Mobile Notification System for Blood Pressure and Heartbeat Anomaly Detection

Saswat Raj Pandey[1], David Hicks[1], Ayush Goyal[1], Devottam Gaurav[2] and Sanju Mishra Tiwari[3,*]

[1]*Department of Electrical Engineering and Computer Science, Texas A&M University, Kingsville, United States*
[2]*Department of Computer Science and Engineering, IIT Delhi, India*
[3]*Universidad Autonoma de Tamaulipas, Mexico*
E-mail: sanju.tiwari.2007@gmail.com
[*]*Corresponding Author*

Received 23 March 2020; Accepted 18 August 2020;
Publication 10 December 2020

Abstract

In today's fast-paced world where patients may need to be remotely monitored while they are away or out of hospitals, there is a need for mobile applications that can gather the biometric and biomedical signals from any number of devices and sensors, collecting biometric or biomedical data from a patient. This effort boons the improvement of a circulatory strain and heartbeat anomaly detection and notice apparatus as an Android application that permits quick discovery of any variations from the norm in a patient's fundamental dependent on the Pan-Tompkins algorithm and reports it to the pertinent emergency clinic or clinical staff. The blood ECG information can be gotten from the health tracker sensors by means of a Bluetooth association and the patient can enter their Blood pressure esteems. In this case, the information gathered from a set of reproduced data, which is identified with a triggering notice from Firebase Cloud function. This notification is further acknowledged by the enrolled specialist. The system's security part is represented by the fine-grained consent procedure which directs that solitary significant authorizations are required for the best possible working of the

Journal of Web Engineering, Vol. 19_5–6, 747–774.
doi: 10.13052/jwe1540-9589.19568

application which ought to be given to the application. An encryption method using the Blowfish algorithm is included as a feature of the developed mobile Android application to provide secure data transfer of the patient's vital signals.

Keywords: Anomaly detection, Pan-Tompkins algorithm, Firebase cloud messaging service, diastolic blood pressure, systolic blood pressure, ECG.

1 Introduction

In a world loaded up with pressure, where individuals need everything to be in a hurry, the health area likewise are adjusted to the variable situation and to remain refreshed with the present changing technologies. An exceptionally well-timed sector where a crossing point is discovered amid the fitness segment and the universe of portable world. The strength area takes the option to remain at stride with the expanding requests of the quick stridden ecosphere by fusing the versatility and the pervasiveness of the portable biosphere. This intersection is termed as mHealth, this concept involves using mobile devices to collect health-related data, monitoring the patient's indispensable signs and making the data available for doctors, patients as well as researches whereby providing direct real-time health care by utilizing telemedicine [1].

In the previous decade, cell phones have been set up as a fundamental piece of our ever-propelling society. The pervasiveness of these cell phones makes them one of the most advantageous methods for correspondence that have highlights, for example, health condition observing. High blood pressure (BP) is the main cardiovascular hazard aspects, hitherto here occurs actual fewer consciousness related to hypertension and the controller tariffs is likewise short. A considerable lot of the individuals experiencing it do not realize while experiencing hypertension. The hazard may be diminished radically through simply overseeing hypertension. Current BP observing innovation, for example cuff less, utilizes different trackers to screen the patients' pulse and thus the following of the hushed assassin suitable and available to lots everywhere throughout the ecosphere. Along with this, if one can monitor their heart condition that would help in reducing any such problems.

A significant progression right now would be the capacity to distinguish the irregularity progressively and afterward have the option to advise the related person. Information gathered ought to be followed and made accessible to the specialist or clinical staffs who would then be able to make the vital strides toward the path, that might be nasty perhaps sparing a ton of

lives. American Heart Association (AHA), has expressed that 90% of the patients aren't ready to understand that thou are next to high hazard till the cardiovascular assault gangs in [2]. This hazard may be fundamentally diminished if the victim has devices for following own afflictive. As suggested through the AHA [2], the perfect period among the variances in the imperative cyphers and notifies the linked work force is generally amongst 4–6 minutes that is additionally careful as the ideal retro whichever might perhaps be the issue that spares the patient's lifespan. Recalling this as a main priority the developed system provides a means for the real-time detection and notification of abnormalities.

In addition to that, with the advancement of technology, there has been a near equal amount of increase in cyber crimes as well. Especially the medical data has its price as it is being sold for research purposes. Often time being distributed illegally without the consent of the concerned party. Hence in order to protect this data, we need to ensure proper security measures are taken. So keeping in mind the doctor-patient confidentiality the application that is developed in this work provides and ensures the data of the patient is secured and will not be mishandled. Figure 1 shows a basic overview of the system where the users' vital data transferred via Bluetooth connection, in the existing scenario the facts is obtained after the MIT-BIH record and is transferred via Bluetooth to the application. In the case of an anomaly, an alert is produced by the system which is sent to the registered clinical contact.

The remaining portion of the paper is organized as follows. In segment 2, the related works done in the arena of fitness portable application and

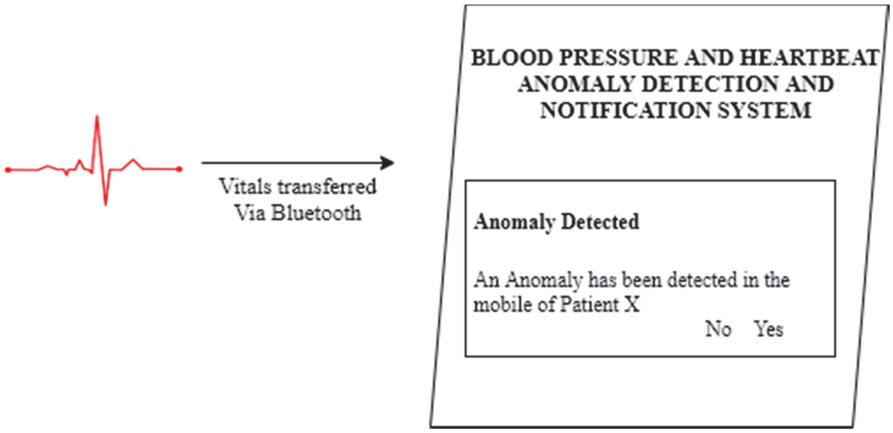

Figure 1 Basic application operation.

refuge are reviewed. Section 3 talk about the methodology that has been adopted along with the architecture of the system. The implementation of the algorithm are illustrated in Section 4. Section 5 describes the generation of alert with notification by the system. The discussion of results are shown in Section 6. Finally we have concluded with an overall discussion.

