International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-4 November 2020

Women's Wearable Security and Safety Device

S.K. Anisha, S.Chandana, J.J.Teresa, S.Varma, M. N. Thippeswamy

Abstract: ***In today's world, one of the major issues that women all across the globe face is threats to their safety and security. This paper presents a quick safety device that responds immediately when women are in danger. The device is equipped with a button and on pressing the button, a "HELP"message is sent along with the location coordinatesto the trusted contacts via an SMS. The device is also capable of capturing an image and a video which can then be analyzed to identify the perpetuator. When a woman feels threatened or she finds herself in a compromising situation, she can use this device for her safety.***

Index Terms**: *Internet of Things, Raspberry-Pi, Wearable, Women's security***

I. INTRODUCTION

Safety is a crucial power of an individual whether at home or outside. In today's world, women are less safe and secure. They face critical abusive situations such as assaults where their safety is compromised. The government has introduced various laws and opened many agencies to improve the policies. Many devices have been developed to ensure safety and security of women. Many digital applications have been introduced that serve as a means to battle against offenders against women.[1]

The proposed system is a safety mechanism in case of emergencies whenever women are in grave danger. The proposed system can be used as a wearable device that can be worn by women everyday so that they can use it whenever they feel threatened. The main purpose of the system is to alert the trusted contacts through SMS whenever women press a button. The location of the victim is sent via SMS to the trusted contacts so that they are able to track the location of the victim. A GPS Module is used to capture the location of the victim and a GSM module is used to send SMS to the trusted contacts. The system also has a camera that captures the image of the offender and sends it to predefined emails of the trusted contacts. A video is also recorded and sent to the same contacts. The system is mainly designed for women but can also be used by elderly people and children.

The main objective of the system is to provide safety to women from dangerous people.

Revised Manuscript Received on October 20, 2020.
Manuscript Received On October 06, 2020
*****Correspondence Author
S.K. Anisha, Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Bangalore
S.Chandana, Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Bangalore
J.J.Teresa , Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Bangalore
S.Varma, Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Bangalore
M. N. Thippeswamy, Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Bangalore

When the victim presses the button, the trusted contacts are notified of the location of the victim and an image is sent so that it can be used for further purposes. An android application called SEGURO is also developed so that the victim can use it to send messages to the trusted contacts when the button is inaccessible. Location information can also be sent via the app by the victim.

All the information is stored in clouds like Google Drive and Firebase. Both the clouds contain information sent by the module like the images. A study is carried out to review the already existing systems and the salient features are incorporated in the proposed system. In the proposed safety system, the deficiencies of the existing systems are identified and a novel system is developed. The novel contributions are:

- A Women's wearable device is designed using Raspberry Pi, GSM Module, GPS Module and a camera, which can capture images and record a video to provide visual proof whenever the victim is attacked. Based on this information, the perpetrator can be caught and the victim can be located easily.
- A reporting system is developed to store the visual proof and upload it to cloud and send it via mail for further documentation.
- An Android App is developed to obtain the location of the victim. The victim can also send the location to the trusted contacts through the App. A call feature has also been integrated. The App also provides a portal to inform the necessary emergency authorities whenever the victim is threated.
- A face recognition system is implemented on the recorded video that helps identify the perpetrator in case a face is detected. This enables the emergency authorities to catch the perpetrator easily.

II. RELATED WORKS

The literature survey is undertaken so as to study similar works which had been carried out in the past. These include papers on devices for monitoring various health parameters, smart phone applications, wearables such as wrist bands, pendants, footwear, etc. and the communication mediums that could be used in case of emergency. After studying these papers, we have adapted the important features of a few devices and we have added some modifications to enhance the already existing system. The information obtained from the literature survey was used as a basis to enhance our safety system. The authors have devised a completely electronic GLOVE with the circuitry mounted within the glove and properly insulated from the outside so as to prevent the user from any kind of harm or danger. The user only has to activate the palm side of the glove which is the conducting layer on encounter of any violent activity.

