proc. Int. Conf. Emerg. Smart Comput. Informat. (ESCI)*, Mar. 2020, pp. 257–262.

[26] E. T. Rother, "Systematic literature review X narrative review," *Acta Paul Enferm.*, vol. 20, no. 2, pp. 5–6, 2007.

[27] V. Hyndavi, N. S. Nikhita, and S. Rakesh, "Smart wearable device for women safety using IoT," in *Proc. 5th Int. Conf. Commun. Electron. Syst. (ICCES)*, Jun. 2020, pp. 459–463.

[28] S. Roy, A. Sharma, and U. Bhattacharya, "MoveFree: A ubiquitous system to provide women safety," in *Proc. 3rd Int. Symp. Women Comput. Informat.*, Kochi, India, Aug. 2015, pp. 545–552.

[29] S. S. Raksha, Y. R. Reddy, E. I. Meghana, K. M. Reddy, and P. K. Panda, "Design of a smart women safety band using IoT and machine learning," *Int. J. Contemp. Archit.*, vol. 8, no. 1, 2021.

[30] S. Mohapatra, C. Ramya, N. G. Sahana, V. Savithri, and S. Yashaswini, "A smart women protection system using IoT," in *Data Intelligence and Cognitive Informatics*. Singapore: Springer, 2022, pp. 459–465.

[31] G. C. Harikiran, K. Menasinkai, and S. Shirol, "Smart security solution for women based on Internet of Things (IoT)," in *Proc. Int. Conf. Electr., Electron., Optim. Techn. (ICEEOT)*, Mar. 2016, pp. 3551–3554.

[32] N. Saranya, R. Aakash, K. Aakash, and K. Marimuthu, "A smart friendly IoT device for women safety with GSM and GPS location tracking," in *Proc. 5th Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Dec. 2021, pp. 409–414.

[33] B. R. Reddy, T. Sowjanya, N. B. Subrahmanayam, G. Mahantesh, and S. Prudhvi, "IOT based smart protective equipment for women," *Mater. Today, Proc.*, vol. 80, pp. 2895–2900, 2023, doi: 10.1016/j.matpr.2021.07.058.

[34] A. Bhate and S. H. Parveen, "Smart wrist band for women security using logistic regression technique," *Int. J. Recent Technol. Eng.*, vol. 8, no. 1, pp. 2215–2218, 2019.

[35] M. R. Ruman, J. K. Badhon, and S. Saha, "Safety assistant and harassment prevention for women," in *Proc. 5th Int. Conf. Adv. Elect. Eng.*, 2019, pp. 346–350.

[36] V. K. Devi, A. Kavya, and D. Shruthi, "IoT-SDWD: Internet of Things-based security device for women in danger," in *ICT With Intelligent Applications*. Singapore: Springer, 2021.

[37] K. Venkatesh, S. Parthiban, P. S. Kumar, and C. N. S. V. Kumar, "IoT based unified approach for women safety alert using GSM," in *Proc. 3rd Int. Conf. Intell. Commun. Technol. Virtual Mobile Netw. (ICICV)*, Feb. 2021, pp. 388–392.

[38] M. Chaware, D. Itankar, D. Dharale, D. Borkar, S. K. Pendyala, and K. Pendyala, "Smart safety gadgets for women: A survey," *J. Univ. Shanghai Sci. Technol.*, vol. 22, no. 12, pp. 1366–1369, 2020.

[39] N. B. Nanekar and G. Kauthale, "Woman safety device," *Int. Adv. Res. J. Sci., Eng. Technol.*, vol. 8, no. 5, pp. 542–544, 2021.

[40] D. K. M. AnandKumar, "Smart garb—A wearable safety device for women," *Int. J. Res. Appl. Sci., Eng. Technol.*, vol. 8, no. 5, pp. 513–519, May 2020.

[41] D. Sunehra, V. S. Sreshta, V. Shashank, and B. U. K. Goud, "Raspberry pi based smart wearable device for women safety using GPS and GSM technology," in *Proc. IEEE Int. Conf. Innov. Technol. (INOCON)*, Nov. 2020, pp. 1–5.

[42] C. K. Gomathy, "Women safety device using IoT," 2022.