2 Related Work

In the later phases of the previous decades, the joining of nomad transportations with wearable sensors has encouraged the move of social insurance administrations from center driven to tolerant driven and is named as "Telemedicine" [2, 3]. We live in a world where it is estimated that the greater part of the total populace, 4.6 billion people, will be using a smartphone by 2019 [4], a mobile application designed for real-time monitoring of the user's blood pressure would contribute a lot to the "Telemedicine" sector [2].

From the expansion in the amount of clients who rely on mobile devices, the concern about the privacy and the security aspect also come into light. It is evident that nearly 80% of the mobile market share is encompassed by Android devices and this strength has prompted the improvement of millions of Android applications that add to the ever-growing ecosystem [3]. Android applications specifically, if not developed to be robust according to the security threats, are open to malicious third-party attacks that can steal confidential information from the user's device. This leaves a question for the user to decide whether an app would be safe or not.

With the idea of tracking of personal data of the users, analyzing it for anomalies, and making it available for the related personnel in charge, requires the data to be protected. Security is one of the paramount aspects of this current scenario. A mobile application dealing with such sensitive data needs to encompass all the relevant security protocols, mainly permissions, to be considered safe from the client's perspective.

Along with the security aspect, the storage, collection, and retrieval of the data is also a fundamental aspect of the developed application. It has been told by experts that the world's data has been doubling nearly every two years [5]. Although the relational database model (RDBMS) has been considered enough for handling various kind of datasets, the recent efflux of big data along with the increased need for data availability has inclined the technological world towards NoSQL. The influence of mobile health in the medical sector is ever growing and as a result, there are many applications

that provide useful functionality in one way or the other. Especially in the field of cardiology [6], some of the work relevant to the developed system has been discussed in the section below.

The system talked about in has given a line to the correspondence and warning of clients' crucial symbols to the specialists via the assistance of apparel instruments that separate the imperative data and moves it by means of Bluetooth. Despite the fact that the primary focal point of the system being discussed in [2] and the system created, right now, comparative, there are some characterizing factors that help separate the two. The organization's construction from [2] comprises of a UI, a cell phone and an online interface that does the handling and shows the outcomes to the related clinical person. From the start, the data is removed by the Android device and with the help of the inbuilt remote systems administration that can interface with a web worker which isolates the data and inspects for the experts to see.

As it is expressed in [7], a Wireless Health Monitoring System designed that screens the patients' vitals. Using a "3AHcare" center point as the information securing module responsible for the accompanying and forwarding the data to the compact application that is at risk for the taking care of, getting ready, and appearing of the data sensible by the customers.

The currently made media, of this work, beats this issue by the utilization of fine-grained security rule and encryption that creates the application continuously secure, guaranteeing the crucial data. In like manner recollecting the comfort of the customers the choice of using wearable sensors (in the recent express the reenacted data from the obscure database set aside in another contraption which will be moved by the help of an accomplice application that goes about as a sensor has been used), however, a vest has been used in [7]. One of the exceptional contrasts, regardless, would be the introduction of an additional interface that gives progressing notification to the masters or clinical individual in case of any irregularities. Another application observing a comparable standard of progressing notice has been inspected in [8]. Where the far off checking of the customers basic is done with the help of FORA D15b BG BPM [8] device, used to give sensor readings to the stage which is open monetarily. Another factor would be the security structures that have been joined by applying fine-grained encryption. Close by the extra interface where the customer can select as a patient or the authority accomplishes the included endorsement into the media. This is a relative gap that can be noticed in the framework inspected in [9].

The media discussed in [10] includes three critical parts: Wireless Wearable Body Area Network (WWBAN), Intelligent Central Node (ICN), and

Intelligent Central Server (ICS). The stage discussed in [10], is incredibly beneficial and has made the accompanying amazingly feasible. The made framework, at the present time, from UMHMSE [10], with respect to security features being incorporated as has been referenced in the above substance that has engaged the protected trade of the alert and the patient's data.

The association discussed in [11], is a wide restorative administration framework that engages self-organization for endless patients. The assets include the persevering well being checking framework, social sharing and status logging of the recorded information. The media has been made by the usage of a phone, wearable multi-detecting gadget, administration situated design for correspondence, and microblogging administrations. The test results show that the inspected framework isn't difficult to fathom and is definitely not hard to use.

One of the current qualification between the framework discussed in [12] and the stage that has been made, at the present time, the execution of security incorporates as encryption and the utilization of fine-grained approval principles. Adding to it the login and enlistment incorporate that makes the current association logically secure as it uses the endorsement handiness moreover.

The platform that has been discussed in [13] has a close resemblance with the application that has been developed. The application uses a altered form of Pan-Tompkins algorithm to detect the abnormality in the ECG signal and protects the figures in the server for upcoming reference of the doctor and the patient. The data that is received from the Bluetooth sensor. Some differences between the system that has been discussed in [13] and the system that has been developed are the implementation of the security features that have been achieved by the help of Blowfish algorithm and implementing fine-grained principles. Also, the use of Firebase as the server for storing the data and the use of Firebase cloud functionwhich is stored in the google server, for providing real-time notification makes the application more secure. Another vital fact that the system that has been developed can provide the notification irrespective of whether the user is connected to the internet or not. And the data is never lost as it has made use of Firebase offline capabilities which is further discussed in the upcoming section [14, 15].

The created system, of this work, gives a protected medium to the exchange message by the assistance of encryption and the application has been grown carefully following the fine-grained standards subsequently giving an effective method to monitor the basic variations from the norm in the patient's pulse perusing. It additionally gives secure ongoing notice to the

specialists or clinical person. The areas beneath talk about the execution of the created resources alongside the design that has been followed to get the normal results.

3 Methodology

This exertion introduces the improvement of a circulatory strain and heartbeat anomaly detection and warning apparatus as an Android application. As point by point in the above area and acquaintance this platform has pointed with present a protected application through the expansion of different highlights, in particular:

- Encryption, by the help of Blowfish Algorithm.
- Authentication, by login features and integration to the Firebase Server.
- Usage of the fine-grained structure standards.

These features have been integrated into various modules as will be discussed in the upcoming sections. The detection in the abnormalities in the user's ECG signal has been achieved using Pan Tompkins algorithm and the blood pressure deflection is calculated keeping the age of the patient in mind. The data storage, retrieval, and updating are being handled by using Firebase as the backend real-time server for the reason already discussed in the above section [16].