On activation, the conductive layer gives a frightening shock to the attacker as a result of which the oppressor has a profound impact on the muscular activity, thereby, overpowering the wearer over the attacker with ease. The proposed system in introduces a technique of a wearable fingerprinting device via machine learning that enables addressing the cyber-attacks, provides cyber threat intelligence and also demonstrates the feasibility of the proposed technique to provide reliable cyber threat intelligence.

It focuses on Bluetooth protocol which is a common protocol used by the wearables and other IoT devices. The authors have conducted a detailed survey on commercially available wearable devices ("wearables") and research prototypes. They have classified the wearables, conducted a research on the existing wearables in the market along with drawing comparisons among one another. A partial portable device for the rescue of women was proposed. The authors have tried to create a safety system that mergers the benefits of android applications on phone and wearable apparels or ornaments. The prototype developed by the authors uses Arduino Uno board, GPS module, GSM module, Raspberry Pi, and a Webcam. [2-5]

The work mentioned deals with the development of a good robust and high precision platform of wearable devices of internet of things. Based on the boost algorithm to optimize the path and Agent algorithm, the wireless network data transmission is well designed. A wearable device solely used in both monitoring the patients and preventing repetitive ankle sprain due to chronic ankle instability was designed. This device was connected to a smart phone for storage and analysis. The authors have mentioned thatthe prototype is based on the usage of various sensors to monitor the health conditions of an individual and alert the medical practitioner during any fluctuations in the health parameters. The prototype uses Bluetooth Low Energy (BLE) for communication purposes. BLE is a replacement for Bluetooth as it is more efficient and less power consuming.The system proposed describes the usage of a smart foot device for women to alert friends and relatives during emergency situations. Since a mobile phone may not always come handy for a victim in times of trouble, a smart foot device has been developed. [6-9] The various prototypes developed in the literature survey have provided a basic framework for safety device. Most of the prototypes encountered sent messages containing the location of the victim. Though the prototypes were all developed for the sole purpose of providing safety to women, they are implemented differently, some are implemented as a Foot Device, some are implemented as safety vests and some are implemented as gloves. [2-14]

The proposed device in this work, uses the basic framework mentioned in all prototypes by sending the location to the trusted contacts via SMS. A camera feature is added to the device to capture visual evidence. A face recognition deep learning network is also adapted. An Android app is also developed along with the hardware device.

III. WORKING OF THE SAFETY DEVICE

The proposed prototype aims to develop a wearable device for ensuring the safety of women. The working of the device is briefly explained :

On the first use of the device, the trusted contacts need to be added in the dedicated android device (Seguro). When the button on the device is pressed the following actions occur:

- GPS module activated; current location of the user captured and sent through SMS message via the GSM module to trusted contacts
- Pi camera activated; image captured and uploaded to Drive;image copy sent to email IDs of trusted contacts
- Pi camera still on activated mode; video recorded and sent to the email IDs of trusted contacts
- Captured image/video analyzed by face recognition algorithm; face identified if matched with the database of criminals

The overall structure of the system is given in Figure 1. The proposed system follows the model given in Figure 2.