[43] T. W. Edgar and D. O. Manz, *Research Methods for Cyber Security*. Elsevier, 2017.

[44] C. Bento, "Decision tree classifier explained in real-life: Picking a vacation destination," 2021.

[45] N. Bhardwaj and N. Aggarwal, "Design and development of 'Suraksha'—A women safety device," *Int. J. Inf. Comput. Technol.*, vol. 4, pp. 787–792, Feb. 2014.

[46] J. Sun and X. Zhang, "Study of ZigBee wireless mesh networks," in *Proc. 9th Int. Conf. Hybrid Intell. Syst.*, 2009, pp. 264–267.

[47] M. Syafrudin, G. Alfian, N. Fitriyani, and J. Rhee, "Performance analysis of IoT-based sensor, big data processing, and machine learning model for real-time monitoring system in automotive manufacturing," *Sensors*, vol. 18, no. 9, p. 2946, Sep. 2018.

[48] D. Sunehra, V. S. Sreshta, V. Shashank, and B. U. K. Goud, "Raspberry Pi based smart wearable device for women safety using GPS and GSM technology," in *Proc. IEEE Int. Conf. Innov. Technol. (INOCON)*, Nov. 2020, pp. 1–5.

[49] U. Farooq and T. Kamal, "A review on Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 113, no. 1, pp. 1–7, 2015.

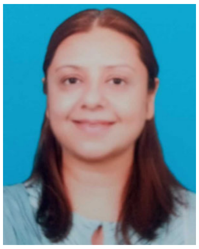
[50] A. D. Mishra, "Women empowerment: Issues and challenges," *Indian J. Public Admin.*, vol. 60, no. 3, pp. 398–406, 2020.

[51] F. R. Kian, M. Alikamali, M. M. Aliei, and A. Mehran, "Patterns of intimate partner violence: A study of female victims in urban versus rural areas of Southeast Iran," *Shiraz E-Med. J.*, pp. 1–7, 2019.

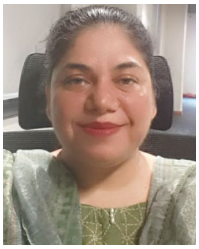
[52] *High-Level Conference on Ending Violence Against Women*, Org. Econ. Cooperation Develop., Paris, France, 2020.

MUHAMMAD SHOAIB FAROOQ is currently a Professor in computer science with the University of Management and Technology, Lahore. He was an affiliate member of George Mason University, USA. He possesses more than 26 years of teaching experience in computer science. He has published many peer-reviewed international journals and conference papers. His research interests include the theory of programming languages, big data, the IoT, the Internet of Vehicles, machine learning, blockchain, and education.

AYESHA MASOOMA received the B.S. degree from Qarshi University, Lahore, in 2021. She is currently pursuing the master's degree in computer science with the University of Management and Technology. She is also a Senior Software Engineer with the University of Management and Technology. Her research interests include machine learning, the IoT, and software engineering.



UZMA OMER received the Ph.D. degree in computer science from the University of Management and Technology, Lahore, Pakistan. She is currently an Assistant professor with the Department of Information Sciences, University of Education, Pakistan. Her research interests include computer science education, machine learning, the IoT, E-learning systems, and educational technology.



RABIA TEHSEEN received the Ph.D. degree in computer science from the University of Management and Technology, Lahore, Pakistan. She is currently an Assistant Professor with the University of Central Punjab, Lahore. She is the author of seven journals and conference papers. Her research interests include machine learning, federated learning, and earthquake physics.

S. A. M. GILANI received the Ph.D. degree in digital imaging from the University of Patras, Greece, in 2002. He is currently a Professor with the Department of Computer Science, FAST National University of Computer and Emerging Sciences, Lahore, Pakistan. His research interests include digital image processing, computer vision, and multimedia data security. He has supervised numerous M.S. and Ph.D. students in the area of image processing and image watermarking.

ZABIHULLAH ATAL received the master's degree in information technology from the VU University of Pakistan. He is currently an Assistant Professor with the Computer Science Department, Kardan University, Afghanistan. His research interests include computer networks and information security, the IoT, machine, neural networks, smart grid applications and technologies, cloud computing, distributed systems, and blockchain.