Authentication helps the application prevent unauthorized users from login to the application and increase entree to the user's critical health information. This acts as the first barrier between the user and the unauthorized personnel. The second protection is applied via. Encryption, where the data is saved to the Firebase real-time database is first encrypted from within the application and then passed on to Firebase for storage [17]. Upon retrieval, the application first gets the data in the form of ciphertext which is then decrypted from within the application to show the users the normal data. In doing so the secret key used for encryption will never be exposed to the cloud or as a matter of fact anywhere which provides the application impenetrable protection [18, 19].

The Bluetooth connection can only be established with another device once the authorized user's logs in to the application. This idea was applied for optimization, by only allowing the authorized personnel to access the features present in the application. Also, to prevent one user's data being passed and stored on to another users profile. The data that is obtained in this case will be sample data present in the MIT-BIH database [20–22]. The data that is

present there is in the .dat format which has first has been changed to the .csv format, in order to give a more realistic approach to the functionality of the application by providing the data format that closely matches the ones that the sensors will provide in real-case scenarios.

Upon receiving the data, it is then analyzed by the assistance of the Pan-Tompkins algorithm that helps in the detection of abnormalities in the dataset. In the event that a variation from the norm is identified, an alarm will be produced which will at that point be sent to the related clinical work force [23, 24]. There are two scenarios where the medium of sending the alert differs. One, when the application has a network connection and the other when it is disconnected from the network. The detailed explanation of the contents and how the alert is sent in different scenarios have been discussed in the upcoming sections. This feature allows the application to function independently without fully relying on the internet connection. Added to this, the alerts that are generated are stored onto the firebase real-time database that can be referenced by the patients and the doctors in the future. The details on how the storage is done can also be found in the upcoming sections [25, 26]. After the memo is directed to the various parts of the platform and will labor non-concurrently to convey the necessary outcome.

Fine-grained permission development methodology [27] has been applied in the development of the application whereby it only uses those components from the user's device that are necessary for it to function. This helps prevent third-party attacks an unwanted hacks onto the user's device. This execution has been accomplished by the assistance of introduce time strategy authorization. This may empower the meaning of isolated ways in the application inside, wherever every way will contain restricted permission to access only the relevant controls that will be required. This will make the issues that arise through over-privileged permissions obsolete [28–30].

For example, the application does not ask the users for permission to access their gallery, media or contacts. So, if a third-party attack is conducted on the developed application the malicious attackers will neither be able to get access to the data that is stored onto the Firebase database, since it is in chipper text [31, 32] which is not understandable, nor will they be able to access other resources on the user's device. This enables the data as well as device security. The upcoming modules elaborate on the architecture of the system model that was selected based on the above-discussed design rationale. Figure 2 below shows the basic system design [33, 34].

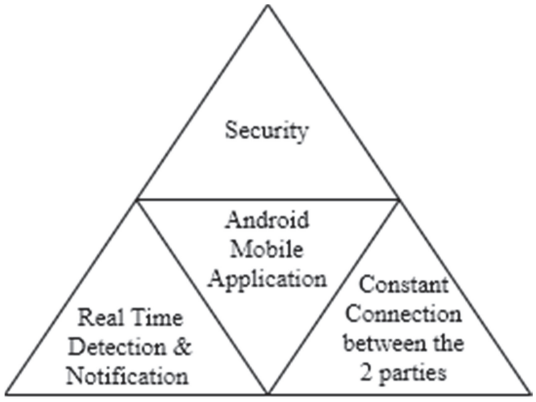

Figure 2 System design.

In this system, a notification module is developed to be responsible for making the doctor aware of the anomalies that are detected. It is the method of communiqué among the patient and the doctor via which they are kept up to date about the anomalies. The notification in the form of a push notification which will be triggered synchronously along with the alert in case of the detection of an anomaly in the vital signals. There are two ways in which the notification may be sent to the enrolled clinical work force based on the availability of an internet connection [35–37]. The two conditions are mentioned below:

(i) When there is an internet connection the notification will be sent to the application itself by the help of Firebase Cloud Messaging (FCM) service.
(ii) When the internet connection is not available the notification is sent by making use of the carrier messaging service.

In this way, the notification will always be directed to the related clinical staff regardless of whether the two parties are connected to the internet connection [38, 39]. The details of the implementation are explained in the sections below. All the modules impart and work non-concurrently by means of the utilization of different Android parts that will happen in every one of the modules. Figure 3 below is the pictorial view of how the various module interact with each other.

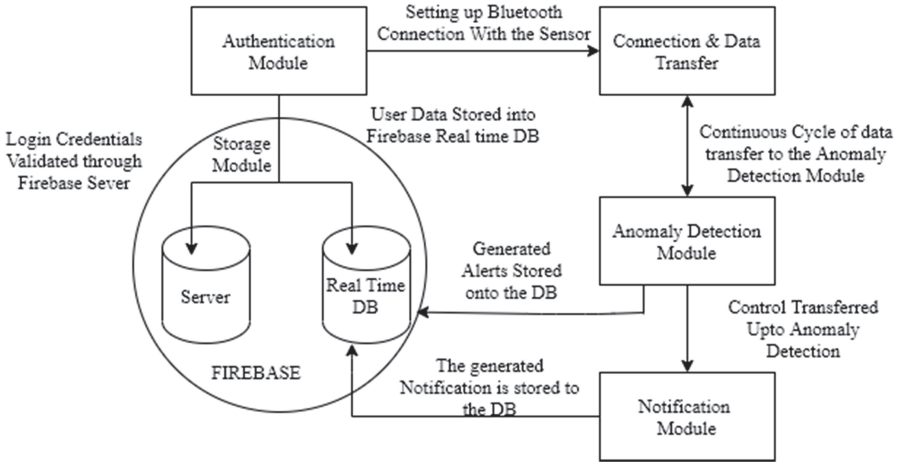

Figure 3 Architecture of the system.

4 Results

The entire functionality of the application is tested in this section. Both the Blood Pressure and ECG Signal are tested separately, where not only the detection but also the delivery of the notification to the user is taken as a criterion. So, the result section is separated broadly into dual foremost classes, viz.: (a) ECG Anomaly detection and Notification. (b) Blood Pressure Anomaly detection and Notification [40, 41].

4.1 Blood Pressure Anomaly detection and Notification

This slice will thoroughly test the application on the Blood pressure criterion. The test is divided into two categories, where one is when the Internet connection is present and another when it's not present [42]. This is because the application is able to work equally efficiently under both conditions. Table 1 below shows the desired range of blood pressure readings and anything above the normal range is taken as an abnormality.