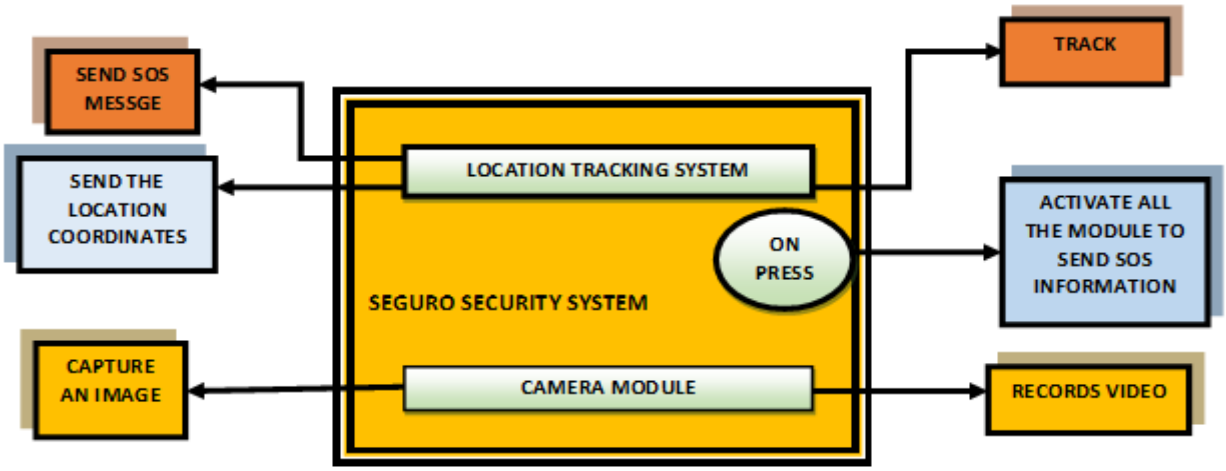

Figure 1: The overall structure of the proposed system.

ure 1: Overall Structure of the proposed system

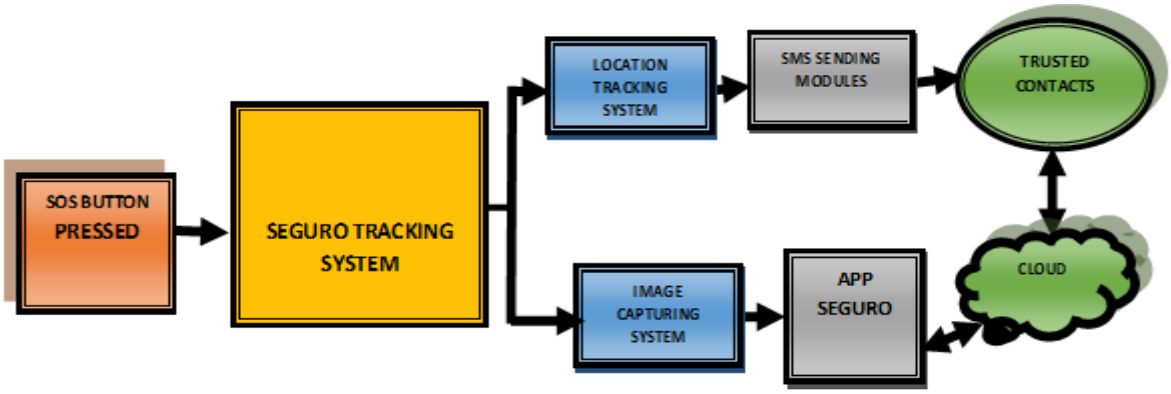

Figure 2 : The Proposed System

A. WORKING OF THE ANDROID APP-SEGURO

An Android Application called SEGURO is developed that can be integrated with the safety system. The app has a login module that allows the users to use the app along with the safety device. The app has modules to add, delete, view and modify trusted contacts to whom the SOS message will be sent. There is an option to send the location as coordinates to the trusted contacts. The app also has an option to call the trusted contacts. The app can also be used to view the image that is captured when the user presses the SOS button from drive. Overall, the app functions as a substitute for the safety device and can be used to provide additional safety to the user.

B. WORKING OF FACE RECOGNTION

Face recognition is a method used to identify and verify the identity of a person through various features of their face. The image captured using the camera when the user presses the SOS button is analysed to see if any face is detected, if detected the face is recognised and the name is notified to the trusted contacts so that the perpetrator can be caught. OpenCV, numpy, Haar Cascade classifier is used for face recognition.

The whole face recognition algorithm can be classified into the steps given below

Step 1: An input containing the images of faces is considered.

Step2: The face is detected.

Step3: The picture is then transformed for more accurate results so that the image is cropped eliminating the unnecessary background.

Step 4: The cropped image is then sent to the deep learning algorithm, Facenet.

Step5: It will output a vector representation of that face.

Step 6: Then the representation is compared against the already trained faces to determine if any known face can be recognised.

IV. IMPLEMENTATION

In this section, the implementation of the wearable security and safety system is briefly discussed. The Table 1 gives all the components used to implement the wearable security and safety system in this work. Figure 3 shows the flowchart for the safety device. Figure 4shows the flowchart for the Android App. The overall working of the system is explained subsequently.