Table 1 Blood pressure chart

Category/Stage	SBP (in mm Hg)	DBP (in mm Hg)
Normal Blood Pressure	90–140	60–90
Low Blood Pressure	40–90	20–60
High Blood Pressure	140–180	90–120
Hypertension	>180	>120
Hypotension	<40	<20

As the Blood Pressure is calculated by a set of two values where the higher range is the Systolic Blood Pressure (SBP) and the lower range is Diastolic Blood Pressure (DBP). The average time for the notification to be delivered when the Internet connection is present is in the range of 1–5 seconds. And the time when there is no Internet connection is 0–10 seconds.

4.1.1 Case 1: Internet Connection Present

Following 25 points of data were entered and the results are shown in Table 2 below for blood pressure abnormality detection with Internet connection, i.e. when the mobile phone and app had Internet connectivity.

Table 2 Results for blood pressure abnormality detection (with Internet connection)

S. No	Systolic Pressure Value	Diastolic Pressure Value	Abnormal Data	Detection and Notification Received
1	50	60	Yes	Yes
2	120	80	No	No
3	185	130	YES	YES
4	145	95	YES	YES
5	130	85	NO	NO
6	110	90	NO	NO
7	77	55	YES	YES
8	100	80	NO	NO
9	35	19	YES	YES
10	41	25	YES	YES
11	160	95	YES	YES
12	150	100	YES	YES
13	190	100	YES	YES
14	95	70	NO	NO
15	120	70	NO	NO
16	155	75	YES	YES
17	50	30	YES	YES
18	95	60	NO	NO
19	90	60	YES	YES
20	200	150	YES	YES
21	113	77	NO	NO
22	133	100	NO	NO
23	60	20	YES	YES
24	70	70	YES	YES
25	139	98	YES	YES

From the results from the table above, the following values for the confusion matrix have been assigned [43, 44].

Condition Positive (P) = 16	Condition Negative (N) = 9
True Positive (TP) = 16	True Negative (TN) = 9
False Positive (FP) = 0	False Negative (FN) = 0

Measure Value Derivations:

- Sensitivity (TPR) = TP / (TP + FN) = 1.0000
- Specificity (SPC) = TN / (FP + TN) = 1.0000
- Precision (PPV) = TP / (TP + FP) = 1.0000
- Negative Predictive Value (NPV) = TN / (TN + FN) = 1.0000
- False Positive Rate (FPR) = FP / (FP + TN) = 0.0000
- False Discovery Rate (FDR) = FP / (FP + TP) = 0.0000
- False Negative Rate (FNR) = FN / (FN + TP) = 0.0000
- Accuracy (ACC) = (TP + TN) / (P + N) = 1.0000

As can be seen from the results of the confusion matrix, the application is well able to detect the abnormality and send notification in case of an Internet connection [45, 46].

4.1.2 Case 2: No Internet Connection

Table 3 below displays the fallouts of the blood pressure abnormality detection in the event of no internet connection, that is, when the mobile phone and app had no Internet connectivity.

From the results from the table above, the following values for the confusion matrix have been assigned [47].

Condition Positive (P) = 16	Condition Negative (N) = 9
True Positive (TP) = 16	True Negative (TN) = 9
False Positive (FP) = 0	False Negative (FN) = 0

Measure Value Derivations:

- Sensitivity (TPR) = TP / (TP + FN) = 1.0000
- Specificity (SPC) = TN / (FP + TN) = 1.0000
- Precision (PPV) = TP / (TP + FP) = 1.0000
- Negative Predictive Value (NPV) = TN / (TN + FN) = 1.0000
- False Positive Rate (FPR) = FP / (FP + TN) = 0.0000
- False Discovery Rate (FDR) = FP / (FP + TP) = 0.0000
- False Negative Rate (FNR) = FN / (FN + TP) = 0.0000
- Accuracy (ACC) = (TP + TN) / (P + N) = 1.0000

Table 3 Results of blood pressure abnormality detection (without Internet connection)

S. No	Systolic Pressure Value	Diastolic Pressure Value	Abnormal Data	Detection and Notification Received
1	50	60	Yes	Yes
2	120	80	No	No
3	185	130	YES	YES
4	145	95	YES	YES
5	130	85	NO	NO
6	110	90	NO	NO
7	77	55	YES	YES
8	100	80	NO	NO
9	35	19	YES	YES
10	41	25	YES	YES
11	160	95	YES	YES
12	150	100	YES	YES
13	190	100	YES	YES
14	95	70	NO	NO
15	120	70	NO	NO
16	155	75	YES	YES
17	50	30	YES	YES
18	95	60	NO	NO
19	90	60	YES	YES
20	200	150	YES	YES
21	113	77	NO	NO
22	133	100	NO	NO
23	60	20	YES	YES
24	70	70	YES	YES
25	139	98	YES	YES

As can be seen from the results of the confusion matrix, the application is well able to detect the abnormality and send notification on the off chance that the application is detached from an Internet connection. The similar result in both the cases shows that the application is equally operational in both the scenarios [48, 49].

4.2 ECG Anomaly detection and Notification

This section like the one above will have two test cases and the data, in this case, has been transferred from the helper application. The data that

is stored to the device, containing the helper application, is sample data present in the MIT-BIH record. The results of the cases are shown below. This section checks various functionality of the application i.e. the Bluetooth connection, the abnormality detection, the efficiency of sending the notification to the doctor. The average time for the notification to be delivered when the Internet connection is present is in the range of 1–5 seconds. And the time when there is no Internet connection is 0–10 seconds. The tables below have all the required information required to calculate the efficiency of the application [50].

4.2.1 Case 1: Internet Connection

Table 4 below illustrates the consequences of the ECG abnormality uncovering with Internet connection, i.e. when the mobile phone and app had Internet connectivity.

From the results from the table above, the following values for the confusion matrix have been assigned.

Condition Positive (P) = 13	Condition Negative (N) = 12
True Positive (TP) = 12	True Negative (TN) = 12
False Positive (FP) = 1	False Negative (FN) = 0

Table 4 Results of ECG abnormality detection (with Internet connection)

S.No	ECG Data Name	Abnormal Data	Detection and Notification Received
1	ecg-mitdb100sig	YES	YES
2	ecg-mitdb101sig	YES	YES
3	ecg-mitdb102sig	YES	YES
4	ecg-mitdb103sig	YES	YES
5	ecg-mitdb105sig	YES	YES
6	ecg-mitdb107sig	YES	YES
7	ecg-mitdb108sig	YES	YES
8	ecg-mitdb109sig	YES	YES
9	ecg-mitdb111sig	YES	YES
10	ecg-mitdb112sig	YES	YES
11	ecg-mitdb123sig	YES	YES
12	ecg-mitdb215sig	YES	YES
13	ecg-mitdb220sig	YES	NO
14	ecg-mitdb16265sig	NO	NO
15	ecg-mitdb16272sig	NO	NO

(*Continued*)

Table 4 Continued

S.No	ECG Data Name	Abnormal Data	Detection and Notification Received
16	ecg-mitdb16420sig	NO	NO
17	ecg-mitdb16483sig	NO	NO
18	ecg-mitdb16539sig	NO	NO
19	ecg-mitdb16795sig	NO	NO
20	ecg-mitdb18177sig	NO	NO
21	ecg-mitdb18184sig	NO	NO
22	ecg-mitdb19090sig	NO	NO
23	ecg-mitdb19093sig	NO	NO
24	ecg-mitdb19140sig	NO	NO
25	ecg-mitdb19830sig	NO	NO

Measure Value Derivations:

- Sensitivity (TPR) = TP / (TP + FN) = 1.000
- Specificity (SPC) = TN / (FP + TN) = 0.9231
- Precision (PPV) = TP / (TP + FP) = 0.9231
- Negative Predictive Value (NPV) = TN / (TN + FN) =1.000
- False Positive Rate (FPR) = FP / (FP + TN) = 0.0769
- False Discovery Rate (FDR) = FP / (FP + TP) = 0.0769
- False Negative Rate (FNR) = FN / (FN + TP) = 0.0000
- Accuracy (ACC) = (TP + TN) / (P + N) = 0.9600

As can be seen from the result, the application shows good accuracy, precision, specificity, and sensitivity [51, 52] which means that the application can predict the abnormality accurately.

4.2.2 Case 2: No Internet Connection

Table 5 below shows the results of the ECG abnormality detection without Internet connection, i.e. when the mobile phone and app had no Internet connectivity.

From the results from the table above, the following values for the confusion matrix have been assigned.

Condition Positive (P) = 13	Condition Negative (N) = 12
True Positive (TP) = 12	True Negative (TN) = 12
False Positive (FP) = 1	False Negative (FN) = 0

Table 5 Results of ECG abnormality detection (without Internet connection)

S.No	ECG Data Name	Abnormal Data	Detection and Notification Received
1	ecg-mitdb100sig	YES	YES
2	ecg-mitdb101sig	YES	YES
3	ecg-mitdb102sig	YES	YES
4	ecg-mitdb103sig	YES	YES
5	ecg-mitdb105sig	YES	YES
6	ecg-mitdb107sig	YES	YES
7	ecg-mitdb108sig	YES	YES
8	ecg-mitdb109sig	YES	YES
9	ecg-mitdb111sig	YES	YES
10	ecg-mitdb112sig	YES	YES
11	ecg-mitdb123sig	YES	NO
12	ecg-mitdb215sig	YES	YES
13	ecg-mitdb220sig	YES	NO
14	ecg-mitdb16265sig	NO	NO
15	ecg-mitdb16272sig	NO	NO
16	ecg-mitdb16420sig	NO	NO
17	ecg-mitdb16483sig	NO	NO
18	ecg-mitdb16539sig	NO	NO
19	ecg-mitdb16795sig	NO	NO
20	ecg-mitdb18177sig	NO	NO
21	ecg-mitdb18184sig	NO	NO
22	ecg-mitdb19090sig	NO	NO
23	ecg-mitdb19093sig	NO	NO
24	ecg-mitdb19140sig	NO	NO
25	ecg-mitdb19830sig	NO	NO

Measure Value Derivations:

- Sensitivity (TPR) = TP / (TP + FN) = 1.000
- Specificity (SPC) = TN / (FP + TN) = 0.9231
- Precision (PPV) = TP / (TP + FP) = 0.9231
- Negative Predictive Value (NPV) = TN / (TN + FN) = 1.000
- False Positive Rate (FPR) = FP / (FP + TN) = 0.0769
- False Discovery Rate (FDR) = FP / (FP + TP) = 0.0769
- False Negative Rate (FNR) = FN / (FN + TP) = 0.0000
- Accuracy (ACC) = (TP + TN) / (P + N) = 0.9600

As can be seen from the results of the confusion matrix, the application is well able to detect the abnormality and send notification on the off chance that the application is detached from an Internet connection. The similar result in both the cases shows that the application is equally operational in both the scenarios. Figures 4 through 7 demonstrate how the ECG anomaly detection is done. Figure 4 shows the application searching for a Bluetooth sensor, in the case of this application it is the mobile device that contains the helper application as seen in Figure 5. The application will list all the nearby Bluetooth devices, and all the user needs to do is select the respective sensor device.

To replicate a real-world scenario, in our case the device that contains the helper application [53–55] is selected. Upon establishing the connection, the helper application will list the sample data that is stored in the device in which the helper application is installed.

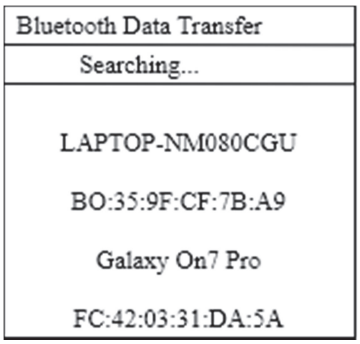

Figure 4 Mobile application searching for Bluetooth device.

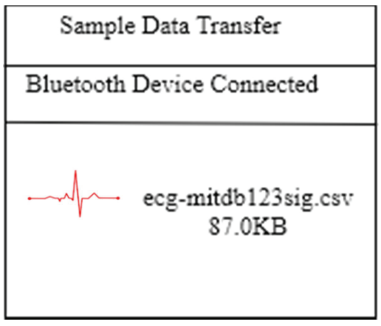

Figure 5 Helper application acting like a sensor housing the sample data.

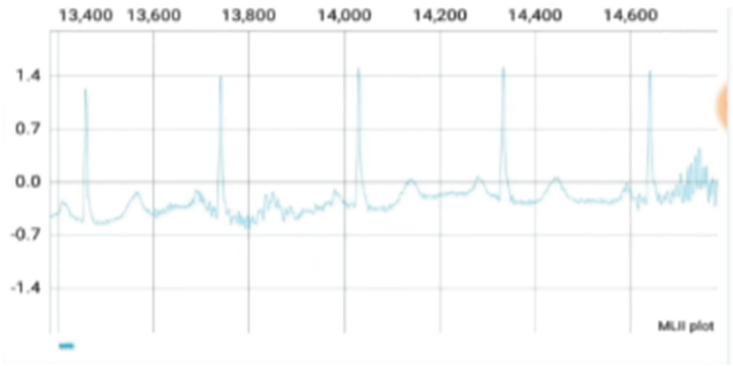

Figure 6 The ECG signal being analyzed in real-time in the mobile app.