Table 1: The various components used in the safety device

Hardware Specifications	**Software Specifications**	
Hardware Requirements	**Hardware Requirements**	**Software Requirements**
Raspberry Pi 3 GPS Module GSM Module Pi camera Buzzer Pushbutton Power Supply	Processor : Intel® Core™ i7-2670 QM @2.20 GHz RAM : 4 GB HDD : 80 GB	Platform : Windows 10, Mac OS Mojave, Ubuntu 16.04, Raspbian Front End : Python Back End : Firebase, Android Phone, Google Drive

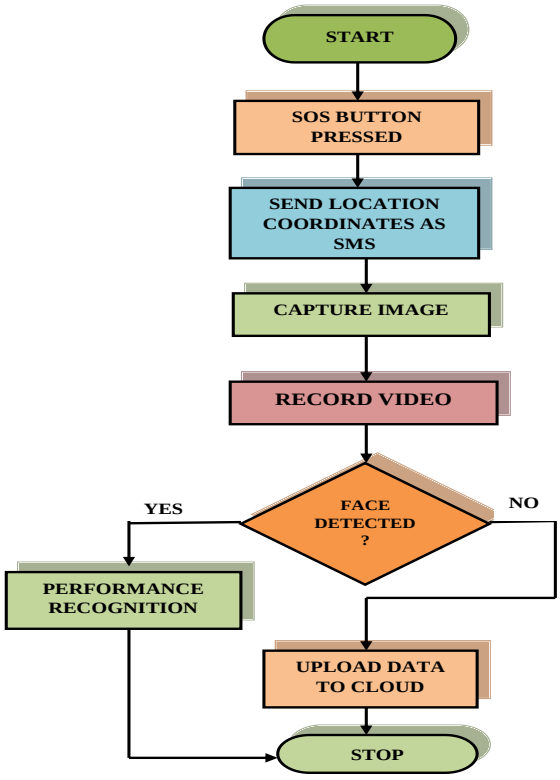

Figure 3: Flowchart for the safety device.

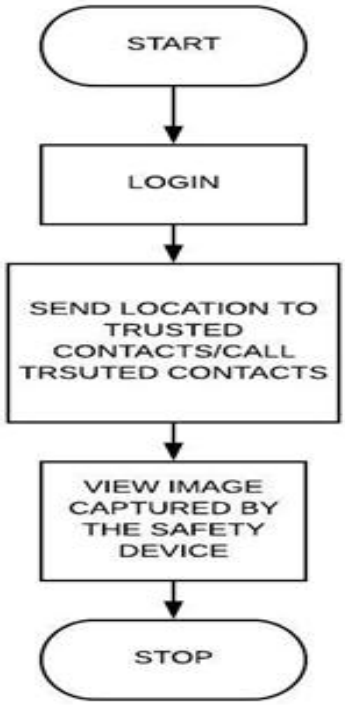

Figure 4: Flowchart for the Android App SEGURO.

V. RESULTS

The design was finalized and the device was assembled as per the protocol defined in the implementation section. The security system was made operational after interfacing with different hardware components and software modules. The results are briefly explained in the following sections.

5.1 GSM and GPS Module Results

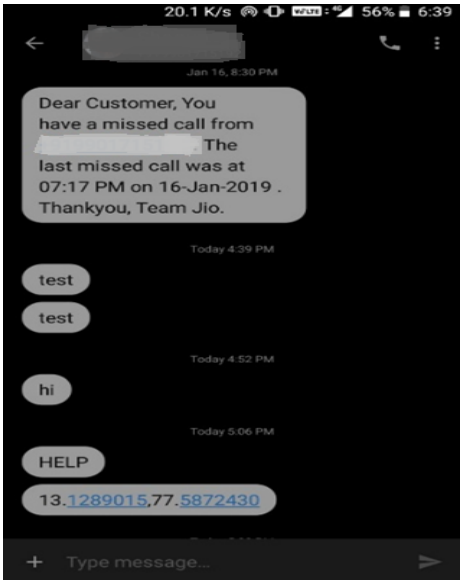

Figure 5: SOS Message

Figure 6: Location on Google Map

When the victim presses the SOS button the GPS module determines the current location of the victim that is sent as an SMS to the trusted contacts (Figure 5). When the coordinates are pasted in Google Maps application, the current location can be determined (Figure 6). A message that says "HELP" is also sent through the GSM module so that trusted contacts get to know that the victim is in danger. (Figure 5)