Abnormality Detected!! Result:PVC: 11/0|
Fused: 5/0|Aberrant: 12/0|APC:6/0|AV:3/0|
Others: 3/0|Heart Rate: 70

Figure 7 The generated alert for abnormality detected in ECG (ecg-mitdb101sig).

In our case, we have selected the sample data with the name, ecg-mitdb123sig.csv, which is then transferred in real time to the application developed for this work which analyzes it in real time plotting the signal as it receives the data as seen in Figure 6.

Since the data being provided is an abnormal data, the anomaly in the signal is detected and the notification as seen in Figure 7 is sent to the related medical personnel [56–60].

5 Conclusion

In the system that has been developed, we have put forth a real-time anomaly detection system that encapsulates security, data protection, and efficiency. The system doesn't just detect the abnormalities in the patient's vital signs but also is responsible for the timely delivery of the data to the related medical personnel. All the while protecting the personal as well as medical information of both the parties involved. Unlike the systems that are responsible for detecting the abnormalities, this application goes a few steps further by providing features such as authentication, cryptography, data storage in NoSQL, and providing real-time notification. Applying fine-grained principles in the development and by storing the server-side code in Google's

server along with storing the data in an encrypted form makes the application really secure against third-party attacks. Added to this, the ability to function efficiently regardless of the network connection enables the system to be a really meaningful and useful application. Below listed are the future works that would mostly be included in the current developed system.

The following sets of application functionality are being looked into to be added on as future features in the application. The list of possible additions is: (a) A remote 911 call to be triggered on extreme anomaly detection with recorded voice message containing location and alert. (b) Enabling messaging service between the two parties involved. (c) Creating a web application for the same which can be used by hospitals. (d) To track the activity when the abnormality occurs. (e) Add more factors into the classification of the abnormality than just the QRS complex.

Acknowledgments

The authors would like to thank and acknowledge the Department of Electrical Engineering and Computer Science at Texas A&M University – Kingsville for providing the resources and labs that were used to conduct this research. This research was part of a master's thesis research conducted in the Department of Electrical Engineering and Computer Science at Texas A&M University – Kingsville.

References

[1] A. Secerbegovic, A. Mujčić, N. Suljanović, M. Nurkic, and J. Tasic, "The research mHealth platform for ECG monitoring," *Proceedings of the 11th International Conference on Telecommunications*, Graz, 2011, pp. 103–108.

[2] P. Kakria, N. Tripathi and P. Kitipawang, "A Real-Time Health Monitoring System for Remote Cardiac Patients Using Smartphone and Wearable Sensors", *International Journal of Telemedicine and Applications*, vol. 2015, pp. 1–11, 2015.

[3] M. Sarkaleh, "Classification Of Ecg Arrhythmias Using Discrete Wavelet Transform and Neural Networks", *International Journal of Computer Science, Engineering and Applications*, vol. 2, no. 1, pp. 1–13, 2012.

[4] "Number of mobile phone users worldwide 2015-2020 | Statista", *Statista*, 2018. [Online]. Available: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/.

[5] G. Friesen, T. Jannett, M. Jadallah, S. Yates, S. Quint,and H. Nagle, "A comparison of the noise sensitivity of nine QRS detection algorithms", *IEEE Transactions on Biomedical Engineering*, vol. 37, no. 1, pp. 85–98, 1990.

[6] Pan and W. Tompkins, "A Real-Time QRS Detection Algorithm", *IEEE Transactions on Biomedical Engineering*, vol. -32, no. 3, pp. 230–236, 1985.

[7] Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B., Cox, L., Jung, J., McDaniel, P. and Sheth, A. (2014). "TaintDroid". *ACM Transactions on Computer Systems*, 32(2), pp. 1–29.

[8] J. Jeon, K. Micinski, J. Vaughan, A. Fogel, N. Reddy, J. Foster,and T. Millstein ."Dr. Android and Mr. Hide: Fine-grained Permissions in Android Applications", *SPSM'12 Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*, pp. 3–14, 2012.

[9] J. Fu, Y. Zhou, H. Liu, Y. Kang and X. Wang, "Perman: Fine-Grained Permission Management for Android Applications," *2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE)*, Toulouse, 2017, pp. 250–259.

[10] Z. Fang, W. Han, and Y. Li, "Permission based Android security: Issues and countermeasures", *Computers & Security*, vol. 43, pp. 205–218, 2014.

[11] M. K. Hasan, N. Ahmed and A. H. M. S. Islam, "Android mobile application: Remote monitoring of blood pressure," *2012 15th International Conference on Computer and Information Technology (ICCIT)*, Chittagong, 2012, pp. 215–220.

[12] D. Lou, X. Chen, Z. Zhao, Y. Xuan, Z. Xu, H. Jin, X. Guo,and Z. Fang, "A Wireless Health Monitoring System based on Android Operating System", *IERI Procedia*, vol. 4, pp. 208–215, 2013.

[13] Singh, G., Kr. Singla, A. and S. Sandha, K. (2012). A Study of New Trends in Blowfish Algorithm. *International Journal of Engineering Research and Applications (IJERA)*, 1(2), pp. 321–326.

[14] B. Rashidi, C. Fung,and T. Vu, "Android fine-grained permission control system with real-time expert recommendations", *Pervasive and Mobile Computing*, vol. 32, pp. 62–77, 2016.

[15] D. Geneiatakis, I. Fovino, I. Kounelis,and P. Stirparo, "A Permission verification approach for android mobile applications", *Computers & Security*, vol. 49, pp. 192–205, 2015.

[16] D. Hee, A. Rabbi, J. Choi,and R. Fazel-Rezai, "Development of a Mobile Phone Based e-Health Monitoring Application", *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 3, 2012.

[17] A. BOUROUIS, M. FEHAM,and A. BOUCHACHIA, "Ubiquitous Mobile Health Monitoring System for Elderly (UMHMSE)", *International Journal of Computer Science and Information Technology*, vol. 3, no. 3, pp. 74–82, 2011.

[18] A. Triantafyllidis, V. Koutkias, I. Chouvarda,and N. Maglaveras, "A Pervasive Health System Integrating Patient Monitoring, Status Logging, and Social Sharing", *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 1, pp. 30–37, 2013.

[19] A. Abdullah, A. Ismael, A. Rashid, A. Abou-Elnour and M. Tarique, "Real Time Wireless Health Monitoring Application Using Mobile Devices", *International Journal of Computer Networks & Communications*, vol. 7, no. 3, pp. 13–30, 2015.

[20] L. Clifton, D. Clifton, M. Pimentel, P. Watkinson,and L. Tarassenko, "Predictive Monitoring of Mobile Patients by Combining Clinical Observations With Data From Wearable Sensors", *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 3, pp. 722–730, 2014.

[21] R. Treskes, E. van der Velde, R. Barendse and N. Bruining, "Mobile health in cardiology: a review of currently available medical apps and equipment for remote monitoring", *Expert Review of Medical Devices*, vol. 13, no. 9, pp. 823–830, 2016.

[22] *People.eecs.berkeley.edu*, 2018. Available: https://people.eecs.berkeley.edu/~daw/papers/perms-webapps11.pdf. [Accessed: 05-Nov-2018].

[23] L. Wu, X. Du and H. Zhang, "An effective access control scheme for preventing permission leak in Android," *2015 International Conference on Computing, Networking and Communications (ICNC)*, Garden Grove, CA, pp. 57–61, 2015.

[24] W. Ahmad, C. Kästner, J. Sunshine and J. Aldrich, "Inter-app Communication in Android: Developer Challenges," *2016 IEEE/ACM 13th Working Conference on Mining Software Repositories (MSR)*, Austin, TX, pp. 177–188, 2016.

[25] K. AlSharqi, A. Abdelbari, A. Elnour,and M. Tarique, "Zigbee Based Wearable Remote Healthcare Monitoring System for Elderly Patients",

International Journal of Wireless & Mobile Networks, vol. 6, no. 3, pp. 53–67, 2014.

[26] F. Wu, H. Zhao, Y. Zhao and H. Zhong, "Development of a Wearable-Sensor-Based Fall Detection System", *International Journal of Telemedicine and Applications*, vol. 2015, pp. 1–11, 2015.

[27] A. Nadeem and M. Y. Javed, "A Performance Comparison of Data Encryption Algorithms," *2005 International Conference on Information and Communication Technologies*, Karachi, Pakistan, pp. 84–89, 2005.

[28] R. Bhanot and R. Hans, "A Review and Comparative Analysis of Various Encryption Algorithms", *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 289–306, 2015.

[29] G. Singh and S. Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES,and AES) for Information Security", *International Journal of Computer Applications*, vol. 67, no. 19, pp. 33–38, 2013.

[30] S. Omer AL Faroog Mohammed Koko and D. Babiker A/Nabi Mustafa, "Comparison of Various Encryption Algorithms and Techniques for improving secured data Communication", pp 62–69, 2015.

[31] P. Kasturia and K. Maheshwar, "Critical Analysis of Various Cryptographic Algorithms", *Journal Of Ultra Computer & Information Technology, Feb. 2017.*

[32] J.X. Sun, A.T. Reisner, R.G. Mark,"A signal abnormality index for arterial blood pressure waveforms", ComputCardiol, pp. 13–16, 2006.

[33] R. Treskes, E. van der Velde, R. Barendse and N. Bruining, "Mobile health in cardiology: a review of currently available medical apps and equipment for remote monitoring", *Expert Review of Medical Devices*, vol. 13, no. 9, pp. 823–830, 2016.

[34] P. Tirumala Rao, S. Koteswarao Rao, G. Manikanta and S. Ravi Kumar, "Distinguishing Normal and Abnormal ECG Signal", *Indian Journal of Science and Technology*, vol. 9, no. 10, 2016.

[35] R. Álvarez, A. Penín and X. Sobrino, "A Comparison of Three QRS Detection Algorithms Over a Public Database", *Procedia Technology*, vol. 9, pp. 1159–1165, 2013.

[36] S. Saraswat, G. Srivastava,and S. Shukla, "Review: Comparison of QRS detection algorithms," *International Conference on Computing, Communication & Automation*, Noida, pp. 354–359, 2015.

[37] Almootassem, O., Husain, S., Parthipan, D. and Mahmoud, Q. (2017). A Cloud-based Service for Real-Time Performance Evaluation of NoSQL Databases.

[38] Jason W. Cornwell,"Blowfish Survey", *Department of Computer Science Columbus State University*.

[39] Valmik, M. and Kshirsagar, P. (2014). Blowfish Algorithm. *IOSR Journal of Computer Engineering*, 16(2), pp. 80–83.

[40] Khawas, C. and Shah, P. (2018). Application of Firebase in Android App Development-A Study. *International Journal of Computer Applications*, 179(46), pp. 49–53.

[41] Overview of Backend as a Service platform –

[42] P. K. Gakare, A. M. Patel, J. R. Vaghela and R. N. Awale, "Real time feature extraction of ECG signal on android platform," *2012 International Conference on Communication, Information & Computing Technology (ICCICT)*, Mumbai, 2012, pp. 1–5. doi: 10.1109/ICCICT.2012.6398230

[43] Manku, S. and Vasanth, K. (2015). Blowfish Encryption Algorithm for Information Security. *ARPN Journal of Engineering and Applied Sciences*, 10(10), pp. 4717–4719.

[44] StefanGradl, Patrick Kugler, Clemens Lohmüller, and BjoernEskofier, Real-time ECG monitoring and arrhythmia detection using Android-based mobile devices, *in 34th Annual International Conference of the IEEE EMBS*, 2012, pp. 2452–2455.

[45] R. Fensli, E. Gunnarson and T. Gundersen, "A wearable ECG-recording system for continuous arrhythmia monitoring in a wireless tele-home-care situation," *18th IEEE Symposium on Computer-Based Medical Systems (CBMS'05)*, Dublin, 2005, pp. 407–412. doi: 10.1109/CBMS.2005.22

[46] N. Vuong, T. Nguyen, L. D. Tran, and T. Van Huynh, "Detect QRS complex in ECG," *2017 12th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, Siem Reap, 2017, pp. 2022–2027. doi: 10.1109/ICIEA.2017.8283170

[47] Tirumala Rao, P., Koteswarao Rao, S., Manikanta, G. and Ravi Kumar, S. (2016). Distinguishing Normal and Abnormal ECG Signal. *Indian Journal of Science and Technology*, 9(10).