5.2 Image and Video Output:

Retrieval Number: 100.1/ijrte.D4894119420
DOI:10.35940/ijrte.D4894.119420
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication

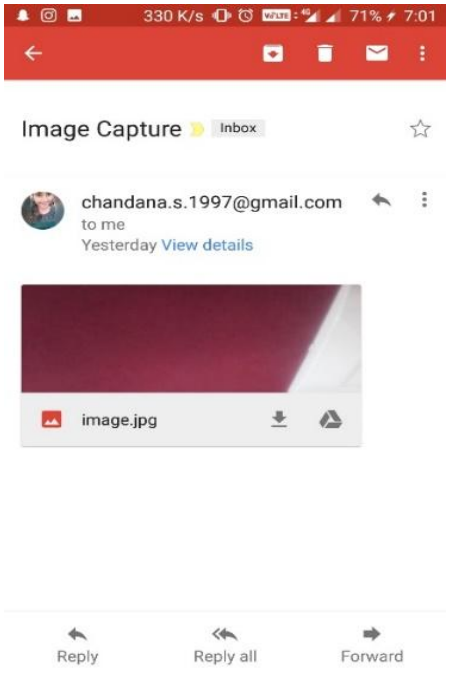

Figure 7:Image sent to Mail

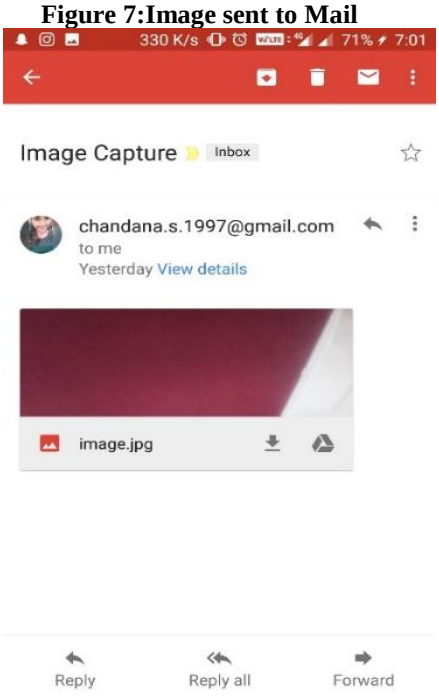

Figure 8:Image uploaded on drive

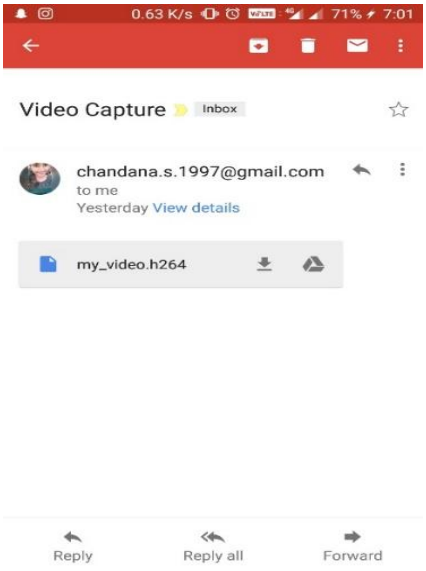

Figure 9:Video sent to Mail .