[48] Gaurav, D., Tiwari, S. M., Goyal, A., Gandhi, N., & Abraham, A. (2019a). Machine intelligence-based algorithms for spam filtering on document labeling. Soft Computing, 1–14.

[49] Rahul, M., Kohli, N., Agarwal, R., & Mishra, S. (2019). Facial expression recognition using geometric features and modified hidden Markov model. International Journal of Grid and Utility Computing, 10(5), 488–496.

[50] Mishra, S., Sagban, R., Yakoob, A., & Gandhi, N. (2018). Swarm intelligence in anomaly detection systems: an overview. International Journal of Computers and Applications, 1–10.
[51] Goyal, A., Hossain, G., Chatrati, S. P., Bhattacharya, S., Bhan, A., Gaurav, D., &Tiwari, S. M. (2020). Smart Home Health Monitoring System for Predicting Type 2 Diabetes and Hypertension. Journal of King Saud University-Computer and Information Sciences.
[52] Gaurav D., Yadav J.K.P.S., Kaliyar R.K., Goyal A. (2019). Detection of False Positive Situation in Review Mining. In: Wang J., Reddy G., Prasad V., Reddy V. (eds) Soft Computing and Signal Processing. Advances in Intelligent Systems and Computing, vol 900. Springer, Singapore.
[53] Tiwari, S. M., Jain, S., Abraham, A., & Shandilya, S. (2018). Secure Semantic Smart HealthCare (S3HC). Journal of Web Engineering, 17(8), 617–646.
[54] Aditya, T. R., Pai, S. S., Bhat, K., Manjunath, P., & Jagadamba, G. (2020, July). Real Time Patient Activity Monitoring and Alert System. In2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 708-712). IEEE.
[55] Fang, L., Li, Y., Liu, Z., Yin, C., Li, M., & Cao, Z. J. (2020). A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services Against External Attacks. IEEE Transactions on Industrial Informatics.
[56] Sihombing, P., Barus, Y. E., Sembiring, S., & Zamzami, E. M. (2020, June). The Development of Heart Rate Detection Using Arduino Microcontroller and Android. InJournal of Physics: Conference Series (Vol. 1566, No. 1, p. 012027). IOP Publishing.
[57] Srinivasan, P., Khan, A. A., Prabu, T., Manoj, M., Ranjan, M., & Karthik, K. (2020). Heart beat sensor using fingertip through Arduino. Journal of Critical Reviews, 7(7), 1058–1060.
[58] Li, H., & Boulanger, P. (2020). A Survey of Heart Anomaly Detection Using Ambulatory Electrocardiogram (ECG). Sensors, 20(5), 1461.
[59] Ben Amor, L., Lahyani, I., & Jmaiel, M. (2020). AUDIT: AnomaloUs data Detection and Isolation approach for mobile healThcare systems. Expert Systems, 37(1), e12390.
[60] Phaltankar, S., Tyagi, K., Prabhu, M., Jaguste, P., Sahu, S., & Kalbande, D. CuraBand: Health Monitoring and Warning System. InInternational Conference on Innovative Computing and Communications (pp. 1017–1026). Springer, Singapore.

Biographies

Saswat Raj Pandey completed his Masters in Computer Science from Texas A&M University-Kingsville. He has conducted research in telemedicine, combining mobile and health together as his thesis project to develop an application that tracks anomalies in the patient's blood pressure and heart rate and for sending notifications to the relevant doctors. He is an experienced mobile app developer who has a track record of successfully owning the entire development lifecycle from selecting roadmap features, including design, development, testing, release, and post-release support for both Android and iOS platforms.

David Hicks is an Associate Professor in the Electrical Engineering and Computer Science Department at Texas A&M University-Kingsville. Before joining TAMU-K he served as Associate Professor and Department Head at Aalborg University in Esbjerg, Denmark. He has also held positions in research labs in the U.S. as well as Europe, and spent time as a researcher in the software industry. His research interests include knowledge management, software engineering, mobile computing platforms, and computer science education. Dr. Hicks received his B.S. degree in Computer Science from Angelo State University, and his MCS and Ph.D. degrees in computer science from Texas A&M University.

Ayush Goyal completed his Ph.D. in computer science from the University of Oxford in 2013. Currently, he is an Assistant Professor of Computer Science in the Department of Electrical Engineering and Computer Science at Texas A&M University – Kingsville. His research interests are in machine learning algorithms and artificial intelligence models with applications in computer vision, machine vision, pattern recognition, object detection, and biomedical engineering and image processing. He has worked as a research assistant at King's College London in biomedical engineering, in the area of cardiac MRI image processing. He has also done post-doctoral research at Tulane University in bioinformatics.

Devottam Gaurav is currently working as Sr. Project Assistant in the department of Computer Science & Engineering, IIT, Delhi. He worked as Assistant Professor in NIET, Gr. Noida for 3 years. He received his B.E. degree in Information Science & Engineering from Basaveshwar Engineering College, Karnataka in 2012 and MTech – Computer Science & Engineering from Birla Institute of Technology, Ranchi in 2015. His research areas include machine learning, artificial intelligence.

Sanju Mishra Tiwari is a Senior Researcher at Universidad Autonoma de Tamaulipas (70 years old University), Mexico. She has worked as a Post-Doctoral Researcher in Ontology Engineering Group, Universidad Polytecnica De Madrid, Spain. Prior to this, she has worked as a Research Associate for a sponsored research project "Intelligent Real time Situation Awareness and Decision Support System for Indian Defence" funded by DRDO, New Delhi in Department of Computer Applications, National Institute of Technology, Kurukshetra. In this project, she has developed and evaluated a Decision Support System for Indian Defence. Her current research interests include, Ontology Engineering, Knowledge Graphs, Linked Data Generation and Publication, Semantic Web, Reasoning with SPARQL and Machine Intelligence. She has designed a Smart Health Care Ontology and published it on Linked Data. She has to-date published 26 research papers and 6 book chapters with International and National publishers and 2 Springer books in AISC and CCIS series. She is the member of IEEE. She is working as a General Chair (KGSWC-2020), Session Chair (IEMIS-2020) and worked as Organizing Chair, Proceeding Chair and Publicity Chair for the International Conferences and Workshops (2019) of MIR Labs, USA. She is a PC Member of Research and Innovation Track in SEMANTiCS 2019–20, Karlsruhe and CIKM2020 Ireland conference. She has edited a Springer Proceeding Book as a Co-Editor for the SoCPaR-2019. She has worked as a Guest Editor for IGI-Global and Inderscience Journals and currently working as a Guest Editor for MTAP Springer Journal.