Figure 10: Location on the App

The image captured is sent to Gmail(Figure 7) and it is uploaded on Drive (Figure 8) so that the user can recognize the attacker. The image can be accessed through Drive and viewed through the app. A live video is recorded for ten seconds and it is mailed to the trusted contacts. The video can be viewed using VLC Media Player to recognize any familiar surroundings. The format of the recorded video is h244.(Figure 9)

5.3 SEGURO output

Figure 11: About the App

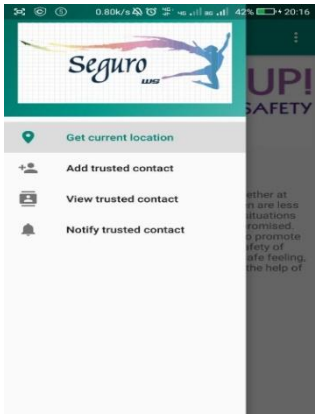

Figure 12: App functions

The App provides various features like displaying current location (Figure 10), sending current location to trusted contacts, add or view trusted contacts, call trusted contacts. It can also be used to view the image that is captured by the safety device. (Figure 11 and 12).

VI. CONCLUSION

The primary focus of the work is to ensure women's safety when the situation calls for it. With this thought in mind, the device is modelled and developed, providing accurate data which would help the women in times of need. Equipped with GPS module, GSM module and Camera, the location, image and video data are stored, sent to the trusted contacts and analyzed for further action. The device can be prototyped into various sizes ranging from a pendant to wearable vest.

REFERENCES

1. She the People TV, "RAVAN", [Online] Available : https://www.shethepeople.tv/blog/revenge-porn-stalking-body-shaming-heads-cyber-rava
2. Hongkiat, "Best 10 Personal Safety Apps for Women", [Online] Available: https://www.hongkiat.com/blog/android-personal-safety-women-apps/
3. A. Helen, M. F. Fathila, R. Rijwana and Kalaiselvi V.K.G., "A smart watch for women security based on IoT concept 'watch me'," *2017 2nd International Conference on Computing and Communications Technologies (ICCCT)*, Chennai, 2017, pp. 190-194. doi: 10.1109/ICCCT2.2017.7972266
4. Y. Lee, W. Yang and T. Kwon, "Data Transfusion: Pairing Wearable Devices and Its Implication on Security for Internet of Things," in *IEEE Access*, vol. 6, pp. 48994-49006, 2018. doi: 10.1109/ACCESS.2018.2859046
5. S. Seneviratne *et al*., "A Survey of Wearable Devices and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2573-2620, Fourthquarter 2017. doi: 10.1109/COMST.2017.2731979
6. M. Mahajan, K. Reddy and M. Rajput, "Design and implementation of a rescue system for safety of women," *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, 2016, pp. 1955-1959. doi: 10.1109/WiSPNET.2016.7566484
7. Wang, L & Feng, L. (2016). Preliminary Study on Wearable Devices based on Artificial Intelligence Algorithms. RevistaTecnica De La Facultad De Ingenieria Universidad Del Zulia. 39. 157-163. 10.21311/001.39.12.20.
8. [8] D. Chand, S. Nayak, K. S. Bhat, S. Parikh, Y. Singh and A. A. Kamath, "A mobile application for Women's Safety: WoSApp," *TENCON 2015 - 2015 IEEE Region 10 Conference*, Macao, 2015, pp. 1-5. doi: 10.1109/TENCON.2015.7373171
9. N. D. Wanjari and S. C. Patil, "Wearable devices," *2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT)*, Pune, 2016, pp. 287-290. doi: 10.1109/ICAECCT.2016.7942600
10. N. Viswanath, N. V. Pakyala and G. Muneeswari, "Smart foot device for women safety," *2016 IEEE Region 10 Symposium (TENSYMP)*, Bali, 2016, pp. 130-134. doi: 10.1109/TENCONSpring.2016.7519391
11. S. H. Nguyen, N. Ellis and R. Amirtharajah, "Powering smart jewelry using an RF energy harvesting necklace," *2016 IEEE MTT-S International Microwave Symposium (IMS)*, San Francisco, CA, 2016, pp. 1-4. doi: 10.1109/MWSYM.2016.7540339
12. G. C. Harikiran, K. Menasinkai and S. Shirol, "Smart security solution for women based on Internet Of Things(IOT)," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, 2016, pp. 3551-3554. doi: 10.1109/ICEEOT.2016.7755365
13. T. M. R, Aishwarya, C. K. S, D. M. K and N. H, "IoT Based Smart Security Gadget for Women's Safety," *2019 1st International Conference on Advances in Information Technology (ICAIT)*, Chikmagalur, India, 2019, pp. 348-352, doi: 10.1109/ICAIT47043.2019.8987242.
14. V. Hyndavi, N. S. Nikhita and S. Rakesh, "Smart Wearable Device for Women Safety Using IoT," *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, COIMBATORE, India, 2020, pp. 459-463, doi: 10.1109/ICCES48766.2020.9138047.

AUTHOR'S PROFILES

Anisha Sajit Kamat is currently employed at WIPRO as a project engineer. She pursued her bachelor's in computer science and Engineering atatNitte Meenakshi Institute of Technology. Her first project at WIPRO invloved statistical analysis of enormous amounts of customer data of Oriental Bank of Commerce(client)using SAS Business Intelligence tools. Presently, she's working with Punjab National Bank on a project that involves creating a strong foundation framework that enables the analysis of various business domains across the bank. Her work primarily focuses on analyzing and developing reports for client through SAP Business Objects, thereby assisting the bank in decision making and analysis.

Chandana S is currently working as a software engineer at Robert Bosch Engineering and Business Solutions Private Limited, Bengaluru, India. She has been working in RBEI for the past year. She pursued her bachelor's in computer science and Engineering at Nitte Meenakshi Institute Of Technology, Bengaluru, India. She was the gold medalist for her batch for the Computer Science and Engineering stream. She is currently working on a project that primarily focuses on handling the various servers in Business to Business applications at RBEI. She has also participated in developing a monitoring API for her department to track the department's daily and monthly progress. She also actively participated in setting up the webpage for her department. An avid art enthusiast, she focuses her free time with paints pencils and brushes.

J Jubila Teresa is currently working as a Software Development Engineer at McAfee Software India. She pursued her Bachelors at Nitte Meenakshi Institute of Technology, Bengaluru and majored in Computer Science and Engineering. She is passionate about solving problems and has shown her interest in the field of cyber security. She is currently working on design and development of software with an understanding of the existing system. She has developed internal tools for the company. Prior to this, she has worked for Wipro Limited as a Project Engineer where she used ETL tools such as DataStage and Informatica to design and enhance jobs to load daily sales data for the client. She is capable of adapting to new technologies and is fond of taking up new challenges.

Shagun Varma is currently a Masters student at University Of Massachusetts, USA majoring in Computer Science. She pursued her bachelor's in computer science and Engineering at atNitte Meenakshi Institute Of Technology, IND and majored in Computer Science And Engineering(CSE), predominantly focused on Artificial Intelligence. At Umass, she joined the UCaN lab in the Spring of 2020 and is currently working on a research project focused on analysis of the device usage and mobility and the diverse and time varying characteristics of wireless devices in ultradense wireless networks in order to evaluate accurate values and representations of the realistic systems as compared to the statistical analysis.

Dr. Thippeswamy M.N, Professor and Head, Department of Computer Science and Engineering (CSE), NitteMeenakshi Institute of Technology, Bengaluru. He holds Engineering Degree B.E (CSE) from JNNCE, Shimoga, Kuvempu University, INDIA. MTech (CSE) Degree from MSRIT, VTU, Bengaluru. He completed his Doctorate Degree from Howard college campus, University of KwaZulu-Natal, DURBAN, South Africa. A hard working creative professional and Sr. Academician offering 20+ years of experience and 5+ Research experience. He has worked in well-known colleges in Karnataka state and African universities. He has applied around 8 patents, co-authored Books and Book chapters, published around 17 journal papers and 42 conference papers of repute. He is a recipient of UKZN doctoral fund to design energy efficient MAC protocol for WSN from university of KwaZulu-Natal, DURBAN, South Africa. Further he has received a research grant of 15,000 ZAR (Grant in Rands) for developing data gathering algorithm for WSNs. He has completed 8 Research projects sponsored by various agencies of Govt. of INDIA and Govt. of Karnataka and Private Software Companies. His Interest areas are in the areas of IoT, Big data Analytics, Wireless Sensor Networks.